HACKTHEBOX

INTRO TO NETWORK TRAFFIC ANALYSIS

CHEAT SHEET

Cheat Sheet

Keep in mind, unless you are utilizing root, `sudo` privileges will be required to execute any applications that need to bind a network interface or set it into promiscuous mode.

Nomachine Connection Information

- Target IP == 10.129.43.4
- Username == htb-student
- Password == HTB_@cademy_stdnt!

Tcpdump

Command	Description
`tcpdump --version`	Prints the tcpdump and libpcap version strings then exits.
`tcpdump -h`	Prints the help and usage information.
`tcpdump -D`	Prints a list of usable network interfaces from which tcpdump can capture.
`tcpdump -i (interface name or #)`	Executes tcpdump and utilizes the interface specified to capture on.
`tcpdump -i (int) -w file.pcap`	Runs a capture on the specified interface and writes the output to a file.

Command	Description
`tcpdump -r file.pcap`	TCPDump will read the output from a specified file.
`tcpdump -r/-w file.pcap -l | grep 'string'`	TCPDump will utilize the capture traffic from a live capture or a file and set stdout as line-buffered. We can then utilize pipe (|) to send that output to other tools such as grep to look for strings or specific patterns.
`tcpdump -i (int) host (ip)`	TCPDump will start a capture on the interface specified at (int) and will only capture traffic originating from or destined to the IP address or hostname specified after `host`.
`tcpdump -i (int) port (#)`	Will filter the capture for anything sourcing from or destined to port (#) and discard the rest.
`tcpdump -i (int) proto (#)`	Will filter the capture for any protocol traffic matching the (#). For example, (6) would filter for any TCP traffic and discard the rest.
`tcpdump -i (int) (proto name)`	Will utilize a protocols common name to filter the traffic captured. TCP/UDP/ICMP as examples.

Tcpdump Common Switches and Filters

Switch/Filter	Description
`D`	Will display any interfaces available to capture from.
`i`	Selects an interface to capture from. ex. -i eth0
`n`	Do not resolve hostnames.
`nn`	Do not resolve hostnames or well-known ports.
`e`	Will grab the ethernet header along with upper-layer data.
`X`	Show Contents of packets in hex and ASCII.
`XX`	Same as X, but will also specify ethernet headers. (like using Xe)

Switch/Filter	Description
`v, vv, vvv`	Increase the verbosity of output shown and saved.
`c`	Grab a specific number of packets, then quit the program.
`s`	Defines how much of a packet to grab.
`S`	change relative sequence numbers in the capture display to absolute sequence numbers. (13248765839 instead of 101)
`q`	Print less protocol information.
`r file.pcap`	Read from a file.
`w file.pcap`	Write into a file
`host`	Host will filter visible traffic to show anything involving the designated host. Bi-directional
`src / dest`	`src` and `dest` are modifiers. We can use them to designate a source or destination host or port.
`net`	`net` will show us any traffic sourcing from or destined to the network designated. It uses / notation.
`proto`	will filter for a specific protocol type. (ether, TCP, UDP, and ICMP as examples)
`port`	`port` is bi-directional. It will show any traffic with the specified port as the source or destination.
`portrange`	`Portrange` allows us to specify a range of ports. (0-1024)
`less / greater "< >"`	`less` and `greater` can be used to look for a packet or protocol option of a specific size.
`and / &&`	`and` `&&` can be used to concatenate two different filters together. for example, src host AND port.
`or`	`or` Or allows for a match on either of two conditions. It does not have to meet both. It can be tricky.

HTB ACADEMY CHEATSHEET

Switch/Filter	Description
`not`	`not` is a modifier saying anything but x. For example, not UDP.

TShark

Command	Description
`tshark -h`	Prints the help menu.
`tshark -D`	List available interfaces to capture from.
`tshark -i (int)`	Capture on a selected interface. Replace (int) with the interface name or number.
`tshark -i eth0 -f "host (ip)"`	apply a filter with (-f) looking for a specific host while utilizing tshark
`D`	Will display any interfaces available to capture from and then exit out.
`L`	Will list the Link-layer mediums you can capture from and then exit out. (ethernet as an example)
`i`	choose an interface to capture from. (-i eth0)
`f`	packet filter in libpcap syntax. Used during capture.
`c`	Grab a specific number of packets, then quit the program. Defines a stop condition.
`a`	Defines an autostop condition. It can be after a duration, specific file size, or after a certain number of packets.
`r (pcap-file)`	Read from a file.
`W (pcap-file)`	Write into a file using the pcapng format.
`P`	Will print the packet summary while writing into a file (-W)

