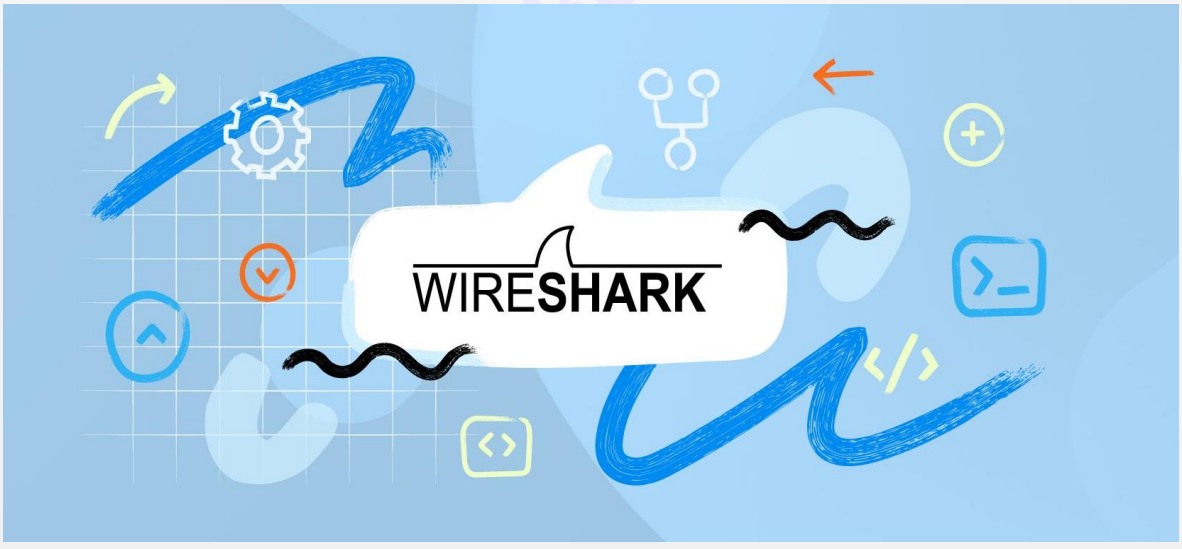
Cyber Public School

WIRESHARK CHEAT SHEET

https://cyberpublicschool.com/

WIRESHARK CHEAT SHEET



WIRESHARK cheat sheet

Wireshark cheat sheet

Here's a cheat sheet for using Wireshark:

1. **Starting a capture:**
   - Open Wireshark and select the interface you want to capture on.
   - Click on the "Start" button to begin capturing packets.

2. **Display Filters:**
   - Use display filters to focus on specific packets or protocols.
   - To apply a display filter, enter it in the filter bar at the top of the Wireshark window.

3. **Packet List Pane:**
   - The packet list pane shows a summary of each captured packet.
   - You can click on a packet to see more detailed information in the packet details pane.

4. **Packet Details Pane:**
   - The packet details pane shows the full details of a selected packet.
   - You can expand each section to see more information about the packet.

5. **Follow TCP Stream:**
   - The "Follow TCP Stream" feature allows you to view the full contents of a TCP session.
   - Right-click on a TCP packet and select "Follow TCP Stream" to view the session.

WIRESHARK cheat sheet

6. **Coloring Rules:**
- Coloring rules allow you to customize how packets are displayed in the packet list.
- You can create rules based on criteria such as protocol, source/destination IP address, or packet length.

7. **Exporting Packets:**
- You can export captured packets to a variety of file formats.
- Go to "File" > "Export" to export packets in a specific format.

8. **Statistics:**
- Wireshark provides a variety of statistics for analyzing captured packets.
- Go to "Statistics" in the menu bar to view statistics such as packet length distribution, protocol hierarchy, and more.

9. **Filter Expressions:**
- Wireshark allows you to create complex filter expressions using logical operators such as "and", "or", and "not".
- Use the "Apply" button to apply a filter expression to the current capture.

10. **Expert Info:**
- Wireshark provides "Expert Info" messages to highlight potential issues with captured packets.
- Look for messages in the packet details pane that indicate issues such as retransmissions or TCP checksum errors.

WIRESHARK cheat sheet

Wireshark tool

Wireshark is a network protocol analyzer tool that allows you to capture and analyze network traffic in real-time or from a saved capture file. It is open-source software and is available for free on multiple platforms such as Windows, macOS, and Linux.

With Wireshark, you can analyze network traffic at the packet level and gain insights into the network's behavior, protocols, and potential issues. Wireshark supports hundreds of protocols and provides detailed information about each packet's contents, including the protocol used, source and destination IP addresses, and much more.

