

Forum:[Hack Forums](#)

Thread: [Looking to form or join an off-site hacking-oriented crew.](#)

Phizo - July 16, 2019, 4:19 pm

EDIT:

So, I've had quite a lot of offers, three of which seemed worthwhile. One PM'd me twice and then dropped off after my second reply (hasn't responded for a while despite being online/active), another hit me up on XMPP but haven't heard anything since, the other being on-site and the only one I've taken up: Sui Generis (cheers Tyler).

Due to this, I may just spin something up of my own off-site (while still being a part of Sui Generis). PM me if you meet the requirements. I'd appreciate it if you don't PM me otherwise, as I do not want my time wasted. A degree in Computer Science or equivalent would be much preferred. If you cheated your way through university, and therefore cannot prove yourself; again, please don't waste my time.

Please note this is not about bragging; I'm seriously looking for some cool individuals to hang with. Also note that I'm not necessarily suggesting that I'm forming the crew and inviting others in. I'm either looking for an existing crew or forming one.

As can be observed on my profile, I've been here since February '09. I've seen a lot of groups/crews but nothing of immediate interest. I haven't frequented these forums in quite some time due to the lack of intriguing content. However, I'll be on to scout for anything of interest for the next couple weeks to see if there's anything interesting to reply to and to check for responses to this thread; for the past couple years or so, mostly I come online just to answer others' enquiries through random threads and received PMs.

Requirements

No skids.

Proficiency in at least one area per person related to hacking (but preferably several areas each) with a continued curiosity/development in general.

A degree in Computer Science or equivalent would be much preferred.

My own experience and knowledge can be observed in my threads and posts. However, I will demonstrate some of my experience below.

Introduction

I have a degree in computer science (among others) and have since been working as a security consultant/penetration tester. I majored in digital systems security and finished with a distinction. I was also invited/added to an honours society for being (anywhere) within the top 15% of computer science studies in the state. I have a fair amount of programming and general computer science and security experience.

From a testing standpoint, I have decent experience with web-apps, web services (e.g., APIs), mobile-apps, internal/external infrastructures, wireless, VoIP (e.g., RTP/SIP/H.323 attacks, VLAN hopping, eavesdropping, spoofing, etc.), cloud and virtualisation, social engineering, source code review, etc. Also more specialised testing such as reverse engineering, cryptanalysis and general cryptography/cryptanalysis knowledge, (zero-day) exploit development (of various layers),

red-teaming, etc. Note that this is not an exhaustive list.

Examples of programming experience

Within the past few years, I have demonstrated fluency in the following programming languages:

Assembly (x86/x86-64)

C

C++

Java

Fortran

Lisp

Prolog

Haskell

Ruby

Python

PHP

JavaScript

XML (including XQuery and XPath)

HTML

CSS

Note that this is not exhaustive; I have worked in many other languages. This is simply what I've worked with during the past few years. I have been programming for a very long time.

I am also very familiar with the following programming paradigms:

Imperative

Object-oriented

Declarative: functional and logic

Literate

I have no problem proving that I am fluent in any of the above (or otherwise).

I'm pedantic when it comes to the quality of code and have worked on plenty of complex projects - hacking/security-related and otherwise.

I will mention a few projects, challenges, etc., I've involved myself in to demonstrate knowledge/experience. Currently working through [set 5/8](#) of [Matasano's cryptography challenges](#) (now NCC Group). Let me know if you want to see some code.

GNU/Linux rootkit (see below for more info). Let me know if you want to see some code.

Participate in modern binary exploitation labs/challenges such as RPISEC MBE, STS, OTW, etc.

Developed a PHP shell back in 2011 which bypassed Suhosin-protected environments among other (unique) features (and was better than Fuhosin).

To give an idea regarding the rootkit: it is a highly-dynamic GNU/Linux user-land (ring 3) LD_PRELOAD rootkit written in C (at its core) in the sense that the code will modify itself at both compile-time and run-time (one example being that it will determine hooks and correlating shared objects, macros, etc., and populate its arrays at run-time). It is not publicly available, as it includes functionality not typically found in public rootkits. In addition to the aforementioned, disclosable features include anti-detection/forensics/debugging via reverse engineering of the Linux dynamic linker (ld.so) and developing a patch for it, hiding relevant memory mappings from /proc/pid/maps, hooking libdl.so functions (most importantly dlsym()) to hide the addresses of the interposed symbols by returning the address of the "real" symbols), file/user/process-hiding via shared library function hooking/interposition (primarily libc.so - the C library as a shared object), PAM hooks for /bin/su local privilege escalation (to root; uid=0) and to self-authenticate SSH connections as root (via port-knocking over a random set of ports under a user-defined login name correlating with PAM hooks), on-the-fly creation and destruction of hidden LXC container environments, etc. The general

anti-detection will fool even smart sysadmins and typical detections tools such as rkhunter/chrootkit/etc.

Note that this is not a fork of Jynx2/Azazel/Umbreon or otherwise, as they're, quite frankly, are awful and the developer's know nothing about C.

I know the developers. They're admittedly not good at working at such a low-level and programming in general (at least at the time). Sue me.

I am also developing a fully-weaponised Linux C2 / post-exploitation agent (Listeners, Stagers, Modules, etc.), as there are already many dedicated to Windows (however, I'll incorporate functionality to allow for Windows targets down the track). It will be, as it's name suggests (redacted), very focused on being weaponised while efficiently evading IPS/IDS/AV/etc., incorporating malware-evasive techniques, and tunnelling connections and transactions non-suspiciously in a seemingly-legitimate fashion. It will have some neat features such as in-memory ELF binary execution to prevent touching disk and other types of way of executing native code (perhaps equivalent things to process hollowing and doppleganging on Windows). It has an adjustable beacon interval, which can also be randomised each time to seem like requests are even more legitimate, for each target among other things, so infected clients will check the C2 server every so often for tasks in the queue commanded via HTTP or DNS (typically - to look legit; however, other protocols also exist). TLS for end-to-end encryption so NIDSs and such won't flag packets based on the payload or strange TCP/IP streams in general; e.g., the aggregated payload data of sequenced packets and/or unusual data in the headers of each individually or aggregated [signifying data like magic bytes or configuration of TCP flags to distinguish C2 related traffic from the rest]. It'll be pretty dynamic. For instance, the colour scheme (and theme in general), among other settings, can be overloaded with a YAML config file. Also modules/payloads are grouped and ranked according to things like cleverness, portability, etc. They're listed in an ASCII-drawn table noting those attributes. Just a few things. Not going over everything.

PHP Code

```
<?php
```

```
...
drwxr-xr-x 5 phizo staff 160 4 Feb 10:09 Clever
drwxr-xr-x 4 phizo staff 128 4 Feb 10:09 Common
drwxr-xr-x 3 phizo staff 96 4 Feb 10:09 Common (Easily Identified)
drwxr-xr-x 4 phizo staff 128 4 Feb 10:09 Less Common
...
```

I may even mix this and the rootkit to develop a more powerful C2 where itself and the rootkit are either entirely codependent or, more likely, independent with a compatibility layer in the rootkit that provides an interface (abstracting Local IPC) with which it (the rootkit) and the C2 can interact to combine functionality both automatically (dynamically event-driven and such) as well as in response to defined commands issued through the rootkit's interface to further aid in fulfilling each others' individual purposes (which have a strong overlap on a subset of their given functions).

Both are well into development; I'm not just rambling. In any case, if there are any decent individuals out there, give me a shout.

EDIT: I actually got a PM because someone was interested in the fact I'm acquainted with Prolog. I thought I may as well quote this set theory math challenge I did in Prolog a while back (also incorporated asymptotic computational complexity theory and other math).

(Nov 8, 2016 02:27 PM)Phizo Wrote: [\[CITE\]](#) 2 ez tbh imo etc et al. :\

I decided to solve it mostly using first-order predicate calculus, computationally in Prolog, which I did follow up with some handwork.

Here is an illustration of the program that computes all solutions in $P([0, 5])$, where P is a function which maps a given set into a powerset (the set of all subsets):

PHP Code

```
<?php
```

```
| ?- [n0sya].
```

```
compiling /private/tmp/n0sya.pl for byte code...
```

```
/private/tmp/n0sya.pl compiled, 21 lines read - 3838 bytes written, 6 ms
```

```
(1 ms) yes
```

```
| ?- make_list(0, 5, L), maplist(go, L).
```

```
Reduced powerset: [[0],[]]
```

```
Number of subsets: 2
```

```
Reduced powerset: [[0,1],[1],[],[0]]
```

```
Number of subsets: 4
```

```
Reduced powerset: [[1,2],[2],[],[1],[0],[0,1]]
```

```
Number of subsets: 6
```

```
Reduced powerset: [[2,3],[3],[],[2],[1],[1,2],[0,3],[0],[0,1]]
```

```
Number of subsets: 9
```

```
Reduced powerset: [[3,4],[4],[],[3],[2],[2,3],[1,4],[1],[1,2],[0,3,4],[0,4],[0],[0,3],[0,1,4],[0,1]]
```

```
Number of subsets: 15
```

```
Reduced powerset: [[4,5],[5],[],[4],[3],[3,4],[2,5],[2],[2,3],[1,4,5],[1,5],[1],[1,4],[1,2,5],[1,2],[0,4,5],[0,5],[0],[0,4],[0,3],[0,3,4],[0,1,4,5],[0,1,5],[0,1],[0,1,4]]
```

```
Number of subsets: 25
```

It can solve for:[0, 10] in ~7ms.

