CYBER SECURITY WORKSHOP

19 June 2024

Introduction to Kali Linux

- What is Kali Linux?
- Why Use Kali Linux?
- Key Features of Kali Linux
- Popular Kali Linux Tools - Nmap
- Popular Kali Linux Tools - Metasploit Framework
- Popular Kali Linux Tools - Wireshark

What is Kali Linux?

- Open-source Linux distribution
- Developed and maintained by Offensive Security
- Designed for penetration testing and security auditing
- Pre-loaded with a vast arsenal of security tools
- Free to download and use

Why Use Kali Linux?

- Wide range of pre-installed security tools
- User-friendly interface for experienced users
- Extensive documentation and community support
- Regularly updated with the latest security tools
- Free and open-source software

Key Features of Kali Linux

- Extensive collection of security tools (over 600!)
- Pre-configured environments for specific tasks
- Comprehensive package management system
- Rolling release model for continuous updates
- Regular penetration testing tools updates

Popular Kali Linux Tools - Nmap

- Open-source network scanner
- Used for network exploration and security auditing
- Identifies hosts and services on a network
- Detects open ports and operating systems
- Can be used for vulnerability scanning

Popular Kali Linux Tools - Metasploit Framework

- Open-source penetration testing framework
- Extensive collection of exploits, payloads, and encoders
- Allows for simulating real-world attacks
- Valuable for identifying and exploiting vulnerabilities
- Can be used to test the effectiveness of security controls

Popular Kali Linux Tools - Wireshark

- Powerful network protocol analyzer
- Captures and analyzes network traffic
- Identifies protocols, ports, and data content
- Used for troubleshooting network issues
- Valuable for security investigations

Introduction to Wireshark

- Select the network interface for capturing traffic
- Choose the capture filter (optional)
- Start the capture process
- Stop the capture process when desired

Capturing Traffic with Wireshark

- Select the network interface for capturing traffic
- Choose the capture filter (optional)
- Start the capture process
- Stop the capture process when desired

Analyzing Captured Packets in Wireshark

- Packet list pane: Displays a chronological list of captured packets
- Packet details pane: Provides detailed information about the selected packet
- Dissection pane: Decodes the packet based on its protocol layers
- Data pane: Displays the raw data content of the packet

THANK YOU

Q & A

Thank you.