CSCI 400-1

Wireless Penetration Testing

Presented by Group 8: Folusho Adeoti, Arif Ahmed, Josue Nunez

Wireless Penetration Testing

Overview

Wireless Penetration Testing

Introduction

Penetration testing is the set of techniques used by authorized practitioners to exploit vulnerabilities to determine whether unauthorized access or other malicious activity is possible

The aim of this project is to preform penetration testing in a wireless network. We will perform packet sniffing to capture sensitive data, and Packet analysis to extract important information like IP addresses, MAC addresses and others, as well as Denial of Service attacks to disrupt network connectivity.

Wireless Penetration Testing

Benefits

Identifying Vulnerabilities - Penetration testing helps identify weaknesses in systems, networks, and applications before attackers can exploit them.

Risk Mitigation - By uncovering vulnerabilities, penetration testing enables organizations to asses and prioritize risks effectively. They can implement appropriate security controls and measures to mitigate these risks and strengthen their overall cybersecurity posture.

Testing Incident Response Plans - Testing can simulate real-world cyber attacks, which allows organizations to test their incident response plans and procedures. This helps them identify gaps in response capabilities and ensure that they are well prepared in responding to security incidents.

Wireless Penetration Testing

The Phases

Reconnaissance

The gathering information and preparation phase

Gaining Access

Exploit the vulnerabilities found during scanning to gain access to the system

Scanning

The phase in which we use tools and techniques to discover vulnerabilities within the target system

Analysis/Report

Evaluate the findings, and document every detailed finding. The documentation usually includes technical risks, any vulnerabilities that were found, and how they were found.

Wireless Penetration Testing

Attacks

Deauthentication

This attack is a type of Denial of Service (Dos) attack that will disrupt the connectivity of the network by sending deauthentication frames to the client, causing legitimate users to disconnect from the wireless network.

Packet Sniffing

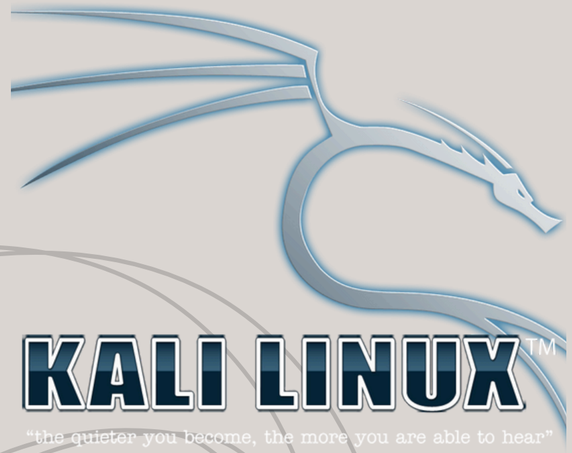
This attack captures network traffic to inspect the data packets being transmitted over the wireless network. This is done to identify sensitive information, such as usernames, passwords, or other confidential data.

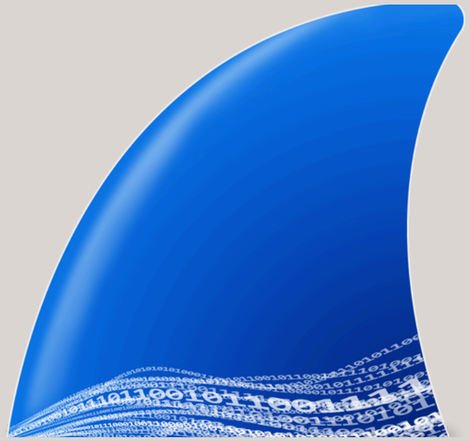
Packet Analysis

This attack analyzes the captured network packets to extract important information like users IP addresses, their MAC addresses, the protocols used, and other network characteristics.

