

Forum: [Hack Forums](#)

Thread: [Spreading in a LAN](#)

ApexLead - August 20, 2018, 6:13 am

Hello everyone,

I'm playing around with RATs for a while now, and after having enough of controlling one machine I would like to learn spreading over a LAN methods, I don't know how to say it so let me explain: Say I have control over a machine (Shell, uploading files to the machine, downloading files from it and executing files on it), what are the methods for hopping to other machines and other users within the same LAN? Should I use tools or there are more elegant ways to do it?

P.S - I'm not necessarily looking for a specific solution, a direction will help as well.

Thanks in advance ?

Nick (Name) - August 20, 2018, 9:01 am

I remember that CursedScreech had a function to phish Windows credentials with Powershell, this was back when I was testing WiFi Pineapples. Here's the original post on hak5's forum:

<https://forums.hak5.org/topic/37759-official-cursedscreech/>

Once you have credentials you can use PsExec to execute a program on the remote LAN machine.

Last_viking - August 20, 2018, 6:44 pm

you can use mimikatz and spread on lan using psExec

another method is to arp spoof and redirecting him

To download the payload this kind of attacks are very noisy and not stable

PsExec only works if passwords similar or same

CyberStrike - August 20, 2018, 7:31 pm

(Aug 20, 2018 09:01 AM)Nick (Name) Wrote: [\[CITE\]](#) I remember that CursedScreech had a function to phish Windows credentials with Powershell, this was back when I was testing WiFi Pineapples. Here's the original post on hak5's forum: <https://forums.hak5.org/topic/37759-official-cursedscreech/>

Once you have credentials you can use PsExec to execute a program on the remote LAN machine. +1 once you have credentials from others users around a network wmiexec, or simple pssession works fine, Psexec you will denote that on some networks it's not going to happen. You can easily get credentials using various methods from responder to booby trapped pdf's and documents which will retrieve a "file" from you smb server.

ApexLead - August 20, 2018, 11:09 pm

(Aug 20, 2018 09:01 AM)Nick (Name) Wrote: [\[CITE\]](#) I remember that CursedScreech had a function to phish Windows credentials with Powershell, this was back when I was testing WiFi Pineapples. Here's the original post on hak5's forum: <https://forums.hak5.org/topic/37759-official-cursedscreech/>

Once you have credentials you can use PsExec to execute a program on the remote LAN machine. Thanks, I'll have a look :)

(Aug 20, 2018 06:44 PM)last viking Wrote: [\[CITE\]](#) you can use mimikatz and spread on lan using psExec

another method is to arp spoof and redirecting him

To download the payload this kind of attacks are very noisy and not stable

PSEXEC only works if passwords similar or same

(Aug 20, 2018 07:31 PM)SilentWatch Wrote: [\[CITE\]](#) +1 once you have credentials from others users around a network wmiexec, or simple pssession works fine, PSEXEC you will denote that on some networks it's not going to happen. You can easily get credentials using various methods from responder to booby trapped pdf's and documents which will retrieve a "file" from you smb server.

Thanks guys, but can you please elaborate or direct me to how the methods work? I mean I know PSEXEC but how exactly can I use it to spread, and Ive heard about the responder method but don't really know how to do it.. If you can elaborate a bit more I'll be more than happy :)

CyberStrike - August 20, 2018, 11:48 pm

(Aug 20, 2018 11:09 PM)ApexLead Wrote: [\[CITE\]](#) Thanks, I'll have a look :)

Thanks guys, but can you please elaborate or direct me to how the methods work? I mean I know PSEXEC but how exactly can I use it to spread, and Ive heard about the responder method but don't really know how to do it.. If you can elaborate a bit more I'll be more than happy :)

Well assuming that there is an actual network smb/AD even netbios it basically runs a fake server for each of those services, Windows likes to authenticate to anything pretty much, so after capturing of credentials we will have a hash value, now mind you we may not have to crack it why? Because we need to pass the hash, windows accepts hashes of the passwords for credentials. So now PSEXEC/pssession/wmiexec we can run remote commands on machines where we have credentials, maybe they can download a file from our local server or from the internet, from there same program we execute remotely. For example we get an admin account be it domain admin or something along those lines those credentials have access to pretty much every box. Or say that we get credentials for a user who their machine is part of the IT staff or another OU (Organizational Unit) where we can now infect several machines including a multihomed endpoint, so we now are pivoting and moving to the next subnet.