Command	Description
`x`	will add Hex and ASCII output into the capture.
`h`	See the help menu

WireShark

Capture Filter	Description
`host x.x.x.x`	Capture only traffic pertaining to a certain host
`net x.x.x.x/24`	Capture traffic to or from a specific network (using slash notation to specify the mask)
`src/dst net x.x.x.x/24`	Using src or dst net will only capture traffic sourcing from the specified network or destined to the target network
`port #`	will filter out all traffic except the port you specify
`not`	will capture everything except the variable specified. ex. `not port 80`
`and`	AND will concatenate your specified ports. ex. `host 192.168.1.1 and port 80`
`portrange x-x`	Portrange will grab traffic from all ports within the range only
`ip / ether / tcp`	These filters will only grab traffic from specified protocol headers.
`broadcast / multicast / unicast`	Grabs a specific type of traffic. one to one, one to many, or one to all.

Display Filter	Description
`ip.addr == x.x.x.x`	Capture only traffic pertaining to a certain host. This is an OR statement.
`ip.addr == x.x.x.x/24`	Capture traffic pertaining to a specific network. This is an OR statement.

HTB ACADEMY CHEATSHEET

Display Filter	Description
`ip.src/dst == x.x.x.x`	Capture traffic to or from a specific host.
`dns / tcp / ftp / arp / ip`	filter traffic by a specific protocol. There are many more options.
`tcp.port == x`	filter by a specific tcp port.
`src.port / dst.port ==x`	will capture everything except the port specified.
`and / or / not`	AND will concatenate, OR will find either of two options, NOT will exclude your input option.
`tcp.stream eq #`	Allows us to follow a tcp session in which we captured the entire stream. Replace (#) with the session to reassemble.
`http`	Will filter for any traffic matching the http protocol.
`http && image-jfif`	This filter will display any packet with a jpeg image file.
`ftp`	Filters for the ftp protocol.
`ftp.request.command`	Will filter for any control commands sent over ftp control channel.
`ftp-data`	Will show any objects transfered over ftp.

Misc Commands

Command	Description
`sudo *`	Sudo will run the command that proceeds it with elevated privileges.
`which (application)`	Utilizes which to determine if (application) is installed on the host. Replace the application with what you are looking for. ex. `which tcpdump`

HTB ACADEMY CHEATSHEET

Command	Description
`sudo apt install (application)`	Uses elevated privileges to install an application package if it does not exist on the host. ex. `sudo apt install wireshark`
`man (application)`	Displays the manual pages for an application. ex. `man tcpdump`.

Common Ports and Protocols

Port Number	Protocol	Description
20	FTP-Data	Data channel for passing FTP files.
21	FTP-Command	Control channel for issuing commands to an FTP server.
22	SSH	Secure Shell Service port. Provides secure remote communications
23	Telnet	Telnet service provides cleartext communications between hosts.
25	SMTP	Simple Mail Transfer protocol. Utilized for email transmissions between servers.
53	DNS	Domain Name Services. Provides name resolution with multiple protocols
69	TFTP	Trivial File Transfer Protocol. A lightweight, minimal-function transfer protocol.
80	HTTP	HyperText Transfer Protocol. Provides dynamic web services
88	Kerberos	Providing cryptographic network authentication
110	POP3	Mail service utilized by clients to retrieve email from a server.
111	RPC	Remote Procedure Call. Remote service for managing network file systems.

HTB ACADEMY CHEATSHEET

Port Number	Protocol	Description
115	SFTP	SSH File Transfer Protocol. An extension of SSH providing secure and reliable FTP services.
123	NTP	Network Time Protocol. Provides timing and sync services for network devices.
137	Netbios-NS	Local network name resolution.
139	Netbios-SSN	Provides session services for data transfer. Services like SMB can utilize it.
179	BGP	Border Gateway Protocol. BGP is a protocol for exchanging routing info with autonomous systems worldwide.
389	LDAP	Lightweight Directory Access Protocol. System agnostic authentication and authorization services.
443	HTTPS	HyperText Transfer Protocol Secure. An extension of HTTP utilizing SSL/TLS for encrypting the communications.
445	SMB	Server Message Block. SMB allows for the sharing of services, files, networking ports, and printers between hosts.

HTB ACADEMY CHEATSHEET