Wireless Penetration Testing

Hardware/Tools



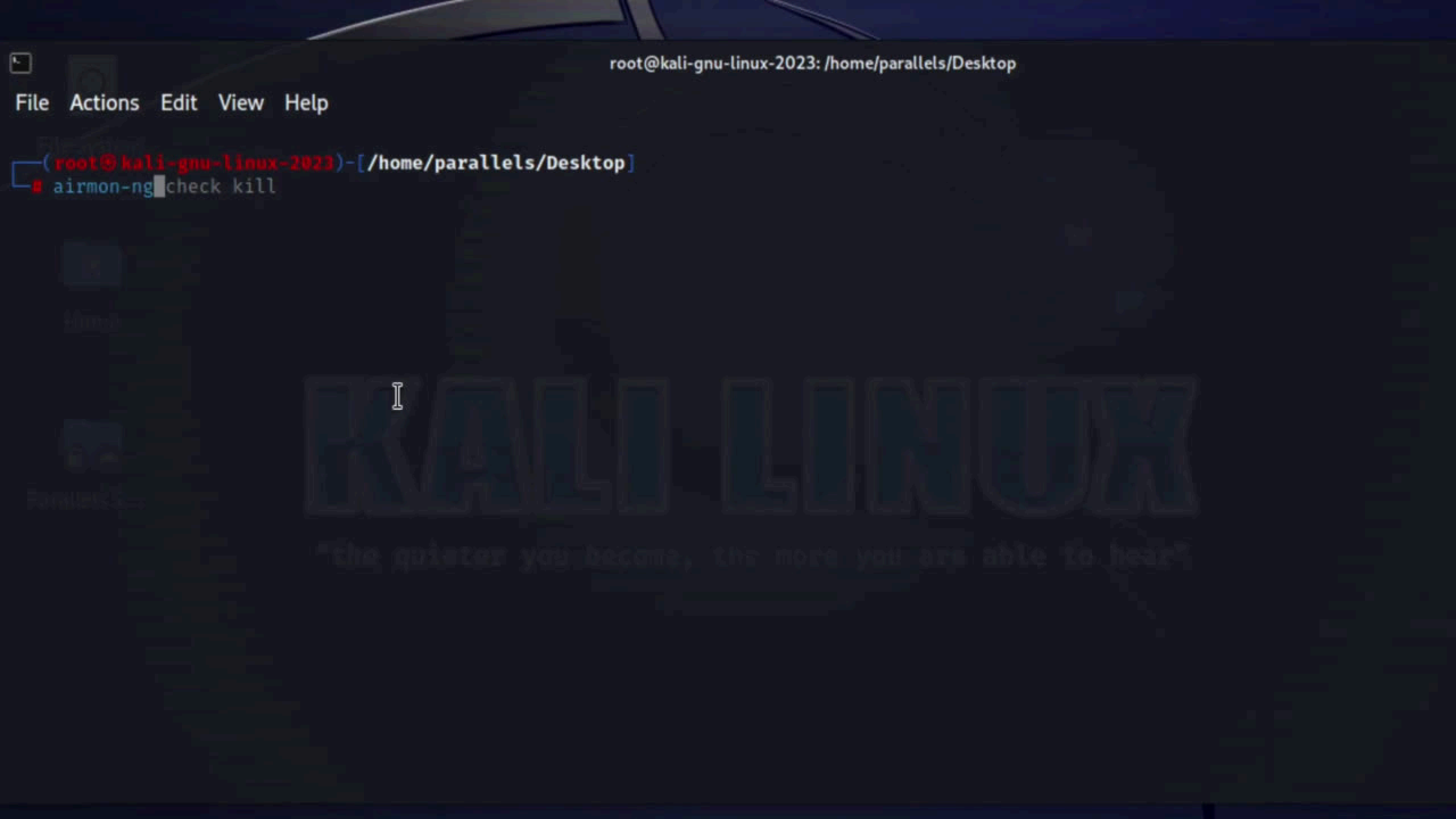


- Wireless USB WiFi Adapter
- Kali Linux Virtual Machine
- Wireshark
- Aircrack-ng