[0, 15] in ~179ms

[0, 20] in ~6 seconds

[0, 21] in ~12 seconds

[0, 22] in ~24 seconds

[0, 24] in ~1.9 minutes

[0, 25] in ~3.47 minutes

[0, 26] in ~6.8 minutes

As you may notice, an increment in set cardinality causes an increase in computational time by a factor of ~2.09 on average, which can be represented functionally by $t(f(n+k)) = t(f(n)) \cdot 2.09^k$, where t is a function that measures computational time and $f = \text{go}$ (my top-level Prolog predicate).

That is, the running time is $O(2^n)$ (exponential with a linear exponent), which is fairly inefficient. Note that Prolog (and logic programming in general) is not concerned with runtime efficiency: the declarative paradigm promotes theorem-proving, and consequently program correctness, to programmers and proof procedures, which are often computationally expensive.

As it is such a computationally complex problem, I cannot practically compute the solution for the set [0, 31], as it will take $t(f(31)) \sim t(f(26)) \cdot 2.09^5 = \sim 4.5$ hours.

So, I will compute the rest of the solution by hand. :)

Allow P to represent the powerset and f = go (my top-level Prolog predicate). I analyse f with the intent of finding a pattern such that I can conceptually derive solutions for any x in f(x).

I worked backwards in order to determine a pattern and define the necessary base conditions. I layed out $f(x) = y$ such that $0 \leq x \leq 11$.

Quite clearly, f is akin to the Fibonacci function, but with a seperate rule for odd numbers in its domain.

n is even $\Rightarrow f(n) = f(n-1) + f(n-2)$

n is odd $\Rightarrow f(n) = f(n-1) + f(n-3) + f(n-4)$

Code $f(0) = 2 = f(-1) + f(-1)$

$f(1) = 4 = f(0) + f(-1) + f(-1)$

$f(2) = 6 = f(1) + f(0)$

$f(3) = 9 = f(2) + f(0) + f(-1)$

$f(4) = 15 = f(3) + f(2)$

$f(5) = 25 = f(4) + f(2) + f(1)$

$f(6) = 40 = f(5) + f(4)$

$f(7) = 64 = f(6) + f(4) + f(3)$

$f(8) = 104 = f(7) + f(6)$

$f(9) = 169 = f(8) + f(6) + f(5)$

$f(10) = 273 = f(9) + f(8)$

$f(11) = 441 = f(10) + f(8) + f(7)$

These are the base cases I subsequently defined:

Code $P(\{\}) = \{\{\}\}$

$f(-1) = 1 = |P(\{\})|$

The time has come. What is $f(31)$? A Husaid would never fugg know a thing of this. ./ jaz0r ?

Code $f(31) = f(30) + f(28) + f(27)$

$= [f(29) + f(28)] + [f(27) + f(26)] + [f(26) + f(24) + f(23)]$

$= [f(29) + f(28)] + [f(27) + 602070] + [602070 + 229970 + 142129]$

$= [f(29) + f(28)] + [974169 + 602070] + 974169$

$= [f(29) + 1576239] + 1576239 + 974169$

$= [[f(28) + f(26) + f(25)] + 1576239] + 1576239 + 974169$

$= [[1576239 + 602070 + 372100] + 1576239] + 1576239 + 974169$

$= 6677056$

Hence, $f(31) = 6677056$. That'll be \$10. Cheers and thanks.

Mad76e. - July 16, 2019, 6:01 pm

(Jul 16, 2019 04:19 PM)Phizo Wrote: [\[CITE\]](#) Requirements

No skids, proficiency in at least one area per person (but preferably several areas each) relating to hacking, and a continued curiosity/development in this field. My own experience and knowledge can be observed in my threads and posts. However, I will demonstrate some of my experience below.

.....

Im sorry.. No skids That wont be happening in HF. Those guys that did everything by themselves, programming their own tools etc and hacked the planet are long gone by now, or just not interested to participate in groups. Most of them banned since long due to have been a pain in Omnis hiney. The majority of the guys in HF uses tools who in various ways are written by others, Its simply stupid to re-invent the wheel over and over. If youre looking for specialists you are in the wrong forum. This

forum is full with know-hows, skids, plebs, wannabies and researchers in various degrees. Some are here for the money, some are here for friends, and some to start to learn. HF is "preschool of hacking" not the actual "high school of hacking".

There are no idea to post deep analysis of hacking or do tutorials down to packet level in the analysis because no one will appreciate them, or even comment on them because they dont understand it. It has been done before you know..

Some of us have certs, some have not, but a common rule is that we dont brag about em. I can guarantee that no group in HF will treat you fair if you posts things like this.

Look around in this SF perhaps you find a thread youre interested in

Phizo - July 16, 2019, 8:25 pm

(Jul 16, 2019 06:01 PM)Mad76e. Wrote: [\[CITE\]](#) Im sorry.. No skids That wont be happening in HF. Those guys that did everything by themselves, programming their own tools etc and hacked the planet are long gone by now, or just not interested to participate in groups. Most of them banned since long due to have been a pain in Omnis hiney. The majority of the guys in HF uses tools who in various ways are written by others, Its simply stupid to re-invent the wheel over and over. If youre looking for specialists you are in the wrong forum. This forum is full with know-hows, skids, plebs, wannabies and researchers in various degrees. Some are here for the money, some are here for friends, and some to start to learn. HF is "preschool of hacking" not the actual "high school of hacking".

There are no idea to post deep analysis of hacking or do tutorials down to packet level in the analysis because no one will appreciate them, or even comment on them because they dont understand it. It has been done before you know..

Some of us have certs, some have not, but a common rule is that we dont brag about em. I can guarantee that no group in HF will treat you fair if you posts things like this.

Look around in this SF perhaps you find a thread youre interested in

I've been here since the beginning of 2009; according to your profile, you've been here for a little over a month. Yet you're filling me in on the obvious fact that this forum is full of skids. Obviously, I'm quite aware of that, presumably far more than you. I was in root from the beginning, I knew several people from HTP and was even part of a spin-off group lead by SF. You seem to presume after all these years I was never part of the scene or even this forum. I've watched this forum progress since 2009; and yes, I agree, it's terrible now. It peaked in quality around 2013. This is the #1 skid community. I don't entirely expect an ideal response to be generated from this thread, but it is at least worth a try. Why would I bother browsing the sub-forum where skids are declaring invitations to their lame groups? That is counter-productive. I have a much higher probability of either receiving a decent response from non-skids or receive no worthwhile response at all posting this thread. Chasing skiddie groups via the sub-forum is a waste of my time. As long as it's not a waste of my time, nothing is lost. This is undoubtedly the best way. "I can guarantee that no group on HF will treat you fair if you post things like this." So, I should just ask to join a group without presenting knowledge and experience? Moreover, I mentioned at the beginning this is not about bragging but to not waste the time of myself and anyone else who is not a skid (and believe it or not, there exists a minority of people who are not skids - I've met a few over time). You're not making much sense. Nevertheless, thanks for your input.

imaretard - July 19, 2019, 4:47 pm

This thread is a joke right?

To give an idea regarding the rootkit: it is a highly-dynamic GNU/Linux user-land (ring 3) LD_PRELOAD rootkit written in C (at its core) in the sense that the code will modify itself at both compile-time and run-time (one example being that it will determine hooks and correlating shared objects, macros, etc., and populate its arrays at run-time). It is not publicly available, as it includes functionality not typically found in public rootkits. In addition to the aforementioned, disclosable features include anti-detection/forensics/debugging via reverse engineering of the Linux dynamic linker (ld.so) and developing a patch for it, hiding relevant memory mappings from /proc/pid/maps, hooking libdl.so functions (most importantly dlsym()) to hide the addresses of the interposed symbols by returning the address of the “real” symbols), file/user/process-hiding via shared library function hooking/interposition (primarily libc.so - the C library as a shared object), PAM hooks for /bin/su local privilege escalation (to root; uid=0) and to self-authenticate SSH connections as root (via port-knocking over a random set of ports under a user-defined login name correlating with PAM hooks), on-the-fly creation and destruction of hidden LXC container environments, etc. The general anti-detection will fool even smart sysadmins and typical detections tools such as rkhunter/chrootkit/etc.

Wow! You're so cool, you can sit and develop trivial rootkit software based on an open-source'd kernel. You're brilliant my man. Have you ever considered manipulating the VAD in such a way that you can map kernel memory into ring3 processes ? Therefore effectively hiding your data in memory ? hiding relevant memory mappings from /proc/pid/maps

Assembly (x86/x86-64)

C

C++

Java

Fortran

Lisp

Prolog

Haskell

Ruby

Python

PHP

JavaScript

XML (including XQuery and XPath)

HTML

CSS

You don't know assembly.

I doubt you're any proficient in C++.

You're probably decent at C.

