

Forum:[Hack Forums](#)

Thread: [Hack Windows 10 computer over LAN ?](#)

Bone85 - February 6, 2016, 2:30 pm

Hello,

is it possible to hack a Windows computer over LAN. There are no shared files. And I can't find the computer under net view. SSL Strip + arpspoof doesn't work with Kali 2.0 x64. Because the computer uses Firefox (newest version).

Is it possible to get invisible remote access to the computer. I've full admin access to the router.

Best regards

Bone85

Ninja_Coder_In_Hell - February 6, 2016, 2:47 pm

You're doing something wrong if you can't find it on the network, especially if you actually have admin access to the router. Basically short of physical access or tricking a user to run something you're going to have to find/use an exploit in Windows 10. I don't know of an existing script, and writing one is going to be way beyond your skill level.

Port scanning or knowing some programs he has on his computer could open up access if there is an exploit. For example a exploitable database server has potential. Scan, gather intel and then search for exploits for those ports/services.

Metasploit would probably be a good beginning for you. Speaking of metasploit it's pretty trivial to make an infected file (ie pdf or image) but without some coding skills you won't get said file past any good antivirus.

(i)(c)(u)(r)(u)(o)(k) - February 6, 2016, 2:59 pm

(Feb 6, 2016 03:30 PM)Bone85 Wrote: [\[CITE\]](#) Hello,

is it possible to hack a Windows computer over LAN. There are no shared files. And I can't find the computer under net view. SSL Strip + arpspoof doesn't work with Kali 2.0 x64. Because the computer uses Firefox (newest version).

Is it possible to get invisible remote access to the computer. I've full admin access to the router.

Best regards

Bone85

Code SSL Strip + arpspoof doesn't work with Kali 2.0 x64. Because the computer uses Firefox (newest version).

That is not true.

Infact you can do a sslstrip and arp spoof attack from any computer/OS.

Be it windows xp-windows 10 or mac/linux it doesnt matter what OS/Bit you are running.

Also it doesnt matter if your target is using firefox newest version. A sslstrip/arp attack will still work on target device no mater what browser they use.

sslstrip/arp spoofing works by running a ssh server on your local system, When doing the arp attack you trick all network systems into thinking you are now the router. By doing so all system and devices will be using your ssh server rather than the default one. Because they are using your ssh server to handle the login the data is sent to you in raw form, At which point you forward the data to the real ssh server and get recieved packets so the user can login and make the https/ssl connection.

Anyways long story short sslstrip/arp spoofing will work if target is in the same LAN.

You could also do a dns spoof attack to allow you to force install files on the windows system.

Infact with a dns spoof attack you can trick the windows system into downloading your file over LAN via the windows update service.

Bone85 - February 6, 2016, 3:13 pm

The windows release isn't activated on his computer.

\\192.168.X.X\c\$ doesn't work.

(i)(c)(u)(r)(u)(o)(k) - February 6, 2016, 3:19 pm

(Feb 6, 2016 04:13 PM)Bone85 Wrote: [\[CITE\]](#) The windows release isn't activated on his computer.

\\192.168.X.X\c\$ doesn't work.

your telling me target has no set LAN IP from the router/modem ??

If target is conected to the router/modem, And has a IP assigned to the system from the router/modem.

Then you can hack there system if you are connected to this same router/modem.

Just do what is known as a dns spoof attack along with a arp spoof attack.

This will allow it so you can make ANY website the target users views another website.

For example the users opens browser and types google.com
or facebook.com

You can have it so there system browser will load facebook/google as your own custom website or file, While still showing it as the real and correct domain name in the users browser.

Fact is the target user can be on ANY type of OS and if they are on windows it doesnt matter if they have widows activiated yet or not none of this matters.

If target is connected to the same router/modem as you and has a assigned LAN IP you can hack them.

Not by exploiting the built-in windows net tools or network viewers but by exploiting the network itself not the user on the network.

Bone85 - February 6, 2016, 3:21 pm

It has a lan ip. But i can only ping it.

