

Forum:[Hack Forums](#)

Thread: [Snooping in a local network.](#)

hack3rcon - November 4, 2018, 9:54 pm

Hello.

In a local network, How can I understand that network admin can sniff my traffic or use any special devices?

Thank you.

Strayaa - November 4, 2018, 9:58 pm

Could you explain a bit more in depth what you're asking

CyberError - November 4, 2018, 10:12 pm

not sure what you want to know ,

but in a lan , a network admin or anyone can sniff all traffic with "WireShark"

hack3rcon - November 5, 2018, 1:56 am

(Nov 4, 2018 10:58 PM)STBG_banappeal Wrote: [\[CITE\]](#) Could you explain a bit more in depth what you're asking

I want to know if I check my email in a local network then can network admin sniff my username and password? I my browser use "HTTPS" then?

CyberStrike - November 5, 2018, 2:03 am

(Nov 5, 2018 02:56 AM)hack3rcon Wrote: [\[CITE\]](#) I want to know if I check my email in a local network then can network admin sniff my username and password? I my browser use "HTTPS" then?

Maybe, if you are going through a proxy which generates their own SSL/TLS (term used interchangeably) cert and it's accepted to your computer then yes example :

<https://docs.mitmproxy.org/stable/howto-wireshark-tls/>

Now the admin probably has access to the machine so they may have setup the environment key then they may not really need to issue out their own SSL key just capture the SSL cert grab the key session and can decrypt that way. If it's your own machine then they would really need to issue their own SSL cert. An Intercepting Proxy may also be used though it'd be a clunky way to do this and SSL would need to be added to machines, all doable just clunky.

sh4moon - November 5, 2018, 5:26 am

(Nov 5, 2018 02:56 AM)hack3rcon Wrote: [\[CITE\]](#) I want to know if I check my email in a local network then can network admin sniff my username and password? I my browser use "HTTPS" then?

as long as you're checking it over https you should be good. even if the sys admin can sniff it on the network layer, he can't decrypt the application layer traffic.

hack3rcon - November 5, 2018, 9:59 pm

(Nov 5, 2018 03:03 AM)SilentWatch Wrote: [\[CITE\]](#) Maybe, if you are going through a proxy which generates their own SSL/TLS (term used interchangeably) cert and it's accepted to your computer then yes example :

<https://docs.mitmproxy.org/stable/howto-wireshark-tls/>

Now the admin probably has access to the machine so they may have setup the environment key then they may not really need to issue out their own SSL key just capture the SSL cert grab the key session and can decrypt that way. If it's your own machine then they would really need to issue their own SSL cert. An Intercepting Proxy may also be used though it'd be a clunky way to do this and SSL would need to be added to machines, all doable just clunky.

Can you show me step by step? Which tool must be installed and...

(Nov 5, 2018 06:26 AM)sh4moon Wrote: [\[CITE\]](#) as long as you're checking it over https you should be good. even if the sys admin can sniff it on the network layer, he can't decrypt the application layer traffic.

Any tools exist for finding snooping devices in a local network?

sh4moon - November 5, 2018, 10:08 pm

(Nov 5, 2018 10:59 PM)hack3rcon Wrote: [\[CITE\]](#) Can you show me step by step? Which tool must be installed and...

Any tools exist for finding snooping devices in a local network?

ooh. as far as I know there's not. granted the attacker would have to have the traffic going through him. there's two kinds of router. one that sends all traffic to all interfaces and one that only sends to the recipient. the one that only sends to recipient is more common. you'd have to arp spoof or something similar which can be detected.

CyberStrike - November 5, 2018, 10:57 pm

(Nov 4, 2018 10:54 PM)hack3rcon Wrote: [\[CITE\]](#) Hello.

In a local network, How can I understand that network admin can sniff my traffic or use any special devices?

Thank you.

(Nov 5, 2018 11:08 PM)sh4moon Wrote: [\[CITE\]](#) ooh. as far as I know there's not. granted the attacker would have to have the traffic going through him. there's two kinds of router. one that sends all traffic to all interfaces and one that only sends to the recipient. the one that only sends to recipient is more common. you'd have to arp spoof or something similar which can be detected.

OP mentioned an admin so we have to assume that they have full access to machines on the network, we are not quite assuming the common switch.. arp poisoning or arp cache poisoning on machines, of an attacker who is running a mitm. We have to think admin, who setup a proxy properly and has pushed their own TLS cert to those machines and accepted them. This is rather common in corporate environments

<https://www.us-cert.gov/ncas/alerts/TA17-075A>

hack3rcon, Not too sure there is a hand holding guide and yes we are assuming that an admin has full control of their network and you just want to know if it's possible.

<https://jimshaver.net/2015/02/11/decrypting-tls-browser-traffic-with-wireshark-the-easy-way/>

MitmProxy Supports this as well the admin generates their own TLS/SSL cert perhaps keeps the sessionskey variable in place to make it easier and quicker.

<https://docs.mitmproxy.org/stable/>

(Yes once again no hand holding)

We all have used Burp/Zap to intercept our requests and responses on HTTPS it'd be a bit unwieldy in a large scale to use one of these to do all that but just an example. It's possible, perhaps to varying degrees but it's done in corporations.

F.B.I - November 5, 2018, 11:00 pm

(Nov 5, 2018 06:26 AM)sh4moon Wrote: [\[CITE\]](#) as long as you're checking it over https you should be good. even if the sys admin can sniff it on the network layer, he can't decrypt the application layer traffic.

What about SSL strip?

CyberStrike - November 5, 2018, 11:31 pm

(Nov 6, 2018 12:00 AM)DotComs Wrote: [\[CITE\]](#) What about SSL strip? and HSTS bypass .. don't forget that one for getting browsers. I got a sneaking suspicion that OP is looking to mitm not sure I really assumed this was "can an admin get my credentials"

Edit: Just to clarify here the admin could just setup a phishing page and send OP to a fake service.. doubtful but who knows.

sh4moon - November 6, 2018, 7:37 am

(Nov 6, 2018 12:00 AM)DotComs Wrote: [\[CITE\]](#) What about SSL strip? if it's a system admin I doubt he'll be ssl stripping.

shelled - November 7, 2018, 7:57 pm

Quote>Edit: Just to clarify here the admin could just setup a phishing page and send OP to a fake service.. doubtful but who knows.

Most practical way to get creds is via phishing. Still a heavy part of any red team engagement because it just takes a few people to enter creds to win.

No point trying to break TLS. Impractical and likely not something your sysad is going to waste his time on.

hack3rcon - November 12, 2018, 4:53 am

Can I use some tools like "OpenSSL" for encrypt my connection?

sh4moon - November 12, 2018, 5:01 am

(Nov 12, 2018 05:53 AM)hack3rcon Wrote: [\[CITE\]](#) Can I use some tools like "OpenSSL" for encrypt my connection?

I'm pretty sure that's not what that's for. use a vpn.

hack3rcon - November 13, 2018, 12:43 am

(Nov 12, 2018 06:01 AM)sh4moon Wrote: [\[CITE\]](#) I'm pretty sure that's not what that's for. use a vpn. Tor? I can't use any trick for encrypting my connections?

sh4moon - November 13, 2018, 3:17 am

(Nov 13, 2018 01:43 AM)hack3rcon Wrote: [\[CITE\]](#) Tor? I can't use any trick for encrypting my connections?

I was saying not openssl.