The others are just byproducts of understanding the foundation of classes.

I am also developing a fully-weaponised Linux C2 / post-exploitation agent (Listeners, Stagers, Modules, etc.), as there are already many dedicated to Windows (however, I'll incorporate functionality to allow for Windows targets down the track). It will be, as its name suggests (redacted), very focused on being weaponised while efficiently evading IPS/IDS/AV/etc., incorporating malware-evasive techniques, and tunnelling connections and transactions non-suspiciously in a seemingly-legitimate fashion. It will have some neat features such as in-memory ELF binary execution to prevent touching disk and other types of way of executing native code (perhaps equivalent things to process hollowing and doppelganging on Windows). It has an adjustable beacon interval, which can also be randomised each time to seem like requests are even more legitimate, for each target among other things, so infected clients will check the C2 server every so often for tasks in the queue commanded via HTTP or DNS (typically - to look legit;

however, other protocols also exist). TLS for end-to-end encryption so NIDSs and such won't flag packets based on the payload or strange TCP/IP streams in general; e.g., the aggregated payload data of sequenced packets and/or unusual data in the headers of each individually or aggregated [signifying data like magic bytes or configuration of TCP flags to distinguish C2 related traffic from the rest]. It'll be pretty dynamic. For instance, the colour scheme (and theme in general), among other settings, can be overloaded with a YAML config file. Also modules/payloads are grouped and ranked according to things like cleverness, portability, etc. They're listed in an ASCII-drawn table noting those attributes. Just a few things. Not going over everything.

Sounds like shit. Most linux malware target IoT. These systems have well defined interfaces that allow you to control the device I.E : NETLINK_CONNECTOR without ring0 interference.

Dynamically forking ELF isn't new. As long as you adhere to ELF, fix relocations (alternatively write position independent code), and use ptrace properly then your only issue is allocating memory for the process which can be handled by using an available codecave, or alternatively allocating memory through the kernel.

Terrible idea to use a plaintext C2, researchers will forfeit your C2 pretty quick.

via reverse engineering of the Linux dynamic linker (ld.so) and developing a patch for it, hiding relevant memory mappings from /proc/pid/maps, hooking libdl.so functions (most importantly dlsym() to hide the addresses of the interposed symbols by returning the address of the "real" symbols), file/user/process-hiding via shared library function hooking/interposition (primarily libc.so - the C library as a shared object)

The issue with this is that other malware competing don't rely on any dynamic linker. Your rootkit would be ineffective.

this all all coming from a windows user, and a windows developer.

I have a much higher probability of either receiving a decent response from non-skids or receive no worthwhile response at all posting this thread.
zero.

Tip: The best way to hide memory is through the VAD. No shitty hooks.
Writing a rootkit module for IoT devices is infeasible.

- #1 You have to support numerous kernel versions
- #2 Some devices may not have built in module commands for loading/unloading which requires writing your own
- #3 Some IoT devices are outdated and therefore have minimal memory usage for everything.

VAD description:

Virtual memory is contained in something called a page which has a standard size of 4KB
Allocate non-paged readable writable executable kernel memory for your data.

Attach to the given process you'd like to hide the memory for.

Read the process CR3 which contains the base of the paging structure hierarchy and PCD/PWT flags

Walk the page-map level 4, page-directory pointer table, page directory table and page table to find page table entry

Because the x86/x64 hardware solves page misses by walking CR3 we know the structure is fixed for all OS

These data structures have flags for if they are present (paged in), read/writable, usermode accessible, have write through, cache disabled, accessed, dirty, page size, and execute disabled. So set the usermode accessible flag for them mentioned above.

TLB and paging lookups are refreshed and managed by the hardware. Therefore the OS is independent, this can be applied to Windows, Linux, Mac-OS, etc. Though "VAD" might not exist in Linux operating systems, the concept still applies. In Linux you'd be looking for the virtual memory areas or VMA.

Linux stores a program's memory within the process's memory descriptor. Within this descriptor you will find numerous virtual memory areas, and their associated page tables. Each VMA has a contiguous range of mapped addresses. Each memory segment within a process corresponds to a single VMA. VMAs are represented as linked lists in the mmap field.

When you enumerate a process's memory space through `/proc/{pid}/maps` the kernel will simply access these linked lists and print each, one by one. When a kernel wants to search for a specific memory area within a specific VA it will search through the `mm_rb` field located in the memory descriptor of the process: http://lxr.linux.no/linux+v2.6.28.1/include/linux/mm_types.h#L175

With my design implementation you will be hidden from all instances of enumerating the memory descriptor.

EDIT: @omniscient I believe there's a mybb parsing bug with bb codes, above shown in the URL.

repl0it - July 20, 2019, 2:57 pm

Are you either a grayhat blackhat whitehat

mrpizzahut - July 21, 2019, 7:35 am

It appears you know enough to start your own crew.

cobaltstrike - July 21, 2019, 1:46 pm

Quote: Within the past few years, I have demonstrated fluency in the following programming languages:

- Assembly (x86/x86-64)
- C
- C++
- Java
- Fortran
- Lisp
- Prolog
- Haskell
- Ruby
- Python
- PHP
- JavaScript
- XML (including XQuery and XPath)
- HTML
- CSS

Over the last year, I have demonstrated fluency in none of these languages, but perhaps you are willing to hang out where I talk about dongs and other subjects, some of them may be relevant to security.

Phizo - July 22, 2019, 10:09 pm

Don't mind "imaretard." There's a reason why his account is closed and has -17 rep currently. He's just randomly trashing and talking out his ass to troll random people. His rants are attributed to outdated threads, which he is aware of while bumping them (but won't bump the newer ones due to knowing he's spouting lies as trolls do to compensate for the fact the content is beyond him), a lack of understanding of what I'm talking about, and adhominems.

Natas - July 22, 2019, 10:13 pm

Some times skids are the most fun to hang out with.

Phizo - July 22, 2019, 10:15 pm

(Jul 20, 2019 02:57 PM)repl0it Wrote: [\[CITE\]](#) Are you either a grayhat blackhat whitehat I have quite a few hats. :~)

(Jul 21, 2019 07:35 AM)mrpizzahut Wrote: [\[CITE\]](#) It appears you know enough to start your own crew.

Indeed. I did say in my threads, perhaps more implicitly rather than explicitly, that I'm open to also forming a group.

(Jul 21, 2019 01:46 PM)cobaltstrike Wrote: [\[CITE\]](#) Over the last year, I have demonstrated fluency in none of these languages, but perhaps you are willing to hang out where I talk about dongs and other subjects, some of them may be relevant to security.

That's okay. I don't expect fluency in a bunch of languages. I'm just interested in some cool people who aren't retarded.

I also host a Discord group with friends of many years where we discuss a large variety of topics, including security. This is unrelated to the group siggestion, as they're not currently interested in forming a group.

(Jul 22, 2019 10:13 PM)Natas Wrote: [\[CITE\]](#) Some times skids are the most fun to hang out with. True, but not to form a serious group with.

Natas - July 22, 2019, 10:20 pm

You could always let one or two in and let them grow and shine.

Js every one gots to start out from some where I remember the 2013 days when I was most active we had a HF group chat.

It was bad ass it was like a team of bad asses lol we had some people kinda dumb but some of them were fun af and its cool teaching people man you can bond with your friend like no other teaching them something.

Phizo - July 22, 2019, 10:39 pm

(Jul 22, 2019 10:20 PM)Natas Wrote: [\[CITE\]](#) You could always let one or two in and let them grow and shine.

Js every one gots to start out from some where I remember the 2013 days when I was most active we had a HF group chat.

It was bad ass it was like a team of bad asses lol we had some people kinda dumb but some of them were fun af and its cool teaching people man you can bond with your friend like no other teaching them something.

You're not wrong, and yeah 2013 was definitely the golden-year. Everything was at its peak then. I miss those days. Especially being part of root@hf and all that surrounded it. Shame Starfall left the scene. I was his first friend on HF when he first joined. A great friendship filled with lots of enjoyable times. Also the couple other people around that crowd. Some were over-glorified and actually didn't know shit, though. There was truly perhaps only 3-4 people max who were actually decent (though others didn't know that).

As for teaching people, I get asked for advice on a nearly-daily basis on a wide-range of topics (many Computer Science related topics, various mathematics, (quantum) physics/mechanics, neuroscience/pharmacology/biology, psychology, philosophy, etc.) even without having an active group (aside from my Discord pals). People from all sorts of places who've met me over the years mostly would just use me as a Google. I'm kind of over it now as of the past year (almost) and only do it for good friends now, as I'm often very verbose. Some appreciate that; some interpret it as arrogance, unfortunately.

cobaltstrike - July 23, 2019, 7:36 pm

(Jul 22, 2019 10:15 PM)Phizo Wrote: [\[CITE\]](#) I have quite a few hats. :~)

Indeed. I did say in my threads, perhaps more implicitly rather than explicitly, that I'm open to also forming a group.

That's okay. I don't expect fluency in a bunch of languages. I'm just interested in some cool people who aren't retarded.

I also host a Discord group with friends of many years where we discuss a large variety of topics, including security. This is unrelated to the group suggestion, as they're not currently interested in forming a group.