DNS spoof works.

SSL Strip works not.

URL snarf works not.

I used this tut:

"How To: Use SSLstrip On Kali Linux"

on YT.

Maybe there is the failure. I used it same way as discribed. With other IP addresses for sure.

(i)(c)(u)(r)(u)(o)(k) - February 6, 2016, 3:26 pm

(Feb 6, 2016 04:21 PM)Bone85 Wrote: [\[CITE\]](#) It has a lan ip. But i can only ping it.
ok thats fine

And dont bother with a port scan on target system all ports will be closed thats like a good 80% chance.

Just arp spoof the network and then dns spoof the network, Lookup dns spoofing tutorials there are some here on HF.

if target is connected to router/modem and has a LAN IP which it does as you said you were able to ping it.

Then a arp spoof attack and dns spoof attack will infact work, Why you think it wont work is beyond me.

Bone85 - February 6, 2016, 3:30 pm

DNS spoof works. But I wont read only the web domains, which are requested by the "victim" computer. I want remote access to the computer.

Which exploit of metasploit is for windows 10?

(i)(c)(u)(r)(u)(o)(k) - February 6, 2016, 3:36 pm

(Feb 6, 2016 04:30 PM)Bone85 Wrote: [\[CITE\]](#) DNS spoof works. But I wont read only the web domains, which are requested by the "victim" computer. I want remote access to the computer. DNS spoof method.

Trick dns on network so when target goes to say google.com or facebook.com it redirects to your website. Have a website that looks like its a windows update or a browser update that must be installed to keep using and viewing websites.

But really just have this file be a RAT.

NOTE while they are on your fake update website it will still show as google.com or facebook.com in there browser.

DNS spoofing just lets us tell there system what name server belongs to what IP.

Now once user downloads and installs the RAT return the dns back to normal and they can browse those websites agian, And now you also have full remote control of there computer.

(Feb 6, 2016 04:30 PM)Bone85 Wrote: [\[CITE\]](#) Which exploit of metasploit is for windows 10?

Dont use a exploit kit or metasploit at all your just gonna be wasting time im tellin ya, Just do a sslstrip or dns spoof attack.

No need to try and find and hope the system has a exploitable service running.

Bone85 - February 6, 2016, 3:42 pm

I have to bypass avira antivir free edition.

The av should not detect the rat. And what's about the certificates. Firefox maybe notice a fake site without legit certificate.

SSLstrip doesn't works, with the tut on yt. The tut is always the same, if you search SSL strip on YT or on google.

There are only failures in the ssl strip log file. There is a theory on web, which says: "If the site is already cached, there is no way that the browser uses the unsecure http protocol."

nmap result on vic computer:

"To many fingerprints match this hosts..."

(i)(c)(u)(r)(u)(o)(k) - February 6, 2016, 3:47 pm

(Feb 6, 2016 04:42 PM)Bone85 Wrote: [\[CITE\]](#) I have to bypass avira antivir free edition.

The av should not detect the rat. And what's about the certificates. Firefox maybe notice a fake site without legit certificate.

you will be fine give the dns settings are setup right.

I would also look into interceptor-ng

As this program can do everything you want but with a very easy and nice GUI.
And can be run on any OS.

The interceptor-ng app for android is really amazing. For example there browser cookie stealer and cookie injector.

This allows you to log directly into a account the target is logged into without knowing the username/password.

Bone85 - February 6, 2016, 3:58 pm

Why cain and able doesn't works?

There are full and half routes. But no result.

No website (http/https/etc.) logged.

There are only packets from the victim. Nothing more.

(i)(c)(u)(r)(u)(o)(k) - February 6, 2016, 4:01 pm

(Feb 6, 2016 04:58 PM)Bone85 Wrote: [\[CITE\]](#) Why cain and able doesn't works?

There are full and half routes. But no result.