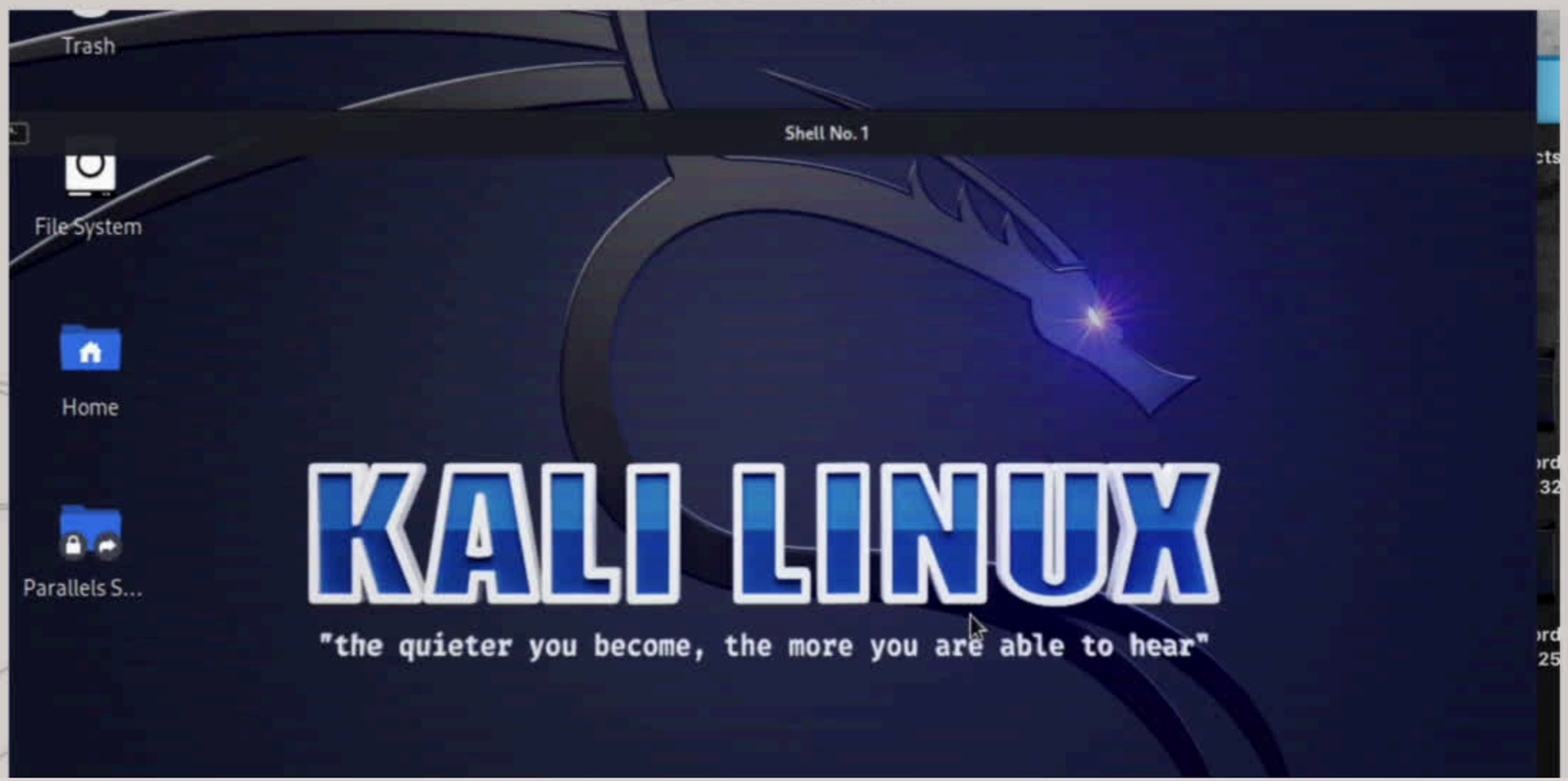
Demonstrations

Turn on monitor mode using the

Run as root


root@kali-gnu-linux-2023: /home/parallels/Desktop
File Actions Edit View Help
┌──(root㉿kali-gnu-linux-2023)-[/home/parallels/Desktop]
└─# airmon-ng check kill
KALI-LINUX
"the quieter you become, the more you are able to hear"

Conecting to a eth interface via terminal/wireshark on kali linux, followed by the nMap command on the terminal



Wireless Penetration Testing

Proposed Solution

Deauthentication Attack

- Deploying wireless intrusion detection and prevention systems (WIDS/WIPS) to detect and mitigate deauthentication attacks.
- Configuring wireless access points to detect and block excessive deauthentication frames or implement rate limiting to prevent flooding attacks
- Network logs should be monitored for suspicious activity and any unauthorized deauthentication attempts should be investigated promptly

Wireless Penetration Testing

Proposed Solution

Packet Sniffing

- Encrypting protocols such as WPA2 (WiFi Protected Access 2) with AES (Advanced Encryption Standard) encryption should be implemented. Those protocols will encrypt data packets transmitted over the network.
- Use secure communication protocols such as HTTPS for web browsing and SSH (Secure Shell) for remote access to prevent sensitive information from being transmitted in plaintext.

Wireless Penetration Testing

Proposed Solution

Packet Analysis

- Network traffic should be monitored regularly using intrusion detection systems (IDS) or intrusion prevention systems (IPS) to detect abnormal or suspicious behavior.

- Encrypt sensitive data transmitted over the network to prevent unauthorized access to plaintext information.

- Implementation network segmentation and access controls to limit the exposure of critical systems and data.

Real World Examples

The Equifax Data Breach

In 2017, Equifax (One of the largest consumer credit reporting agencies) had a data breach that exposed the personal information of 143 million individuals.

Equifax hired a third party vendor to conduct a penetration test on its systems, however the vendor failed to identify a critical vulnerability in their web application framework, which allowed attackers to abuse this vulnerability and gain access to the company's data.

If the vendor had conducted a more through test, this vulnerability would have been identified and patched before the attackers ever had a chance to find and abuse it. It's extremely important to not cut any corners when conducting these tests, for the consequences can be significant.

Real World Examples

The Canadian Cybersecurity Breach

In 2019, the Canadian Government experienced a cybersecurity breach that compromised the personal information of over nine thousand people. The breach was caused by a vulnerability in the online portal for people searching for employment.

The government hired penetration testers to identify these vulnerabilities and patch them. They identified several vulnerabilities that could have been exploited by attackers to gain access to the governments sensitive data.

The penetration testers allowed the Canadian government to identify and address these vulnerabilities before any further attacks occur. They not only patched the already existing vulnerability but managed to find addition ones that the government was not aware of. These tests helped the government improve its cybersecurity posture and mitigate risk.

Problems and Difficulties

- Bluetooth interface commands like hcitool and hciconfig were not working as intended. Problem suspected to be with virtual machine used, or the host computer itself. After using a different virtual machine and an older version of kali linux, bluetooth interface began to work as intended.

- Purchasing a WIFI adapter that was not compatible with Kali Linux.

Wireless Penetration Testing

Conclusion

Our testing using these techniques highlighted the vulnerabilities present in wireless networks. Through our research we've identified several effective solutions that will mitigate risk. By integrating these solutions into our network infrastructure and maintaining a proactive security posture, we can strengthen our defenses and safeguard against any potential breaches coming our way.

Wireless Penetration Testing

Thank You

Presented by Group 8: Folusho Adeoti, Arif Ahmed, Josue Nunez