True, but not to form a serious group with.
shoot over the invite in PMs

Last_viking - July 24, 2019, 3:37 pm

Afaik project insecurity LTD is worth taking part

Cooligan - July 24, 2019, 3:58 pm

(Jul 16, 2019 06:01 PM)Mad76e. Wrote: [\[CITE\]](#) Im sorry.. No skids That wont be happening in HF. Those guys that did everything by themselves, programming their own tools etc and hacked the planet are long gone by now, or just not interested to participate in groups. Most of them banned since long due to have been a pain in Omnis hiney. The majority of the guys in HF uses tools who in various ways are written by others, Its simply stupid to re-invent the wheel over and over. If youre looking for specialists you are in the wrong forum. This forum is full with know-hows, skids, plebs, wannabies and researchers in various degrees. Some are here for the money, some are here for friends, and some to start to learn. HF is "preschool of hacking" not the actual "high school of hacking."

There are no idea to post deep analysis of hacking or do tutorials down to packet level in the analysis because no one will appreciate them, or even comment on them because they dont understand it. It has been done before you know..

Some of us have certs, some have not, but a common rule is that we dont brag about em. I can guarantee that no group in HF will treat you fair if you posts things like this.

Look around in this SF perhaps you find a thread youre interested in
Oh shit, hey Mad!

Haven't seen you in quite some time now, hope all is well for you my man.

I remember all of your wifi hacking books and whatnot too. :p

Mad76e. - July 24, 2019, 5:51 pm

(Jul 24, 2019 03:58 PM)Cooligan Wrote: [\[CITE\]](#) Oh shit, hey Mad!

Haven't seen you in quite some time now, hope all is well for you my man.

I remember all of your wifi hacking books and whatnot too. :p

Yeah, same guy, new account. :)

Nice to see a few still remember ol mad76.

New books om its way :) however still need to write maybe a 100 - 150 pages more, but it has to wait until it gets waay cooler (phun intended)

Aura - July 24, 2019, 5:57 pm

(Jul 24, 2019 05:51 PM)Mad76e. Wrote: [\[CITE\]](#) Yeah, same guy, new account. :)

Nice to see a few still remember ol mad76.

New books om its way :) however still need to write maybe a 100 - 150 pages more, but it has to wait until it gets waay cooler (phun intended)

MAD <3<3<3<3<3

Gary Clark Jr. - July 24, 2019, 6:24 pm

(Jul 24, 2019 05:57 PM)Aura Wrote: [\[CITE\]](#) MAD <3<3<3<3<3
r u a hacker?

Nuworld - July 24, 2019, 6:59 pm

(Jul 24, 2019 06:24 PM)Praise Kek Wrote: [\[CITE\]](#) r u a hacker?

Aura is more than you think.

Be careful.

cobaltstrike - July 24, 2019, 8:13 pm

(Jul 24, 2019 05:51 PM)Mad76e. Wrote: [\[CITE\]](#) Yeah, same guy, new account. :)

Nice to see a few still remember ol mad76.

New books om its way :) however still need to write maybe a 100 - 150 pages more, but it has to wait until it gets waay cooler (phun intended)

why would anyone buy your hacking books when hacking wpa2 is literally capturing a handshake and cracking it? there are FREE github projects that can do everything and probably more

(Jul 24, 2019 06:59 PM)Nuworld Wrote: [\[CITE\]](#) Aura is more than you think.

Be careful.

he's a security consultant based in canada and holds the sans forensics cert

M L T - July 24, 2019, 10:57 pm

(Jul 16, 2019 08:25 PM)Phizo Wrote: [\[CITE\]](#) I knew several people from HTP and was even part of a spin-off group lead by SF. You seem to presume after all these years I was never part of the scene or even this forum.

Julius Kivifagi told me to tell you to suck his shlong. Also aush0k said he's going to rape your sister. Don't shoot the messenger, idk if you even have a sister.

Also hai idk if you even remember me, I believe we used to chat @ stingrayz w/ 0days Skype

Group w/ KMS, K4FR, Starfall, Puremind, etc. I also recall you from wayyyyyy back in some faggy xat h4x0r group, either Incursio ex Subter or Tech Retaliation (s/retaliation/retardation) with the likes of bw0mp and Sora etc, lol..

I'm running a group doing lots of expdev stuff although I doubt you'd wanna join because I was a giant fucking skid-stain last time we actively spoke to eachother.

EDIT: Jesus fuck Omni why the fuck are you editing the word "fu?k"
fu?k fu?k fu?k fu?kity fu?k fu?k, fu?king fu?kers.

Phizo - July 25, 2019, 4:55 am

(Jul 24, 2019 10:57 PM)M L T Wrote: [\[CITE\]](#) Julius Kivifagi told me to tell you to suck his shlong. Also aush0k said he's going to rape your sister.

Don't shoot the messenger, idk if you even have a sister.

Also hai idk if you even remember me, I believe we used to chat @ stingrayz w/ 0days Skype Group w/ KMS, K4FR, Starfall, Puremind, etc. I also recall you from wayyyyyy back in some faggy xat h4x0r group, either Incursio ex Subter or Tech Retaliation (s/retaliation/retardation) with the likes of bw0mp and Sora etc, lol..

I'm running a group doing lots of expdev stuff although I doubt you'd wanna join because I was a giant fugging skid-stain last time we actively spoke to eachother.

EDIT: Jesus fugg Omni why the fugg are you editing the word "fu?k"
fu?k fu?k fu?k fu?kity fu?k fu?k, fu?king fu?kers.

I haven't spoken to that little blonde boy who can't even manage to write simple HTML (check out root's IRC logs - he literally doesn't know how to write an img tag) and asks people to write basic PHP code for him (i.e., me) back in 2013. He can't even determine whether the PHP script I wrote for him back then was secure or not because he's a skid and always has been. Just has a huge ego and trolls. Never seen him or Aush0k do anything but troll, and that's a pretty typical thing he'd say since he knows I don't have a sister rofl.

I was never in leS, I just knew them when I was 12-13. That "affiliation" didn't last long and I wasn't even actively part of the group. They were skids, and back then I was only just beginning. Everyone starts somewhere. Remember the original TeaMP0isoN? K4Fr and I are still tight to this day, very good friends now for years - I know all about those times.

I don't care if you were a skid before. The only thing that matters to me is lack of ego and the ability to evolve. Although, if you still affiliate with the likes of Foolius and Aush0kingly-awful, I'm questioning your offer too.

cobaltstrike - July 25, 2019, 8:38 am

(Jul 25, 2019 04:55 AM)Phizo Wrote: [\[CITE\]](#) I haven't spoken to that little blonde boy who can't even manage to write simple HTML (check out root's IRC logs - he literally doesn't know how to write an img tag) and asks people to write basic PHP code for him (i.e., me) back in 2013. He can't even determine whether the PHP script I wrote for him back then was secure or not because he's a skid and always has been. Just has a huge ego and trolls. Never seen him or Aush0k do anything but troll, and that's a pretty typical thing he'd say since he knows I don't have a sister rofl.

I was never in leS, I just knew them when I was 12-13. That "affiliation" didn't last long and I wasn't even actively part of the group. They were skids, and back then I was only just beginning. Everyone starts somewhere. Remember the original TeaMP0isoN? K4Fr and I are still tight to this day, very good friends now for years - I know all about those times.

I don't care if you were a skid before. The only thing that matters to me is lack of ego and the ability to evolve. Although, if you still affiliate with the likes of Foolius and Aush0kingly-awful, I'm questioning your offer too.

i dont think aurora aka s.t.a.r.f.a.l.l. is still part of the scene tbh

he is now a she btw, not kidding, completely srs

send me a pm with deetz i cant send pms yet

Phizo - July 25, 2019, 9:36 am

(Jul 25, 2019 08:38 AM)cobaltstrike Wrote: [\[CITE\]](#) i dont think aurora aka s.t.a.r.f.a.l.l. is still part of the scene tbh

he is now a she btw, not kidding, completely srs

send me a pm with deetz i cant send pms yet

Yeah, SF hasn't been involved since like 2015 or so. Anyway, it was a while ago.

He's always wanted/acted like a "she." If he finally got that sex-change, good for him.

Elitas - July 25, 2019, 10:19 am

Damn though that's an impressive resume.

Unity was actually a pretty good group when active, had a lot of people in there that were actively doing bug bounties. We identified a lot of bugs in HF as a group too, was overall a lot of fun but unfortunately RaZoR lost his 2fa and the group was sold. Also Crystallize who was the leader got banned.

It was the best "hacker" group I've seen on HF in the past 2-3 years, as it focused a lot on the whitehat scene and was pretty productive. I know there's been a lot of "skiddy" groups but we overall avoided all of that.

tl;dr there is quality on HF still but there's no group which has has an active leadership to run recruitments to actually identify these people. We had some really nice recruitments in Unity. They were easy at first but we started to get more advanced, and we also invited people who were impressive around the forums.

Legends still exists but not really too active. More programming focused than Unity AFAIK so maybe will suit you better idk.

Cooligan - July 25, 2019, 11:57 am

(Jul 24, 2019 05:51 PM)Mad76e. Wrote: [\[CITE\]](#) Yeah, same guy, new account. :)

Nice to see a few still remember ol mad76.