Cain and able does work,

But it doesnt have a sslstrip tool, Meaning the https/ssl data packets you capture on the network will be encrypted data. So you will have to decrypt the https/ssl packets to get the login data. And this isnt easy as sometimes servers use a custom salt/certificate when hashing the https/ssl data packet, Thus making decrypting it very hard.

sslstrip makes it so the network users use our system to get there data and then we send it to the real ssh server so they can handle it.

(Feb 6, 2016 04:58 PM)Bone85 Wrote: [\[CITE\]](#) Why cain and able doesn't works?

There are full and half routes. But no result.

No website (http/https/etc.) logged.

There are only packets from the victim. Nothing more.

is target attempting to view or go to a website while you are running the arp spoof attack doesnt seem like it.

Bone85 - February 6, 2016, 4:10 pm

arp spoof, ssl strip, dns spoof is "working". Where is the result of ssl strip?

There must be preview log under the command line :

ssl strip running....

I dont mean cat sslstrip.log

But there is nothing. And url snarf shows nothing. Only dns spoof shows acitivity.

(i)(c)(u)(r)(u)(o)(k) - February 6, 2016, 4:13 pm

(Feb 6, 2016 05:10 PM)Bone85 Wrote: [\[CITE\]](#) arp spoof, ssl strip, dns spoof is working. Where is the result of ssl strip?

It writes the data into a file named sslstrip.log

you can view it by typing such in terminal

tail -f sslstrip.log

of course the user has to login to a https website before log will have data.

Bone85 - February 6, 2016, 4:13 pm

Is the attack aborted then?

(i)(c)(u)(r)(u)(o)(k) - February 6, 2016, 4:16 pm

(Feb 6, 2016 05:13 PM)Bone85 Wrote: [\[CITE\]](#) Is the attack aborted then?
??

no just let arp spoofer and sslstrip keep running, Once the target system"s login to a https website then log file will have there login data.

You just got to let the services keep running untill they make a login. And it will keep running on the network untill you decide you want to stop by closing the terminal shells.

Also the sslstrip terminal shell window itself will show data once a login is made.

Bone85 - February 6, 2016, 4:18 pm

The vic is offline :D. He restarted the router :D. Because there is no dns resolution.

The sslstrip log tells me: Host resolution error. DNS lookup failed: address wpad.XXXXXXX.ip not found.

I followed the HAK 5 tut exactly.

(i)(c)(u)(r)(u)(o)(k) - February 6, 2016, 4:34 pm

(Feb 6, 2016 05:18 PM)Bone85 Wrote: [\[CITE\]](#) The vic is offline :D. He restarted the router :D. Because there is no dns resolution.

The sslstrip log tells me: Host resolution error. DNS lookup failed: address wpad.XXXXXXX.ip not found.

I followed the HAK 5 tut exactly.

Ok well keep to it glad to hear you got it working out and hak5 is ownage xD

anyways yea next time just run the arpspoof/sslstrip dont do a dns attack.

You should really just do the dns attack if you are trying to get the user to a custom login page you

made or to download a file. Otherwise the arpspoof/sslstrip should allow you to get all there website logins.

Bone85 - February 6, 2016, 4:36 pm

Did dnsspoof disturb ssl strip?

How could my rat bypass avira antivir free edition?

The rat's i know, which are out of a tool, will be simple detected by av's.

(i)(c)(u)(r)(u)(o)(k) - February 6, 2016, 4:39 pm

(Feb 6, 2016 05:36 PM)Bone85 Wrote: [\[CITE\]](#) Did dnsspoof disturb ssl strip?
I think running a dns spoof attack along side sslstrip might cause errors yea.

In the MiTM hak5 tut they dont do a dns spoof attack do they ?

Anyways If you do want to dns spoof attack just dont run the attack while sslstrip is running. But you do need to have arp spoof running while you do a dns spoof attack.

Just get a good paid crypter for your RAT or follow my tut here
<https://hackforums.net/showthread.php?tid=4802039>

Also I would suggest using netcat as your RAT

ncat runs on all OS windows/linux/mac/iOS/android

meaning your server and client can be on any OS. target OS wont matter :)

just search into making a reverse connection RAT with ncat

Or netcat hook cmd/shell reverse socket connection.