Wireshark also provides advanced features such as filter expressions, which allows you to filter out specific packets and focus on the ones that matter. It also provides statistics and graphs to help you visualize and understand network traffic patterns.

Wireshark is widely used by network administrators, security professionals, and developers to troubleshoot network issues, monitor network performance, and detect potential security threats.

WIRESHARK cheat sheet

Wireshark Nmap command

Wireshark and Nmap are two different tools that serve different purposes, but they can be used together to perform network analysis and security testing. Here are some basic commands for using Wireshark and Nmap:

Wireshark:

Starting a capture: sudo wireshark
This command starts Wireshark with root privileges, allowing you to capture packets on all interfaces.

Capturing packets on a specific interface: sudo wireshark -i interface_name
This command starts Wireshark and captures packets only on the specified interface.

Displaying a specific protocol: http
This command will display only the HTTP packets in the packet list.

Filtering packets by IP address: ip.addr == IP_address
This command will filter and display only packets with the specified IP address.

WIRESHARK cheat sheet

Nmap:

Scanning a single host: nmap target_IP
This command will scan a single host and display information about open ports and services.

Scanning multiple hosts: nmap target_IP1 target_IP2
This command will scan multiple hosts and display information about open ports and services on each host.

Scanning a range of IP addresses: nmap IP_range
This command will scan a range of IP addresses and display information about open ports and services on each host.

Scanning specific ports: nmap -p port_number target_IP
This command will scan a specific port on a target host and display information about the service running on that port.

Note: It is important to use these tools responsibly and in compliance with applicable laws and regulations.

WIRESHARK cheat sheet

wire shark nmap command with example

Wireshark and Nmap are two different tools that serve different purposes, but they can be used together to perform network analysis and security testing. Here are some examples of using Wireshark and Nmap together:

1. Using Nmap to scan for open ports on a target host:

Syntax: nmap -p 1-65535 target_IP

Example: nmap -p 1-65535 192.168.1.100

This command will scan all ports on the target host (192.168.1.100) and display information about open ports and services.

2. Using Wireshark to capture network traffic during an Nmap scan:

Syntax: sudo wireshark -i interface_name

Example: sudo wireshark -i eth0

This command will start Wireshark and capture packets on the specified interface (eth0). During an Nmap scan, you can use Wireshark to capture and analyze network traffic to gain insights into the network's behavior and potential issues.

3. Using Nmap to perform a stealth scan and avoid detection:

Syntax: nmap -sS target_IP

Example: nmap -sS 192.168.1.100

4. This command will perform a TCP SYN scan (stealth scan) on the target host (192.168.1.100) to avoid detection by the target's firewall or intrusion detection system (IDS).

Using Wireshark to analyze Nmap scan results:
After performing an Nmap scan, you can use Wireshark to analyze the captured packets and gain insights into the network's behavior and potential issues. For example, you can use Wireshark to filter and display packets that match specific criteria, such as packets with a specific protocol, source or destination IP address, or port number. You can also use Wireshark to create graphs and statistics to help you visualize and understand network traffic patterns.

WIRESHARK cheat sheet

enum4linux wire shark command

Enum4linux is a tool used for enumerating information from Windows and Samba systems. Wireshark is a network protocol analyzer tool that allows you to capture and analyze network traffic in real-time or from a saved capture file. Here are some examples of using enum4linux and Wireshark together:

1. Using enum4linux to enumerate information from a target host:

Syntax: enum4linux -a target_IP

Example: enum4linux -a 192.168.1.100

This command will enumerate information from the target host (192.168.1.100) and display information about users, shares, policies, and more.

2. Using Wireshark to capture network traffic during an enum4linux scan:

Syntax: sudo wireshark -i interface_name

Example: sudo wireshark -i eth0

This command will start Wireshark and capture packets on the specified interface (eth0). During an enum4linux scan, you can use Wireshark to capture and analyze network traffic to gain insights into the network's behavior and potential issues.

3. Using Wireshark to filter and display packets related to Samba protocol:

Syntax: smb

Example: smb

This command will filter and display only the Samba protocol packets in the packet list. This is useful when analyzing the network traffic during an enum4linux scan, as it allows you to focus on the Samba-related packets and gain insights into the Samba configuration and vulnerabilities.

Note: It is important to use these tools responsibly and in compliance with applicable laws and regulations.

WIRESHARK cheat sheet

wire shark enum4linux command with example

Enum4linux is a tool used for enumerating information from Windows and Samba systems. Wireshark is a network protocol analyzer tool that allows you to capture and analyze network traffic in real-time or from a saved capture file. Here's an example of using enum4linux and Wireshark together:

1. Using enum4linux to enumerate information from a target host:

Syntax: enum4linux -a target_IP

Example: enum4linux -a 192.168.1.100

This command will enumerate information from the target host (192.168.1.100) and display information about users, shares, policies, and more.