New books om its way :) however still need to write maybe a 100 - 150 pages more, but it has to wait until it gets waay cooler (phun intended)

That's nice to hear man.

Do you still have them for sale on Amazon as well? ?

stupidcntbro - July 25, 2019, 1:03 pm

(Jul 22, 2019 10:09 PM)Phizo Wrote: [\[CITE\]](#) Don't mind "imaretard." There's a reason why his account is closed and has -17 rep currently. He's just randomly trashing and talking out his ass to

troll random people. His rants are attributed to outdated threads, which he is aware of while bumping them (but won't bump the newer ones due to knowing he's spouting lies as trolls do to compensate for the fact the content is beyond him), a lack of understanding of what I'm talking about, and ad hominem.

But.. you're hooking in 2019 to hide memory access
Your new threads still cover trivial concepts.

not even sure why im wasting my time replying to this thread, other than the fact that you seem to equate understanding of primitive concepts with "hacking". Your threads haven't shown any ability to analyze a system and exploit vulnerabilities. The capacity to which you can hack (from observing) is at most "SQLi" and other trivial web app attack vectors.

Your explanation of developing a multi-staged linux bot, despite receiving criticism on your design, shows your rudimentary understanding of general malware development.

I've outlined the flaws with your design.

I've also outlined how you portray yourself online: IE. Explain CRC32 to some skid, show off a "PRNG". I get it, you learned these concepts in class, studied them, and were tested on them. LCG's and primitive cyclic redundancy checks are common knowledge for CS graduates. What differentiates an excellent developer from a mediocre one is not through regurgitation of standards, but it's through analysis and design. You've shown no ability to test and maintain any type of system.

It would be sufficient for someone like yourself to post actual work.

Also your prolog solution approach is similar to that of the extended euclidean algorithm (or Fibonacci)... have you tried projecteuler.net? I've solved fairly difficult problems that I can attest that even PhD's had trouble solving. Your prolog example demonstrates your ability to solve problems, and apply your knowledge effectively. But, no hacker group wants someone that's inexperienced with specific concepts. You do tend to over exaggerate your previous work, and experience. "I've written a shell that bypassed.." means nothing, as it's trivial to anyone such as myself.

Talk to me when you've written a full bypass for a multi billion dollar companies' proprietary rootkit that resulted in multiple law suits for "john doe".

Any real hacking group, or crew, would see your exaggeration and ignore you.
the proper process is to show code, and show work.

There are many mathematicians I know of, with PhDs that would obliterate anyone here when it comes to number theory, set theory, anything of that sort.. but they're complete nuisances when it comes to computer security.

Note: that you have shown NO proof in relation to low-level exploit development, reverse engineering, and computer system architecture fundamentals. I won't ridicule you for misunderstanding calling conventions back in 2013, but at this point in time you should demonstrate some proof of ability based on your experiences.

So let's end it off with, this thread is a joke, right?

SUKMYD - July 25, 2019, 2:05 pm

Lol imagine flexing a php shell and some shitty prolog code

Mad76e. - July 25, 2019, 2:45 pm

(Jul 24, 2019 05:57 PM)Aura Wrote: [\[CITE\]](#) MAD <3<3<3<3<3Long time no see.. I hear things going just good for you.. Thats nice :) You deserve it!

(Jul 25, 2019 11:57 AM)Cooligan Wrote: [\[CITE\]](#) That's nice to hear man.

Do you still have them for sale on Amazon as well? ?Everywhere, even on google books Just follow my link in the sig, copy the ISBN and use it in any bookshop irl to order :p

(Jul 24, 2019 08:13 PM)cobaltstrike Wrote: [\[CITE\]](#) why would anyone buy your hacking books when hacking wpa2 is literally capturing a handshake and cracking it? there are FREE github projects that can do everything and probably more

My paycheck says the differ. I see my books more as a studying books then claiming to have new content, most of it is public. its not JUST "capturing a handshake" kinda book. How on earth do you think i manage to write 86 pages about "one thing" that you could fit in an small piece of paper?

And a small note. I do not like automated shit scripts thats depended on the aircrack-ng suite running in the background

M L T - July 25, 2019, 2:52 pm

(Jul 25, 2019 04:55 AM)Phizo Wrote: [\[CITE\]](#) I haven't spoken to that little blonde boy who can't even manage to write simple HTML (check out root's IRC logs - he literally doesn't know how to write an img tag) and asks people to write basic PHP code for him (i.e., me) back in 2013. He can't even determine whether the PHP script I wrote for him back then was secure or not because he's a skid and always has been. Just has a huge ego and trolls. Never seen him or Aush0k do anything but troll, and that's a pretty typical thing he'd say since he knows I don't have a sister rofl.

I was never in leS, I just knew them when I was 12-13. That "affiliation" didn't last long and I wasn't even actively part of the group. They were skids, and back then I was only just beginning. Everyone starts somewhere. Remember the original TeaMP0isoN? K4Fr and I are still tight to this day, very good friends now for years - I know all about those times.

I don't care if you were a skid before. The only thing that matters to me is lack of ego and the ability to evolve. Although, if you still affiliate with the likes of Foolius and Aush0kingly-awful, I'm questioning your offer too.

Imao aush0k hates me, I just happen to be in a group DM with him. And yes I'm fully aware of zeekill's lack of talent, the only half-impressive things I've seen him do were some DNS hijackings as a result of Starfall handing him access to WebNIC.. even then that's him getting handed access to something though. By root I assume you're talking about Blair? and yeah, I just remember when I first got into "hacking" on xat.com I saw you around leS... of course they were a skid group. I wasn't tryna meme you or anything by bringing them up, just sayin' that's where I first ever remember seeing yhou around.

What do you mean by the "original TeaMp0isoN" ? as in, the forums? Also, K4 is still around? I haven't seen him in years.

Anyway I can assure you the likes of aush0k or Julius aren't in my group, here's some examples of our recent work:

https://www.theregister.co.uk/2018/08/07/openemr_vulnerabilities/

<https://www.hackread.com/live-chat-widgets-leaking-details-of-employees/>

<https://threatpost.com/canadian-telcos-patch-an-apt-ready-flaw-in-disability-services/136704/>

<https://www.zdnet.com/article/mobile-giant-left-code-system-online-default-password/>

Mainly we're auditing webapps withiin the EDU and Medical Sectors, lately getting into some SCADA/ICS/PLC stuff too. We primarily do webapp exploitation, although we are doing some lower-level projects too. We're currently trying to exploit a TOC/TOU race condition bug in a popular linux app pre-packaged w/ most distros but having a little trouble exploiting it efficiently.. Sitting on a

few nice 0day's to drop too, several forum software (current versions), some large wordpres/joomla/drupal plugins, a popular IRC client, and several bugs for electron which are affecting Discord/Slack/Skype/etc

if you do decide you want to help out then I'm happy to have you on board, if not though that's fine. Maybe you could chat with the members in our private IRC channel and determine for yourself whether you think they're skids or not :P I assure you its nobody similar to the likes of julius or aush0k though.

Phizo - July 26, 2019, 9:29 am

(Jul 25, 2019 02:52 PM)M L T Wrote: [\[CITE\]](#) lmao aush0k hates me, I just happen to be in a group DM with him. And yes I'm fully aware of zeekill's lack of talent, the only half-impressive things I've seen him do were some DNS hijackings as a result of Starfall handing him access to WebNIC.. even then that's him getting handed access to something though. By root I assume you're talking about Blair? and yeah, I just remember when I first got into "hacking" on xat.com I saw you around leS... of course they were a skid group. I wasn't tryna meme you or anything by bringing them up, just sayin' that's where I first ever remember seeing yhou around.

What do you mean by the "original TeaMp0isoN" ? as in, the forums? Also, K4 is still around? I haven't seen him in years.

Anyway I can assure you the likes of aush0k or Julius aren't in my group, here's some examples of our recent work:

https://www.theregister.co.uk/2018/08/07/openemr_vulnerabilities/
<https://www.hackread.com/live-chat-widgets-leaking-details-of-employees/>
<https://threatpost.com/canadian-telcos-patch-an-apt-ready-flaw-in-disability-services/136704/>
<https://www.zdnet.com/article/mobile-giant-left-code-system-online-default-password/>

Mainly we're auditing webapps withiin the EDU and Medical Sectors, lately getting into some SCADA/ICS/PLC stuff too. We primarily do webapp exploitation, although we are doing some lower-level projects too. We're currently trying to exploit a TOC/TOU race condition bug in a popular linux app pre-packaged w/ most distros but having a little trouble exploiting it efficiently.. Sitting on a few nice 0day's to drop too, several forum software (current versions), some large wordpres/joomla/drupal plugins, a popular IRC client, and several bugs for electron which are affecting Discord/Slack/Skype/etc

if you do decide you want to help out then I'm happy to have you on board, if not though that's fine. Maybe you could chat with the members in our private IRC channel and determine for yourself whether you think they're skids or not :P I assure you its nobody similar to the likes of julius or aush0k though.