Bone85 - February 6, 2016, 4:45 pm

I dont want the rat on my host system. Is that possible to send the rat only over my virtual machine with kali linux to the vic? I think so, because it should be linux based :D.

Do u have experience with hacking a Ubiquiti Edge Router. I have full access to the web interface. But i don't know the login information. The standard username and password dont work.

Open ports:

HTTP, HTTPS, DNS

(i)(c)(u)(r)(u)(o)(k) - February 6, 2016, 4:51 pm

(Feb 6, 2016 05:45 PM)Bone85 Wrote: [\[CITE\]](#) I dont want the rat on my host system. Is that possible to send the rat only over my virtual machine with kali linux to the vic?

Do u have experience in hacking a Ubiquiti Edge Router. I have full access to the web interface. But i don't know the login information.

you can host the RAT anywhere you like as long as the target can access it.

I would just create a webhosting account or ftp account and upload your RAT there.. And then its not on your system, And make a php/html page that downloads that file as a fake browser or windows update.

Then when you do decide to do a dns spoof attack you can redirect traffic to that website with your RAT/Fake update.

As for cracking into the router yea just use a brute forcer like hydra or ncrack, Or lookup the default login for that router type.

OHHH ok I see you mean host as in the socket server of the RAT.

You can avoid this by using a botnet and not a RAT or use a VPN that supports port forwarding on the system you will host the RAT server socket on.

A botnet is a RAT that works on a webserver so you dont need to host the server socket on any system rather the website itself is the server host.

But yes if you use netcat RAT then you can run the server socket host on the linux OS and port forward it past router/modem once you can login to it im guessing.

Or you could use a cheap vpn like nvpn and just bypass that router all together.

Bone85 - February 6, 2016, 4:54 pm

Default username and password didn't work.

I tried medusa and hydra, both show me password cracked x times. But it isn't. A false positive.

If you dont know the user name, u have to bruteforce both? The password and the user name?

The os on the router is edgemax.

Is there no exploit?

(i)(c)(u)(r)(u)(o)(k) - February 6, 2016, 4:58 pm

(Feb 6, 2016 05:54 PM)Bone85 Wrote: [\[CITE\]](#) I tried medusa and hydra both show me password cracked x times. But it isn't. A false positive.

If you dont know the user name, u have to bruteforce both? The password and the user name?

Is there no exploit?

As I said you can avoid using the router to port forward by using a cheap vpn that supports it like nvpn.

As for cracking it no exploits off hand I know of, I would try using ncrack to brute force the login.

And if you dont know the username then yes you need a wordlist for both username and password. But ncrack shouldnt give any false positives its pretty reliable.

This is the only exploit I found off a quick skim online

<http://community.ubnt.com/t5/EdgeMAX/security-CVE-2014-6271-Bash-quot-remote-quot-vulnerability/td-p/1025659>

But that isnt going to help us at all from what I gather.

You could try arp spoofing the target and do a dns spoof that forces target to the router login page when they type in any web address thus forcing the user to login to there router and then you can capture there login to it that way.

Bone85 - February 6, 2016, 5:02 pm

This takes years?

Cracking WPA2 handshakes take years, with 20 random digits strong password.

If you have no GPU based server farm, like an intelligence, you can't crack it with bruteforce attack.

And this is GPU/CUDA based, on a GTX 980 TI with ~98 % GPU load.

Pyrit didnt work with db attack. So I had to use ocl hashcat.

(i)(c)(u)(r)(u)(o)(k) - February 6, 2016, 5:07 pm

(Feb 6, 2016 06:02 PM)Bone85 Wrote: [\[CITE\]](#) This takes years?

Cracking WPA2 handshakes take years, with 20 random digits strong password.

If you have no GPU based server farm, like an intelligence, you can't crack it with bruteforce attack.

