

Forum:[Hack Forums](#)

Thread: [Question about Nmap and PenTesting](#)

BinarOper - March 9, 2018, 2:24 pm

Hello, i am doing some research on a few interesting topics about security and i have a question to ask.

Nmap provides a few tools and techniques that can be use to "evade" a firewall. Correct me if i am wrong but those techniques only work if the target's firewall is misconfigured. So what does a professional PenTester do if the firewall is not misconfigured or if he cannot "evade" said firewall? Are there other ways to port scan? Or does he not port scan at all and simply tries a different approach? And if so, what kind of approach?

You do not need to give me a tutorial, i am asking this for educational purposes so i only need "theory" not "practice". Thank you very much :D !

pomwtin - March 9, 2018, 3:49 pm

(Mar 9, 2018 03:24 PM)BinarOper Wrote: [\[CITE\]](#) Hello, i am doing some research on a few interesting topics about security and i have a question to ask.

Nmap provides a few tools and techniques that can be use to "evade" a firewall. Correct me if i am wrong but those techniques only work if the target's firewall is misconfigured. So what does a professional PenTester do if the firewall is not misconfigured or if he cannot "evade" said firewall? Are there other ways to port scan? Or does he not port scan at all and simply tries a different approach? And if so, what kind of approach?

You do not need to give me a tutorial, i am asking this for educational purposes so i only need "theory" not "practice". Thank you very much :D !

Well there are some passive fingerprinting techniques. Some of them are implemented in pof and sinpf. But bare in mind that it can be a bit difficult and take a lot of time, since fingerprint is opurtinistic... based on events which happens "normally" in the network.

Another messy way to go is "hail mary"... blindly execute all exploits you have your hands on.. maybe one will work... BUT, in this case a looooot of noise is produced and therefor it is not really usefull.

BinarOper - March 10, 2018, 3:09 am

(Mar 9, 2018 04:49 PM)pomwtin Wrote: [\[CITE\]](#) Well there are some passive fingerprinting techniques. Some of them are implemented in pof and sinpf. But bare in mind that it can be a bit difficult and take a lot of time, since fingerprint is opurtinistic... based on events which happens "normally" in the network.

Another messy way to go is "hail mary"... blindly execute all exploits you have your hands on.. maybe one will work... BUT, in this case a looooot of noise is produced and therefor it is not really usefull.

Thanks a lot for the answer!

CyberStrike - March 12, 2018, 2:30 am

Well now a days the perimeter is well defended. Before it was not like this, and often books or tutorials explain a bit about scanning yet because that perimeter is well defended it isn't well explained. It's a bit of old school how it was and sometimes still works, but generally the model of

Recon/Scan/enumeration/exploit/access isn't how the real world is. Real world lets call Recon phase which encompasses all of the above as well as also figuring people out, how do most attackers gain access to a network exploit? Generally in CEH they discuss exploit in the classic terms of running code for remote exploit, in the real world you end up with an employee who decides to open a document or whatever and proceeds to give us access.

So generally firewalls tend to deny a ton of stuff, and normal port scans often are quickly pinpointed and blocked externally. When we are discussing remote scanning from the outside of a network in the real world this is a rare occurrence that we plan a compromise by attacking a well defended perimeter. Instead what we are looking to do by enumerating the firewalls is after exploiting machines within the network we will want to blend in with traffic. For example if I have one machine that is connected to some odd host and an odd TCP port it doesn't hit normal traffic. Also if we are sending some massive chunks of data on that connection it's bad. Now in the real world you have an ssl certificate, not one that you make at home you have actual infrastructure. A domain legit and a legit ssl also you have your pentesting infrastructure in the back as subdomains.

I got a little something on infrastructure that is needed to be successful in large scale engagements, from 400-65,000 machines in one engagement

<https://hackforums.net/showthread.php?tid=5728866>

There are a few things I tend to like doing tcpdump even tshark/wireshark but we are looking at but we look at different "window size" and TTL for packets we receive. For example TTL value of 64 unix... 124-128 Windows 255 Cisco/solaris.