2. Using Wireshark to capture network traffic during an enum4linux scan:

Syntax: sudo wireshark -i interface_name

Example: sudo wireshark -i eth0

This command will start Wireshark and capture packets on the specified interface (eth0). During an enum4linux scan, you can use Wireshark to capture and analyze network traffic to gain insights into the network's behavior and potential issues.

3. Using Wireshark to filter and display packets related to the SMB protocol:

Syntax: smb

Example: smb

This command will filter and display only the SMB protocol packets in the packet list. This is useful when analyzing the network traffic during an enum4linux scan, as it allows you to focus on the SMB-related packets and gain insights into the Samba configuration and vulnerabilities.

4. Using Wireshark to display the authentication process during an enum4linux scan:

Syntax: smb.auth.username == username || smb.auth.password == password

Example: smb.auth.username == admin || smb.auth.password == P@ssw0rd

This command will filter and display only the SMB packets related to the authentication process for the specified username and password. This is useful when analyzing the network traffic during an enum4linux scan, as it allows you to gain insights into the authentication process and potential vulnerabilities.

Note: It is important to use these tools responsibly and in compliance with applicable laws and regulations.

WIRESHARK cheat sheet

wireshark command filter

Wireshark allows you to filter captured network traffic based on various criteria such as protocol, IP address, port number, and more. Here are some examples of Wireshark filter commands:

1. Displaying HTTP traffic only:

Syntax: http

Example: http

This command will filter and display only the HTTP packets in the packet list.

2. Displaying traffic to or from a specific IP address:

Syntax: ip.addr == target_IP

Example: ip.addr == 192.168.1.100

This command will filter and display only the packets to or from the specified IP address (192.168.1.100).

3. Displaying traffic to a specific port number:

Syntax: tcp.port == target_port

Example: tcp.port == 80

This command will filter and display only the TCP packets to the specified port number (80).

WIRESHARK cheat sheet

4. Displaying traffic containing a specific keyword:

Syntax: frame contains keyword

Example: frame contains login

This command will filter and display only the packets containing the specified keyword (login) in the packet list.

5. Displaying traffic using logical operators:

Syntax: filter1 && filter2

Example: tcp.port == 80 && ip.addr == 192.168.1.100

This command will filter and display only the TCP packets to port 80 and from IP address 192.168.1.100.

Note: Wireshark filters are case-insensitive and can be combined using logical operators such as && (AND), || (OR), and ! (NOT). Also, it is important to use Wireshark responsibly and in compliance with applicable laws and regulations.

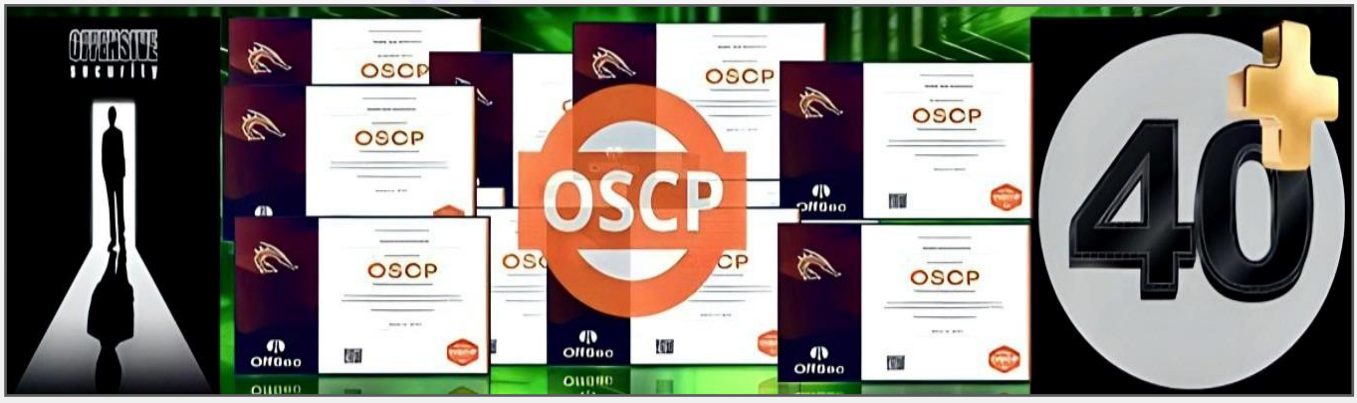
WIRESHARK cheat sheet

Contacts us

https://cyberpublicschool.com/

https://www.instagram.com/cyberpublicschool/

Phone no.: +91 9631750498 India
+61 424866396 Australia



Our Successful Oscp Student.