

Forum:[Hack Forums](#)

Thread: [failed MITM by using arpspoof](#)

hikaris - January 2, 2020, 9:28 am

server don't reply SYN/ACK when I transfer the TCP SYN packet by scapy or by windows default routing services. But I can transfer packets from server to the PC attacked.

I use my python script and many tools like ettercap, nighthawk, arpspoof. But got same results.

Shisho - January 2, 2020, 12:58 pm

That's not how routing works. You should get a better grasp of layer 3 routing before you try to MITM via arp poisoning.

If the packets are not being forwarded by the switch you are not doing anything to the MAC table and will have packets routed normally to their designated host which will result in an RST.

hikaris - January 3, 2020, 2:12 am

(Jan 2, 2020 01:58 PM)Shisho Wrote: [\[CITE\]](#) That's not how routing works. You should get a better grasp of layer 3 routing before you try to MITM via arp poisoning.

If the packets are not being forwarded by the switch you are not doing anything to the MAC table and will have packets routed normally to their designated host which will result in an RST.

but why tools failed? Ettercap and arpspoof.

CyberStrike - January 4, 2020, 6:10 am

(Jan 2, 2020 01:58 PM)Shisho Wrote: [\[CITE\]](#) That's not how routing works. You should get a better grasp of layer 3 routing before you try to MITM via arp poisoning.

If the packets are not being forwarded by the switch you are not doing anything to the MAC table and will have packets routed normally to their designated host which will result in an RST.

(Jan 3, 2020 03:12 AM)hikaris Wrote: [\[CITE\]](#) but why tools failed? Ettercap and arpspoof.

He told you why, because currently you are sending a packet, each machine locally is checking "Hey is that me?" if it's not said machine the arp packet is discarded.

Please read the following, although a good understanding of networking would be better:

[https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc758357\(v=ws.10\)?redirectedfrom=MSDN](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc758357(v=ws.10)?redirectedfrom=MSDN)

hikaris - January 5, 2020, 12:48 am

(Jan 3, 2020 03:12 AM)hikaris Wrote: [\[CITE\]](#) but why tools failed? Ettercap and arpspoof.

but i'm forwarding a TCP packet from the one I'm poisoning but not a arp packet. I know how arp poisoning works. It's a bi-directional poisoning, and have tested ip_forward on each single direction.

CyberStrike - January 5, 2020, 3:35 am

Remember that browsers use HSTS as well you got some real learning to go and do, or the frustration you currently are seeing will either lead you to exiting or just skipping material because you are unwilling to go out and learn what's going on. This site I am guessing is also https and not a

local resource correct?

Shisho - January 5, 2020, 12:06 pm

(Jan 5, 2020 01:48 AM)hikaris Wrote: [\[CITE\]](#) but i'm forwarding a TCP packet from the one I'm poisoning but not a arp packet. I know how arp poisoning works. It's a bi-directional poisoning, and have tested ip_forward on each single direction.

Have you confirmed that ARP entries on the target system are indeed poisoned and that your switch is not using some form of static ARP entries based on physical link?

Flow should be as follows:

Attacker <> Switch <> Poisoned Target

With the switch forwarding only attacker traffic to the gateway after it passes through from the poisoned target.

Nomad.Null - January 5, 2020, 7:44 pm

There are multiple reasons this may fail, but the most likely is that you are faced up against a smart switch with arpspoof protection. Simply put, arpspoofing is the least subtle, most detectable, and obnoxious form of Man-in-the-Middle attack you can perform, and almost every modern (smart)switch or switching router possesses countermeasures to detect and discard your spoofed packets.

Arpspoofing is like screaming into a bullhorn that THIS IS THE MAC ADDRESS YOU ARE LOOKING FOR to everyone on the network at the same time without ever being asked. The number of ARP packets generated in the first 10 seconds of the attack alone is a sufficient indication of what is happening, and a smart switch can use this to simply drop all incoming ARP replies coming from your machine.

These days, NBNS, MDNS, LLMNR, and DNS spoofing are all the rage, and are especially effective against windows domain environments. It's even more effective on networks with servers predating Windows Server 2016. Check out the SMB/NTLM relay attacks. You'll probably have much better luck with them. You won't intercept all traffic, but you'll intercept the important kind... creds. :)

hikaris - January 5, 2020, 10:29 pm

(Jan 5, 2020 04:35 AM)CyberStrike Wrote: [\[CITE\]](#) Remember that browsers use HSTS as well you got some real learning to go and do, or the frustration you currently are seeing will either lead you to exiting or just skipping material because you are unwilling to go out and learn what's going on. This site I am guessing is also https and not a local resource correct?

Thanks for your reply. I'm glad to got reply from anyone who wants to help me. I'm new to this area and don't familiar with terminology. I just can't figure out why I failed. I have followed tutorials and try my best to understand every professional term appeared in tutorials. It's http but not https, and it's a verify page of campus network in my university. I'm sure that gateway was receiving my arp reply packet, because I have successfully deceived gateway that I'm someone else. The gateway send packets to me and then, I forward packets to someone else(call him host B). I opened wireshark on host B and it only receive packets from me indeed.

(Jan 5, 2020 01:06 PM)Shisho Wrote: [\[CITE\]](#) Have you confirmed that ARP entries on the target system are indeed poisoned and that your switch is not using some form of static ARP entries based on physical link?

Flow should be as follows:

Attacker <> Switch <> Poisoned Target

With the switch forwarding only attacker traffic to the gateway after it passes through from the poisoned target.

Yes I confirmed. Let us call the one being attacked as host B, my PC as Host A.

If I only send arp reply to gateway(but don't send to host B), then I can intercept packets from outside to host B. Host B can only receive packets forwarded by me. This result can be a proof that I have successfully deceived gateway. It can also proof that the IP_FORWARDING on my PC is working well, isn't it?

(Jan 5, 2020 08:44 PM)True Demon Wrote: [\[CITE\]](#) There are multiple reasons this may fail, but the most likely is that you are faced up against a smart switch with arpspoof protection. Simply put, arpspoofing is the least subtle, most detectable, and obnoxious form of Man-in-the-Middle attack you can perform, and almost every modern (smart)switch or switching router possesses countermeasures to detect and discard your spoofed packets.

Arpspoofing is like screaming into a bullhorn that THIS IS THE MAC ADDRESS YOU ARE LOOKING FOR to everyone on the network at the same time without ever being asked. The number of ARP packets generated in the first 10 seconds of the attack alone is a sufficient indication of what is happening, and a smart switch can use this to simply drop all incoming ARP replies coming from your machine.

These days, NBNS, MDNS, LLMNR, and DNS spoofing are all the rage, and are especially effective against windows domain environments. It's even more effective on networks with servers predating Windows Server 2016. Check out the SMB/NTLM relay attacks. You'll probably have much better luck with them. You won't intercept all traffic, but you'll intercept the important kind... creds. :)

Thanks for your reply and suggestion. I think what you said cannot resolve my question. But I will learn more about what you recommend. Thank you.