<http://www.netresec.com/?page=Blog&month=2011-11&post=Passive-OS-Fingerprinting>

But also a good understanding of networking because more than anything we are trying to figure out the firewall rules to get out without setting off all the alarmbells and whistles with some fireworks.

BinarOper - March 13, 2018, 11:18 am

(Mar 9, 2018 04:49 PM)pomwtin Wrote: [\[CITE\]](#) Well there are some passive fingerprinting techniques. Some of them are implemented in pof and sinpf. But bare in mind that it can be a bit difficult and take a lot of time, since fingerprint is oportinistic... based on events which happens "normally" in the network.

Another messy way to go is "hail mary"... blindly execute all exploits you have your hands on.. maybe one will work... BUT, in this case a looooot of noise is produced and therefor it is not really usefull.

Thank you for the answer, i did some research on passive tools like p0f and got all my questions answered.

(Mar 12, 2018 02:30 AM)sirru5h Wrote: [\[CITE\]](#) Well now a days the perimeter is well defended. Before it was not like this, and often books or tutorials explain a bit about scanning yet because that perimeter is well defended it isn't well explained. It's a bit of old school how it was and sometimes still works, but generally the model of Recon/Scan/enumeration/exploit/access isn't how the real world is. Real world lets call Recon phase which encompasses all of the above as well as also figuring people out, how do most attackers gain access to a network exploit? Generally in CEH they discuss exploit in the classic terms of running code for remote exploit, in the real world you end up with an employee who decides to open a document or whatever and proceeds to give us access.

So generally firewalls tend to deny a ton of stuff, and normal port scans often are quickly pinpointed and blocked externally. When we are discussing remote scanning from the outside of a network in the real world this is a rare occurrence that we plan a compromise by attacking a well defended

perimeter. Instead what we are looking to do by enumerating the firewalls is after exploiting machines within the network we will want to blend in with traffic. For example if I have one machine that is connected to some odd host and an odd TCP port it doesn't hit normal traffic. Also if we are sending some massive chunks of data on that connection it's bad. Now in the real world you have an ssl certificate, not one that you make at home you have actual infrastructure. A domain legit and a legit ssl also you have your pentesting infrastructure in the back as subdomains.

I got a little something on infrastructure that is needed to be successful in large scale engagements, from 400-65,000 machines in one engagement

There are a few things I tend to like doing tcpdump even tshark/wireshark but we are looking at but we look at different "window size" and TTL for packets we receive. For example TTL value of 64 unix... 124-128 Windows 255 Cisco/solaris.

But also a good understanding of networking because more than anything we are trying to figure out the firewall rules to get out without setting off all the alarmbells and whistles with some fireworks. Thanks a lot for taking the time to write this. I think this fully covers everything. I also the links you posted were very helpful and even enjoyable to read.

P.S Removed the links from the quotes because HF wouldn't let me post this.

CyberStrike - March 13, 2018, 11:37 am

Awesome I hope it does help you will find that if you have everything infrastructure wise in place you will find that odd balled issues like "I can't get around smartscreen" will work itself out.

Ki11Mach - March 13, 2018, 1:36 pm

Hey sirru5h thanks for the comment, I found it informative.

stickeebuds420 - July 2, 2018, 10:15 am

(Mar 12, 2018 02:30 AM)sirru5h Wrote: [\[CITE\]](#) Well now a days the perimeter is well defended. Before it was not like this, and often books or tutorials explain a bit about scanning yet because that perimeter is well defended it isn't well explained. It's a bit of old school how it was and sometimes still works, but generally the model of Recon/Scan/enumeration/exploit/access isn't how the real world is. Real world lets call Recon phase which encompasses all of the above as well as also figuring people out, how do most attackers gain access to a network exploit? Generally in CEH they discuss exploit in the classic terms of running code for remote exploit, in the real world you end up with an employee who decides to open a document or whatever and proceeds to give us access.