Rofl the DNS hijacking that was handed to him on a silver-platter is how he "earned" his Black Hat award. Cute. Starfall was good, don't know why he hang around and help that tool work up a reputation as the best hacker on HF (seriously - I don't think you were active, or were under a different name at the time). When I said the "original TeaMp0isoN," he told me some stuff that happened those days a long time ago. I wasn't aware he was in TP (under another alias at the time), but he did say "we" (TP) were essentially just another skid group. As you say, don't shoot the messenger. That's why I found it a bit ironic to bring up leS and such (even though they were skids). Of course, I'm not saying TP is that way now. I wouldn't know. This was a while ago. K4 is not doing computer-related stuff, and hasn't in a couple years now, but we still chat. As I mentioned before, we've met up, etc., so we're essentially IRL friends too rather than just Internet buddies. Shame, though, as he's got a lot of potential.

Definitely sounds more intriguing than anything else I'll find on this forum. I pretty much came back on here after a while of continual on-and-off inactivity just to look for or start a crew. I wouldn't mind

checking it out (and most likely jumping on-board). I will note that my workload is pretty hectic, but the difference in timezones will probably even some of that out. In any case, I don't think you'll be disappointed having me around. I doubt this thread would've went anywhere when I started writing it, so I appreciate the invite. I have some of my own "goals/work" that could be done alone, of course, but it's always good to have some decent people you can work with to align like-minded efforts, etc.

Out of curiosity, are you still calling the crew TP? That's not a deciding factor by any means - just pure curiosity. Understandably, there's things that are better discussed without big-brother watching. EDIT: Ah, I suppose that would be "Project Insecurity LTD." Also, by "root," I meant the group root@hf lead by Starfall. You weren't around at the time (at least under your "true" handle). It was an official HF group and no doubt the best hacking-related group that ever came to HF. The IRC logs were leaked and are public.

bastar - July 26, 2019, 10:13 pm

(Jul 16, 2019 04:19 PM)Phizo Wrote: [\[CITE\]](#) Note that this is not a fork of [crap rootkit]/[crap rootkit]/Umbreon or otherwise, as they're, quite frankly, are awful and the developer's know nothing about C.

I know the developers. They're admittedly not good at working at such a low-level and programming in general (at least at the time).

I could assume you either haven't seen the code for the latest version of Umbreon or don't actually know who developed it; because of who you are, I'm sure it isn't the latter. Claiming to be more knowledgeable than that person, of ALL people you could've referenced instead, doesn't seem like the right way to go about a thread that "isn't about bragging". I'm not looking for trouble, but out of every topic you could've claimed to know more about than him like PHP or something which you could actually defend, you chose C and low-level development/exploitation? WHAT?

Also, he certainly isn't gone from the scene. I talked to him very recently, he still does some black/gray hat development. I don't blame him for halting communication with most of the people he was in contact with though.

Other than that small criticism, I like this thread. I really wish you would've posted this 5 years ago when I was still interested in things like this, I used to read your posts all the time and would've loved to work with you.

Phizo - July 27, 2019, 2:08 am

(Jul 26, 2019 10:13 PM)bastar Wrote: [\[CITE\]](#) I could assume you either haven't seen the code for the latest version of Umbreon or don't actually know who developed it; because of who you are, I'm sure it isn't the latter. Claiming to be more knowledgeable than that person, of ALL people you could've referenced instead, doesn't seem like the right way to go about a thread that "isn't about bragging". I'm not looking for trouble, but out of every topic you could've claimed to know more about than him like PHP or something which you could actually defend, you chose C and low-level development/exploitation? WHAT?

Also, he certainly isn't gone from the scene. I talked to him very recently, he still does some black/gray hat development. I don't blame him for halting communication with most of the people he was in contact with though.

Other than that small criticism, I like this thread. I really wish you would've posted this 5 years ago when I was still interested in things like this, I used to read your posts all the time and would've loved to work with you.

Perhaps not the latest version if it's been revised over the past couple years. It's not an "old" version, though. I need to double-check which version I have, as I do not have it on this box. Yes, I

know who developed it. I stand by what I said. I can point out a bunch of problems which demonstrate lack of C/rootkit knowledge. I'm not trying to bash, I'm just being honest. I am more fluent in C/C++ than perhaps any other language, and I'm fluent in quite a lot, so I would argue that I do know more considering at the time "that person" confessed to me that he did not know any low-level exploitation and only knew pretty rudimentary C over Skype at the time. I'm not saying that person isn't good; in fact, I mentioned in this thread that that person was one of the few who was actually good in general (as a hacker). I have nothing but respect and love for that person. I'm just going off facts here. Everyone (with potential) improves, though, so I never meant to imply my old friend never improved or lacked the ability to. Quite the contrary.

Yeah, I wasn't really interested in getting into a group back then. Over the past couple years, though, I have pondered it. The trouble is finding a good group/people.

Reading e-zines definitely brought on motivation. I also enjoyed reading the zines attributed to the group that person was involved with (or founded, rather, IIRC).

Thanks for your feedback, though. Appreciated. Glad you at least enjoyed the read. I'm also happy to hear he hasn't completely left the scene, as that would've been a waste.

cobaltstrike - July 27, 2019, 10:50 am

(Jul 27, 2019 02:08 AM)Phizo Wrote: [\[CITE\]](#) Perhaps not the latest version if it's been revised over the past couple years. It's not an "old" version, though. I need to double-check which version I have, as I do not have it on this box. Yes, I know who developed it. I stand by what I said. I can point out a bunch of problems which demonstrate lack of C/rootkit knowledge. I'm not trying to bash, I'm just being honest. I am more fluent in C/C++ than perhaps any other language, and I'm fluent in quite a lot, so I would argue that I do know more considering at the time "that person" confessed to me that he did not know any low-level exploitation and only knew pretty rudimentary C over Skype at the time. I'm not saying that person isn't good; in fact, I mentioned in this thread that that person was one of the few who was actually good in general (as a hacker). I have nothing but respect and love for that person. I'm just going off facts here. Everyone (with potential) improves, though, so I never meant to imply my old friend never improved or lacked the ability to. Quite the contrary.

Yeah, I wasn't really interested in getting into a group back then. Over the past couple years, though, I have pondered it. The trouble is finding a good group/people.

Reading e-zines definitely brought on motivation. I also enjoyed reading the zines attributed to the group that person was involved with (or founded, rather, IIRC).

Thanks for your feedback, though. Appreciated. Glad you at least enjoyed the read. I'm also happy to hear he hasn't completely left the scene, as that would've been a waste.
htp zines lit af

Cooligan - July 28, 2019, 5:42 am

(Jul 25, 2019 02:45 PM)Mad76e. Wrote: [\[CITE\]](#) Long time no see.. I hear things going just good for you.. Thats nice :) You deserve it!

Everywhere, even on google books Just follow my link in the sig, copy the ISBN and use it in any bookshop irl to order :p

That's too fucking awesome man haha. I'd imagine you've sold quite a few copies by now.

And lol I can just imagine asking the person working at the book store, "yeah I need this wifi hacking book" ?

bastar - July 28, 2019, 8:57 am

(Jul 27, 2019 02:08 AM)Phizo Wrote: [\[CITE\]](#) Yeah, I wasn't really interested in getting into a group

back then. Over the past couple years, though, I have pondered it. The trouble is finding a good group/people.

Reading e-zines definitely brought on motivation. I also enjoyed reading the zines attributed to the group that person was involved with (or founded, rather, IIRC).

Knowing that your motivation for wanting to be in a group is the same as mine was a few years ago is even more mind blowing. Reading e-zines was probably one of my favorite past times, but at the time I faced the same problem as you - couldn't find good people or a good group. Dyme and I tried starting a group but it was fucking pathetic, all we could find was "here to learn" kiddies. Not that there's anything wrong with them, but they're obviously not the people you want in a serious group. I can only assume it has gotten worse, considering the infestation of dox/swat monkeys never died down and probably never will die down.

If only I hadn't already quit my information security job and changed my major from computer science, we could've formed a group ?

M L T - July 28, 2019, 9:22 am

(Jul 26, 2019 09:29 AM)Phizo Wrote: [\[CITE\]](#) Rofl the DNS hijacking that was handed to him on a silver-platter is how he "earned" his Black Hat award. Cute. Starfall was good, don't know why he hang around and help that tool work up a reputation as the best hacker on HF (seriously - I don't think you were active, or were under a different name at the time). When I said the "original TeaMp0isoN," he told me some stuff that happened those days a long time ago. I wasn't aware he was in TP (under another alias at the time), but he did say "we" (TP) were essentially just another skid group. As you say, don't shoot the messenger. That's why I found it a bit ironic to bring up leS and such (even though they were skids). Of course, I'm not saying TP is that way now. I wouldn't know. This was a while ago. K4 is not doing computer-related stuff, and hasn't in a couple years now, but we still chat. As I mentioned before, we've met up, etc., so we're essentially IRL friends too rather than just Internet buddies. Shame, though, as he's got a lot of potential.