And this is GPU/CUDA based, on a GTX 980 TI with ~98 % GPU load.

Pyrit didnt work with db attack. So I had to use ocl hashcat.

haha

you are not cracking a wpa key the router web based login doesnt use wpa to login thats for the wifi signal connection.

If you are trying to crack the password encryption of the wifi signal thats cracking wpa.

The router login is just a basic http login brute force attack.

Bone85 - February 6, 2016, 5:10 pm

Yep, I know. It takes much, much more time. Especially if the router rejected your request.

And if a WPA 2 handshake takes years with 1 variable, and x 1000 passwords per second, you can imagine how long a https based attack with 2 variables takes.

Is there a way to transfer a wpa handshake into a md5 hash ?

(i)(c)(u)(r)(u)(o)(k) - February 6, 2016, 5:15 pm

(Feb 6, 2016 06:10 PM)Bone85 Wrote: [\[CITE\]](#) Yep, I know. It takes much, much more time. Especially if the router rejected your request.

Is there a way to transfer a wpa handshake into a md5 hash ?
not that I know of,

Code you can imagine how long a https based attack with 2 variables takes.
This isnt really correct at all. wpa cracking is not http post data brute forcing. Not the same at all..

http brute forcing isnt really even cracking it doesnt decrypt or crack any strings or values.

So now you need to crack the wifi password lol....?

Well if the wifi is using wpa/wpa-2 then cracking it is gonna be a pain no doubt.

And will all depend on how large your database is on cracking it as it works off a list, It cant auto crack off handshakes like wep type encryptions.

Another option could be a wps exploit.

Most routers nowadays have a wps option and the default data for this isnt changed much, And its a exploitable service on many routers.

Hacking the wps key may be much much easier than hacking the wpa at times.

Bone85 - February 6, 2016, 5:17 pm

There is no wps activated (no pbc and no pin) . This is a modern router with newest firmware. If wps has been manually activated, it will turn it automatically off, after 2 minutes.

11000 Pins are better then billions of passwords :D.

Do you have experience with DLink routers and wps lock ? mdk 3 and aireplay wont shut down the router in order to lose the lock.

The dlink default pin script doesn't work. It's another pin.

Why is here no https available? The login on this site could be easily sniffed by a man in the middle

attack :D.

(i)(c)(u)(r)(u)(o)(k) - February 6, 2016, 5:24 pm

(Feb 6, 2016 06:17 PM)Bone85 Wrote: [\[CITE\]](#) There is no wps activated (no pbc and no pin) . This is a modern router with newest firmware. If wps is manually activated it will turn it automatically off after 2 minutes.

11000 Pins are better than billions of passwords :D.

Do you have experience with DLink routers and wps lock ? mdk 3 and aireplay wont shut down the router in order to lose the lock.

The dlink default pin script doesn't work. It's another pin.
haha sorry nope to be honest I havent used linux in about a full year let alone mess around with network hacking in a linux OS.

Last time I was wifi and network hacking in a linux OS was like 2012.

and I forgot most of the aircrack-ng suite commands and functions

Bone85 - February 6, 2016, 5:28 pm

Which os do u use for "hacking"?

Android (derivative of linux)?

(i)(c)(u)(r)(u)(o)(k) - February 6, 2016, 5:30 pm

(Feb 6, 2016 06:28 PM)Bone85 Wrote: [\[CITE\]](#) Which os do u use for "hacking"?

Android (derivative of linux)?

Glad to see you know android is just a linux distro

haha I used to use the android unix kernel alot yea ARM arch

But I infact do use windows most of the time for my hacking believe it or not.

I find you can do anything on windows you can do on linux for the most part give you have the correct drivers installed or modded.

Just doesnt have a good shell system is all but im ok with it.

Bone85 - February 6, 2016, 5:37 pm

Could delete this post please ?

NBGovernment - February 6, 2016, 9:05 pm

Which os do u use for "hacking"?

Bone85 - February 7, 2016, 3:36 am

I use kali linux x64 for this.