So generally firewalls tend to deny a ton of stuff, and normal port scans often are quickly pinpointed and blocked externally. When we are discussing remote scanning from the outside of a network in the real world this is a rare occurrence that we plan a compromise by attacking a well defended perimeter. Instead what we are looking to do by enumerating the firewalls is after exploiting machines within the network we will want to blend in with traffic. For example if I have one machine that is connected to some odd host and an odd TCP port it doesn't hit normal traffic. Also if we are sending some massive chunks of data on that connection it's bad. Now in the real world you have an ssl certificate, not one that you make at home you have actual infrastructure. A domain legit and a legit ssl also you have your pentesting infrastructure in the back as subdomains.

I got a little something on infrastructure that is needed to be successful in large scale engagements, from 400-65,000 machines in one engagement

<https://hackforums.net/showthread.php?tid=5728866>

There are a few things I tend to like doing tcpdump even tshark/wireshark but we are looking at but we look at different "window size" and TTL for packets we receive. For example TTL value of 64 unix... 124-128 Windows 255 Cisco/solaris.

<http://www.netresec.com/?page=Blog&month=2011-11&post=Passive-OS-Fingerprinting>

But also a good understanding of networking because more than anything we are trying to figure out the firewall rules to get out without setting off all the alarmbells and whistles with some fireworks. Is it possible to spoof the source address as a non routable up? Spoof as 192.168 so that the firewall thinks it is it's own traffic

Last_viking - July 2, 2018, 10:48 am

Before bypassing firewalls learn how firewall functions

Most of the advance firewall block ICMP packets //or any tcp packet

How do you bypass firewall?

You send fragmented packets over the network, fragment means breaking packet into pieces because

Firewall scans entire packet header and data and drops the request if it is malformed

In fragment packets it sends packets in sequence first packet -->second packet soon after first packet

Thus packet bypass firewall

And later first and second packets joined together

If u trying to bypass professional firewalls look into custom packet crafting by colasoft

More info here

<https://www.kitploit.com/2018/04/nemesis-command-line-network-packet.html>

CyberStrike - July 3, 2018, 2:07 am

(Jul 2, 2018 10:15 AM)stickeebuds420 Wrote: [\[CITE\]](#) Is it possible to spoof the source address as a non routable up? Spoof as 192.168 so that the firewall thinks it is it's own traffic

Well if you are within the network then you can forward packets to specific ports and a specific destination through what I would call "redirects". Basically a machine which is compromised, it has no tools, no data but all it does it just redirect traffic from an attack machine to a target machine.

<https://hackforums.net/showthread.php?tid=5733292>

There is a section in that tutorial on how to do this, it's titled "" Setting up redirects on target machine" has both powershell and cmd. But as for spoofing the source that can be done sure, but when dealing with firewalls much traffic is blocked/rejected definitely on the parameter you will see this. Within the network more than likely a firewall will detect the scans and the spoofing it'd be quite obvious when looking at a frame.

stickeebuds420 - July 3, 2018, 4:19 am

(Jul 3, 2018 02:07 AM)sirru5h Wrote: [\[CITE\]](#) Well if you are within the network then you can forward packets to specific ports and a specific destination through what I would call "redirects". Basically a machine which is compromised, it has no tools, no data but all it does it just redirect traffic from an attack machine to a target machine.