Definitely sounds more intriguing than anything else I'll find on this forum. I pretty much came back on here after a while of continual on-and-off inactivity just to look for or start a crew. I wouldn't mind checking it out (and most likely jumping on-board). I will note that my workload is pretty hectic, but the difference in timezones will probably even some of that out. In any case, I don't think you'll be disappointed having me around. I doubt this thread would've went anywhere when I started writing it, so I appreciate the invite. I have some of my own "goals/work" that could be done alone, of course, but it's always good to have some decent people you can work with to align like-minded efforts, etc.

Out of curiosity, are you still calling the crew TP? That's not a deciding factor by any means - just pure curiosity. Understandably, there's things that are better discussed without big-brother watching. EDIT: Ah, I suppose that would be "Project Insecurity LTD." Also, by "root," I meant the group root@hf lead by Starfall. You weren't around at the time (at least under your "true" handle). It was an official HF group and no doubt the best hacking-related group that ever came to HF. The IRC logs were leaked and are public.

teampoison has been dead for years, K4 was a member but under a different alias, yes it was a skid group. I was around for root@hf, I wasn't very active on these forums (although I did lurk under another account) but I was somewhat active in #root@hf at tsukihi/helldive/nekoarcnetwork whatever that IRC network is called these days.. cool to hear K4 is still around. Been a long while.

Phizo - July 28, 2019, 10:06 am

(Jul 28, 2019 08:57 AM)bastar Wrote: [\[CITE\]](#) Knowing that your motivation for wanting to be in a group is the same as mine was a few years ago is even more mind blowing. Reading e-zines was probably one of my favorite past times, but at the time I faced the same problem as you - couldn't find good people or a good group. Dyme and I tried starting a group but it was fugging pathetic, all

we could find was "here to learn" kiddies. Not that there's anything wrong with them, but they're obviously not the people you want in a serious group. I can only assume it has gotten worse, considering the infestation of dox/swat monkeys never died down and probably never will die down.

If only I hadn't already quit my information security job and changed my major from computer science, we could've formed a group ?

I mean, I have pondered it for some time (over the past few years as well). Mind-blowing in what regard exactly? I've read e-zines over several years, but yeah, reflecting upon their content and re-reading on very rare occasions (in more recent times) is always motivational in terms of wanting to be a part of a decent crew with decent people and working towards common, interesting goals. As someone who enjoys being expressive in my typing, especially when it comes to explaining and teaching interesting topics and enquiries, I would even still be interested in participating in the development of e-zines with respect to the group. I've always been interested in their development and considered doing write-ups like GNY (Go Null Yourself) did but solo since I had no decent connections to decent groups (and the couple I did have never invited me, though I didn't ask either, so I just expected they weren't interested enough), as GNY would cover things like number theoretic concepts, cryptography, set and graph theory, and other discrete mathematics topics while also having some relevance to security/hacking, programming, and so on.

I may know which group you're referring to if it had a Discord group a few years ago, which MLT was in also. If not, then perhaps I don't know of it.

Would you be willing to fill me in over PM, as well as the handle I know you by, if you're willing (I assure you it'll stay with me).

You don't have to have to a degree in computer science as a prerequisite for me to want to join/form a group, but it's definitely preferable. I'm just looking for people who know what they're doing / aren't skids and can demonstrate this. If you do well in computer science (and the uni and their syllabuses/curriculum are decent), the difference in knowledge/experience is shocking. I was not bad prior, but 2/3's into (and especially final year and post-graduation) computer science and majoring in security excelled me in ways I doubt I would've been able to achieve otherwise. I would've missed out on a lot. Anyway, my initial and main point was that I don't mind you've quit your infosec job and moved away from computer science. If you're still good, or semi-good with the potential to excel, I'd still be open to exploring something if interests align and we can get some other trustworthy people who are skilled along board.

(Jul 28, 2019 09:22 AM)M L T Wrote: [\[CITE\]](#) teampoison has been dead for years, K4 was a member but under a different alias, yes it was a skid group. I was around for root@hf, I wasn't very active on these forums (although I did lurk under another account) but I was somewhat active in #root@hf at tsukihi/helldive/nekoarcnetwork whatever that IRC network is called these days.. cool to hear K4 is still around. Been a long while.

I know; I mentioned that in another post: "I wasn't aware he was in TP (under another alias at the time)."

I gather from your reply your mind has changed? Let me know so I can take-up other offers if that's the case.

MLT - July 28, 2019, 10:16 am

(Jul 28, 2019 10:06 AM)Phizo Wrote: [\[CITE\]](#) I know; I mentioned that in another post: "I wasn't aware he was in TP (under another alias at the time)."

I gather from your reply your mind has changed? Let me know so I can take-up other offers if that's the case.

Nope, my mind hasn't changed. If you wanna join there's always a spot for you.

bastar - July 28, 2019, 11:04 am

(Jul 28, 2019 10:06 AM)Phizo Wrote: [\[CITE\]](#) I mean, I have pondered it for some time (over the past

few years as well). Mind-blowing in what regard exactly? I've read e-zines over several years, but yeah, reflecting upon their content and re-reading on very rare occasions (in more recent times) is always motivational in terms of wanting to be a part of a decent crew with decent people and working towards common, interesting goals. As someone who enjoys being expressive in my typing, especially when it comes to explaining and teaching interesting topics and enquiries, I would even still be interested in participating in the development of e-zines with respect to the group. I've always been interested in their development and considered doing write-ups like GNY (Go Null Yourself) did but solo since I had no decent connections to decent groups (and the couple I did have never invited me, though I didn't ask either, so I just expected they weren't interested enough), as GNY would cover things like number theoretic concepts, cryptography, set and graph theory, and other discrete mathematics topics while also having some relevance to security/hacking, programming, and so on.

I may know which group you're referring to if it had a Discord group a few years ago, which MLT was in also. If not, then perhaps I don't know of it.

Would you be willing to fill me in over PM, as well as the handle I know you by, if you're willing (I assure you it'll stay with me).

You don't have to have to a degree in computer science as a prerequisite for me to want to join/form a group, but it's definitely preferable. I'm just looking for people who know what they're doing / aren't skids and can demonstrate this. If you do well in computer science (and the uni and their syllabuses/curriculum are decent), the difference in knowledge/experience is shocking. I was not bad prior, but 2/3's into (and especially final year and post-graduation) computer science and majoring in security excelled me in ways I doubt I would've been able to achieve otherwise. I would've missed out on a lot. Anyway, my initial and main point was that I don't mind you've quit your infosec job and moved away from computer science. If you're still good, or semi-good with the potential to excel, I'd still be open to exploring something if interests align and we can get some other trustworthy people who are skilled along board.

I'd be more than willing to, I can't PM you though since I only have 5 posts. If you PM me with whatever communication medium you prefer I'd love to chatter with you about all of that stuff.

Phizo - July 28, 2019, 12:01 pm

(Jul 28, 2019 10:16 AM)M L T Wrote: [CITE](#) Nope, my mind hasn't changed. If you wanna join there's always a spot for you.

I thought the following was an explicit acceptance to your invitation. The effort behind your posts appeared contrasted to earlier, but perhaps you're busy and/or just skim-read it, which gave me an the impression your desire has changed. You seemed fairly keen on getting me on-board originally.

Quote: Definitely sounds more intriguing than anything else I'll find on this forum. I pretty much came back on here after a while of continual on-and-off inactivity just to look for or start a crew. I wouldn't mind checking it out (and most likely jumping on-board). I will note that my workload is pretty hectic, but the difference in timezones will probably even some of that out. In any case, I don't think you'll be disappointed having me around. I doubt this thread would've went anywhere when I started writing it, so I appreciate the invite. I have some of my own "goals/work" that could be done alone, of course, but it's always good to have some decent people you can work with to align like-minded efforts, etc.

In any case, feel free to forward me however much detail you trust me with at this stage or whatever and we can go from there. Unless you've got something else in mind.

Preferably, I'd like to know as much as possible (the more you intrigue me, the more I'll become increasingly excited and dedicated to improving the group all-around and being more involved (also depending on my level of access/privs and role, of course, presuming any sort of hierarchy). I would be interested in increasing and hardening our operational infrastructure also where necessary in addition to typical expectations. I need to learn a bit more about the group in general anyway (how it operates, its infrastructure, flexibility/diversity in operations and if these can be coordinated between

members, what goals we would like to achieve (essentially a vision statement would be cool), etc.). I know you primarily focus on web-apps currently (or indefinitely) with some working on some other areas. I would be interested in seeing this grow further and being able to facilitate in that if both ends are happy with getting acquainted with one another.

M L T - July 28, 2019, 1:05 pm

(Jul 28, 2019 12:01 PM)Phizo Wrote: [\[CITE\]](#) I thought the following was an explicit acceptance to your invitation. The effort behind your posts appeared contrasted to earlier, but perhaps you're busy and/or just skim-read it, which gave me an the impression your desire has changed. You seemed fairly keen on getting me on-board originally.

I'm absolutely keen for you to join, I did initially just skim-read it hence my response... I've sent you a PM with more info and an invite to our IRC to discuss things further. I didn't realize you'd pretty much stated you were down to join until I went back and re-read your post.. I was just guilty of skimming over it, apologies for any miscommunication lol... but yeah we'd love to have you on board.