<https://www.ntsossecure.com/pwning-with-responder-a-pentesters-guide/>

ApexLead - August 20, 2018, 11:54 pm

(Aug 20, 2018 11:48 PM)SilentWatch Wrote: [\[CITE\]](#) Well assuming that there is an actual network smb/AD even netbios it basically runs a fake server for each of those services, Windows likes to authenticate to anything pretty much, so after capturing of credentials we will have a hash value, now mind you we may not have to crack it why? Because we need to pass the hash, windows accepts hashes of the passwords for credentials. So now PSEXEC/pssession/wmiexec we can run remote commands on machines where we have credentials, maybe they can download a file from our local server or from the internet, from there same program we execute remotely. For example we get an admin account be it domain admin or something along those lines those credentials have access to pretty much every box. Or say that we get credentials for a user who their machine is part of the IT staff or another OU (Organizational Unit) where we can now infect several machines including a multihomed endpoint, so we now are pivoting and moving to the next subnet.

<https://www.ntsossecure.com/pwning-with-responder-a-pentesters-guide/>

Thanks, that makes me understand it better.

I still have a question tho, say we have control over the first machine, where do I put the responder? I need to activate it on this machine?

CyberStrike - August 21, 2018, 12:21 am

(Aug 20, 2018 11:54 PM)ApexLead Wrote: [\[CITE\]](#) Thanks, that makes me understand it better.

I still have a question tho, say we have control over the first machine, where do I put the responder? I need to activate it on this machine?

Well I should be rather clear you are to pivot on that first compromised machine, in metasploit run a socks4a proxy and add the route, you can also do this manually basically run a proxy and add the compromised machine in the route. Now you will use proxychains (of course configured to run with that socks4a proxy in metasploit) to use responder on your machine using the route you added to route traffic back and forth. If you want to upload tools onto a compromised machine that works too for example say we grab up some credentials well let's start building infrastructure within the target network, we can pretty quickly have say 1 c2 using powershell (poshc2) which can deal with other compromised machines say uploading further tools onto other machines, or maybe executing commands on compromised machines.

Generally within a network I follow these basic principals, for every one machine with tools and designated as an "attack" machine I will have 3 machines which are compromised and just forwarding traffic to the next target, no tools nothing just forwarding. This is so if an admin sees some attacks they focus on the machines with no tools it hides what I am doing, hiding an "attack" machine with tools. Also having 100's of machines going out to the internet will raise some flags, so that is where the c2 comes into play I can have maybe 5 machines hitting my c2 on a vps and grabbing a payload from there distributing to other machines on the network. Let's say that I need to exfiltrate a bunch of data .. that's fine, but I break it up onto other machines so if say I have 500 megs that are going out each machine gets maybe 200 megs of that so then if discovered it isn't all lost. Main thing to think about it how not to burn your infrastructure inside of a compromised network or on the internet, so you must always think worst case scenario.

Read parts 1 and 2 also

<https://www.trustwave.com/Resources/SpiderLabs-Blog/Responder-2-0---Owning-Windows-Networks-part-3/>

I did a Windows Post exploitation tutorial and Active Directory "hunting" btw, it covers

<https://hackforums.net/showthread.php?tid=5732104>

Windows Information gathering, this is important to understand the environment you are working in. (pivots are covered here and setting up redirects to hide attacks within the network)

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

(I have a privilege escalation thread and the same on Linux and somewhat on OSX (I need to work on finishing the last OSX guide).