<https://hackforums.net/showthread.php?tid=5733292>

There is a section in that tutorial on how to do this, it's titled "Setting up redirects on target machine" has both powershell and cmd. But as for spoofing the source that can be done sure, but when dealing with firewalls much traffic is blocked/rejected definitely on the parameter you will see this. Within the network more than likely a firewall will detect the scans and the spoofing it'd be quite obvious when looking at a frame. Thanks for the information, I'll definitely have a read after work. Skimming through though it looks like you have to have physical access to the computer. Is there a way to evade a firewall by spoofing a whitelisted address? For instance, the user of the target machine uses steam or some other application that requests outgoing connections. Couldn't you spoof that address and the firewall would just think, "oh it's legitimate traffic coming from a known source, let it through"

CyberStrike - July 3, 2018, 5:02 am

(Jul 3, 2018 04:19 AM)stickeebuds420 Wrote: [\[CITE\]](#) Thanks for the information, I'll definitely have a read after work. Skimming through though it looks like you have to have physical access to the computer. Is there a way to evade a firewall by spoofing a whitelisted address? For instance, the user of the target machine uses steam or some other application that requests outgoing connections. Couldn't you spoof that address and the firewall would just think, "oh it's legitimate traffic coming from a known source, let it through"

Physical access no, but you have to be in the machine, basically a machine in the network. Like if you are thinking I will spoof a steam server's IP send some packets, that is just not how it works, There are several mechanisms to check for errors, basically packets that are bad/not valid, you have the initial handshake to make a connection in TCP, if we are talking IPv6 then MAC addresses can be resolved and used to bridge network segments, so now that is another layer you need to spoof.

https://en.wikipedia.org/wiki/Neighbor_Discovery_Protocol

I keep saying that the perimeter is not the place to start an attack and I am not writing it as filler. Most everyone now looks at getting into a network by compromising a user and then their computer. Within a network you may encounter firewalls but you now have more options.

stickeebuds420 - July 4, 2018, 8:32 am

[quote='sirru5h' pid='57297378' dateline='1530619334']

Physical access no, but you have to be in the machine, basically a machine in the network. Like if you are thinking I will spoof a steam server's IP send some packets, that is just not how it works, There are several mechanisms to check for errors, basically packets that are bad/not valid, you have the initial handshake to make a connection in TCP, if we are talking IPv6 then MAC addresses can be resolved and used to bridge network segments, so now that is another layer you need to spoof.

https://en.wikipedia.org/wiki/Neighbor_Discovery_Protocol

I keep saying that the perimeter is not the place to start an attack and I am not writing it as filler. Most everyone now looks at getting into a network by compromising a user and then their computer. Within a network you may encounter firewalls but you now have more options.

Thanks for the information! Truly appreciated. Social engineering seems to be the way to go in order to obtain an internal pc. In that case, a person would have to encrypt any sort of remote access terminal that is put on the computer?

CyberStrike - July 4, 2018, 11:25 am

(Jul 4, 2018 08:32 AM)stickeebuds420 Wrote: [\[CITE\]](#) Thanks for the information! Truly appreciated.

Social engineering seems to be the way to go in order to obtain an internal pc. In that case, a person would have to encrypt any sort of remote access terminal that is put on the computer? Using crypters is not the only method to bypass an antivirus you would really want to learn as much as you can about antivirus's to be able to bypass them. You are right though the majority of infections end up happening due to social engineering.

stickeebuds420 - July 4, 2018, 12:04 pm

(Jul 4, 2018 11:25 AM)sirru5h Wrote: [\[CITE\]](#) Using crypters is not the only method to bypass an antivirus you would really want to learn as much as you can about antivirus's to be able to bypass them. You are right though the majority of infections end up happening due to social engineering. But if a person does not disguise the signature would their avg go off?

CyberStrike - July 4, 2018, 7:54 pm

(Jul 4, 2018 12:04 PM)stickeebuds420 Wrote: [\[CITE\]](#) But if a person does not disguise the signature would their avg go off?

If you are thinking about code signing certificate then yes, but I am talking about AV signatures those can be changed up. Like I said learn as much as you can on AV's I did this thread a while back but I made sure to include references so users can read on their own.

<https://hackforums.net/showthread.php?tid=5808303>