Venture - July 28, 2019, 7:22 pm

I'm no heavy hitter, but I'm very affluent with Social Engineering, and OSINT. However my coding skills are weak as I work with HTML, CSS, a bit of PHP. and the only programming language I bothered to dabble in are Visual C#, and Visual Basic.

I'm probably no where near qualified but fuck it.

Viktory - August 6, 2019, 4:34 am

Whats a good hacker?

I once into a bar and
free tex mex burger

Tyler777 - August 9, 2019, 2:00 am

The group I lead would be more than happy to accept you into our circle your knowledge and experience would greatly benefit the group and our members. I am going to add you to the group. We are currently reforming and refocusing and would love to hear your input.

Phizo - August 12, 2019, 7:36 pm

So, I've had quite a lot of offers, three of which seemed worthwhile. One PM'd me twice and then dropped off after my second reply (hasn't responded for a while despite being online/active), another hit me up on XMPP but haven't heard anything since, the other being on-site and the only one I've taken up: Sui Generis (cheers Tyler).

Due to this, I may just spin something up of my own off-site (while still being a part of Sui Generis). PM me if you meet the requirements. I'd appreciate it if you don't PM me otherwise, as I do not want my time wasted. A degree in Computer Science or equivalent would be much preferred (I'm going to add this to the OP). If you cheated your way through university, and can't prove yourself, again: please don't waste my time.

R0gu3L1nux - August 14, 2019, 7:37 pm

Hello, so I am new to all of this. I am currently hard at work self studying as well as starting back into school to work on my degree. I do not meet the requirements, obviously, but would just like to follow this Sub Forum for when I do or be able to discuss and learn things from the actual pros. Reading books is not very fun all of the time and there are alot of rip-off learning centers online. I do not want to be a "Skid", that is why I am hard at work trying to learn what I can.

Thanks,

--

jadie - August 15, 2019, 5:18 am

(Aug 12, 2019 07:36 PM)Phizo Wrote: [\[CITE\]](#) So, I've had quite a lot of offers, three of which seemed worthwhile. One PM'd me twice and then dropped off after my second reply (hasn't responded for a while despite being online/active), another hit me up on XMPP but haven't heard anything since, the other being on-site and the only one I've taken up: Sui Generis (cheers Tyler).

Due to this, I may just spin something up of my own off-site (while still being a part of Sui Generis). PM me if you meet the requirements. I'd appreciate it if you don't PM me otherwise, as I do not want my time wasted. A degree in Computer Science or equivalent would be much preferred (I'm going to add this to the OP). If you cheated your way through university, and can't prove yourself, again: please don't waste my time.

Oh man, just call me if you ever just want to discuss the weather ?

JaGLY - August 15, 2019, 9:23 am

Not that i am experienced enough yet to take part in your new plans, posting here for later!

Good luck my man ?

Mad76e - August 15, 2019, 10:36 am

(Jul 16, 2019 04:19 PM)Phizo Wrote: [\[CITE\]](#) EDIT:

So, I've had quite a lot of offers, three of which seemed worthwhile. One PM'd me twice and then dropped off after my second reply (hasn't responded for a while despite being online/active), another hit me up on XMPP but haven't heard anything since, the other being on-site and the only one I've taken up: Sui Generis (cheers Tyler).

You proved me wrong it seems. Welcome to Sui Generis

POLY MATH - August 16, 2019, 8:13 pm

I'd be interested in joining depending on the groups focus.

Phizo - October 10, 2019, 3:20 pm

(Aug 16, 2019 08:13 PM)POLY MATH Wrote: [\[CITE\]](#) I'd be interested in joining depending on the groups focus.

This is to anyone who is interested and meet the requirements.

I imagine something essentially along the lines of either/both:

(Dark-)grey hat activities involving acquiring resources such as root access to a variety of systems as we see fit (combined or individually for our own purposes but as an aggregated set of resources we can share with one another and utilise for future goals as a group and personally [within reason]) - which we would likely obtain by collecting a variety of 0days after auditing code (already done this in the past - not hard) and keeping hold of them with the rootkit I've been developing (which, as mentioned, would be hooked by the C2 I am also developing); essentially, APT-style attacks to acquire mass resources for our use (not talking fraud or carding - more like setting up a network that can do what we want it to; just one example for a subset of devices and usage being the cracking of hashes by creating a P2P overlay network which will crack hashes using GPUs of some owned servers by utilising the OpenCL library for cross-compatible GPU usage). On top of stuff like that, perhaps getting more involved in the scene (and perhaps wiping out the skids who play hacker), develop some e-zines, etc. If one of us has a goal, we can help each other achieve it. If you don't scratch each others' backs, you're not a team player.

Less-dark activities but still similarities. I'm too tired right now to write them out, but let's say more along the lines of security research (including the discovery of 0days, etc., releasing them similarly

to an Anti-Sec movement or even just to vendors themselves). Essentially, a more legal version of the above. Developing open-source hacking tools (i.e., FOSS philosophy), e-zines dedicated more to the teaching (see GNY [Go Null Yourself] for examples: their e-zines teach very interesting stuff related to discrete mathematics, advanced cryptography and general security/hacking - we can still do this with darker hats, though, and I don't mind that idea.).

(Implicitly for both: setup a secure means of communication for us all; I want a cool set of individuals I can both chill with and hack.)

Personally, I'm for the above or a mixture. Though, I'm still happy with a more whiter hat in general. For the most part, I just want a crew of cool people to chill with and hack with who actually know what they're doing.

I wrote this on no sleep because I had a small draft and wanted to just get this out. I'll probably touch it up better and put it in the thread depending on things.

I don't expect 24/7 active participants, but I do expect reasonable levels of contribution. Like most adults who contribute to society, I have a life too. :)

I may spin-up my own crew, set-up a recruitment, etc., if this goes nowhere.

Tommy Springman - November 1, 2019, 6:32 pm

(Oct 10, 2019 03:20 PM)Phizo Wrote: [CITE](#) This is to anyone who is interested and meet the requirements.

I imagine something essentially along the lines of either/both:

(Dark-)grey hat activities involving acquiring resources such as root access to a variety of systems as we see fit (combined or individually for our own purposes but as an aggregated set of resources we can share with one another and utilise for future goals as a group and personally [within reason]) - which we would likely obtain by collecting a variety of 0days after auditing code (already done this in the past - not hard) and keeping hold of them with the rootkit I've been developing (which, as mentioned, would be hooked by the C2 I am also developing); essentially, APT-style attacks to acquire mass resources for our use (not talking fraud or carding - more like setting up a network that can do what we want it to; just one example for a subset of devices and usage being the cracking of hashes by creating a P2P overlay network which will crack hashes using GPUs of some owned servers by utilising the OpenCL library for cross-compatible GPU usage). On top of stuff like that, perhaps getting more involved in the scene (and perhaps wiping out the skids who play hacker), develop some e-zines, etc. If one of us has a goal, we can help each other achieve it. If you don't scratch each others' backs, you're not a team player.

Less-dark activities but still similarities. I'm too tired right now to write them out, but let's say more along the lines of security research (including the discovery of 0days, etc., releasing them similarly to an Anti-Sec movement or even just to vendors themselves). Essentially, a more legal version of the above. Developing open-source hacking tools (i.e., FOSS philosophy), e-zines dedicated more to the teaching (see GNY [Go Null Yourself] for examples: their e-zines teach very interesting stuff related to discrete mathematics, advanced cryptography and general security/hacking - we can still do this with darker hats, though, and I don't mind that idea.).

(Implicitly for both: setup a secure means of communication for us all; I want a cool set of individuals I can both chill with and hack.)

Personally, I'm for the above or a mixture. Though, I'm still happy with a more whiter hat in general. For the most part, I just want a crew of cool people to chill with and hack with who actually know what they're doing.

I wrote this on no sleep because I had a small draft and wanted to just get this out. I'll probably touch it up better and put it in the thread depending on things.

I don't expect 24/7 active participants, but I do expect reasonable levels of contribution. Like most adults who contribute to society, I have a life too. :)

I may spin-up my own crew, set-up a recruitment, etc., if this goes nowhere.

Sorry to burst your bubble but the era of hacking for the sake of hacking is long gone. Everyone from that scene grew up and moved on with their lives. It's all about money now. Good luck finding talent that's willing to commit crimes for little to no financial return.

K4Fr - September 17, 2020, 4:13 am

Helo I will join this group you speak of.

Cooligan - September 17, 2020, 5:08 am

This is the first hacking oriented group I've seen in a very long time that could actually be promising.

Hope something nice comes out of this [Phizo](#) , maybe even try going for one of the 100k Bytes Crews to start? That way at least you'd have the userbar and 10 people as a cap in the Crew. Definitely would be the cheapest option if you wanted to start something official.

As I'm sure you're aware by now, it's much cheaper to get an official group/crew now than it was many years ago.

Xamarin - September 19, 2020, 2:13 am

No offense OP, but this "hacking group" thing never made any sense to me.

I am working in the security field for a while now, and when i want to chill out and discuss something, I usually do it with my co-workers. I don't understand why serious people that work on this field, would ever endanger their good name by joining such a group, when they can get a job, do it legally, have people to discuss things with, and make money, all in the same time.

Anyways, good luck on creating your group, and finding what you are searching for.