WEEK 6 DAY 1

MUHAMMAD BILAL

CONTENT

INTRODUCTION TO NETWORK PACKET SNIFFING

- WIRESHARK AND PACKET CAPTURE BASICS
- ANALYZING CAPTURED PACKETS
- PACKET FILTERING AND DISPLAY OPTIONS
- ADVANCED PROTOCOL ANALYSIS
- PACKET DECRYPTION TECHNIQUES
- CAPTURING AND ANALYZING SSL/TLS TRAFFIC
- SNIFFING ON WIRELESS NETWORKS
- SNIFFING ON SWITCHED NETWORKS

INTRODUCTION TO NETWORK PACKET SNIFFING

INTRODUCTION TO NETWORK PACKET SNIFFING

DEFINITION:

NETWORK PACKET SNIFFING IS THE PROCESS OF CAPTURING AND ANALYZING DATA PACKETS AS THEY TRAVEL ACROSS A NETWORK. THIS ALLOWS NETWORK ADMINISTRATORS OR SECURITY PROFESSIONALS TO MONITOR NETWORK TRAFFIC, TROUBLESHOOT ISSUES, AND DETECT MALICIOUS ACTIVITY.

EXAMPLES:

1:A NETWORK ADMINISTRATOR USES A PACKET SNIFFER TO MONITOR TRAFFIC ON A CORPORATE NETWORK, IDENTIFYING ABNORMAL TRAFFIC PATTERNS THAT COULD INDICATE A DDOS ATTACK.

2:A SECURITY ANALYST CAPTURES AND ANALYZES PACKETS TO DETECT DATA EXFILTRATION ATTEMPTS WHERE SENSITIVE DATA IS BEING SENT OUT OF THE NETWORK TO AN UNAUTHORIZED EXTERNAL SERVER.

TECHNIQUES AND TOOLS:

TOOLS: WIRESHARK, TCPDUMP, NETWORKMINER.

WEBSITES: [WIRESHARK OFFICIAL SITE](HTTPS://WWW.WIRESHARK.ORG/), [TCPDUMP/LIBPCAP](HTTPS://WWW.TCPDUMP.ORG/).

LEGAL AND ETHICAL ASPECTS OF SNIFFING

DEFINITION

PACKET SNIFFING RAISES LEGAL AND ETHICAL CONCERNS BECAUSE IT INVOLVES MONITORING NETWORK TRAFFIC, WHICH CAN INCLUDE SENSITIVE OR PRIVATE INFORMATION. UNAUTHORIZED SNIFFING CAN LEAD TO PRIVACY VIOLATIONS AND LEGAL REPERCUSSIONS.

EXAMPLES:

1: AN EMPLOYEE USES A PACKET SNIFFER TO CAPTURE LOGIN CREDENTIALS OF THEIR COLLEAGUES WITHOUT PERMISSION, VIOLATING PRIVACY LAWS AND COMPANY POLICIES.

2: A NETWORK ADMINISTRATOR LEGALLY MONITORS NETWORK TRAFFIC TO ENSURE COMPLIANCE WITH COMPANY SECURITY POLICIES, ENSURING THAT SENSITIVE INFORMATION IS NOT LEAKED.

TECHNIQUES AND TOOLS

GUIDANCE DOCUMENTS:
ETHICAL HACKING GUIDELINES, CORPORATE IT POLICIES.

WEBSITES: [EFF (ELECTRONIC FRONTIER FOUNDATION)](HTTPS://WWW.EFF.ORG/), [CISSP](HTTPS://WWW.ISC2.ORG/CERTIFICATIONS/CISSP).

WIRESHARK AND PACKET CAPTURE BASICS

WIRESHARK AND PACKET CAPTURE BASICS

DEFINITION

WIRESHARK IS A POPULAR NETWORK PROTOCOL ANALYZER USED TO CAPTURE AND INTERACTIVELY BROWSE THE TRAFFIC RUNNING ON A COMPUTER NETWORK. IT PROVIDES DETAILED INFORMATION ABOUT EACH PACKET CAPTURED, SUCH AS PROTOCOL TYPE, SOURCE, AND DESTINATION.

EXAMPLES

1: A NETWORK TECHNICIAN USES WIRESHARK TO CAPTURE PACKETS AND DIAGNOSE A NETWORK LATENCY ISSUE BY IDENTIFYING A LARGE NUMBER OF RETRANSMISSIONS.

2: A CYBERSECURITY PROFESSIONAL USES WIRESHARK TO CAPTURE AND ANALYZE PACKETS FROM A COMPROMISED MACHINE TO IDENTIFY THE TYPE OF MALWARE COMMUNICATING WITH A COMMAND-AND-CONTROL SERVER.

TECHNIQUES AND TOOLS

TOOLS:WIRESHARK, TSHARK (COMMAND-LINE VERSION OF WIRESHARK).

WEBSITES:

[WIRESHARK OFFICIAL SITE](HTTPS://WWW.WIRESHARK.ORG/), [WIRESHARK Q&A](HTTPS://ASK.WIRESHARK.ORG/).

ANALYZING CAPTURED PACKETS

ANALYZING CAPTURED PACKETS

DEFINITION

ANALYZING CAPTURED PACKETS INVOLVES EXAMINING THE DETAILS OF THE PACKETS CAPTURED DURING SNIFFING TO UNDERSTAND THE DATA BEING TRANSMITTED, IDENTIFY POTENTIAL SECURITY THREATS, OR TROUBLESHOOT NETWORK ISSUES.

EXAMPLES

1: ANALYZING HTTP PACKETS TO IDENTIFY SENSITIVE INFORMATION BEING TRANSMITTED IN PLAINTEXT, SUCH AS LOGIN CREDENTIALS, WHICH SHOULD BE SECURED USING HTTPS.
2: INSPECTING DNS PACKETS TO IDENTIFY SIGNS OF DNS SPOOFING, WHERE A MALICIOUS ACTOR IS REDIRECTING TRAFFIC TO A FRAUDULENT WEBSITE.

TECHNIQUES AND TOOLS

LOREM IPSUM DOLOR SIT AMET, CONSECTETUR ADIPISCING
TOOLS: WIRESHARK, ZEEK (FORMERLY BRO), NETWORKMINER.
WEBSITES:
[WIRESHARK OFFICIAL SITE](HTTPS://WWW.WIRESHARK.ORG/),
[ZEEK](HTTPS://ZEEK.ORG/).
ELIT, SED DO EIUSMOD TEMPOR INCIDIDUNT UT LABORE ET DOLORE MAGNA ALIQUA. UT ENIM AD MINIM VENIAM,

PACKET FILTERING AND DISPLAY OPTIONS

PACKET FILTERING AND DISPLAY OPTIONS

DEFINITION:

PACKET FILTERING ALLOWS USERS TO ISOLATE SPECIFIC PACKETS OF INTEREST FROM A LARGE CAPTURE FILE BASED ON CRITERIA SUCH AS IP ADDRESS, PROTOCOL, PORT NUMBER, OR PAYLOAD CONTENT. DISPLAY OPTIONS IN TOOLS LIKE WIRESHARK ALLOW FOR EASIER ANALYSIS BY HIGHLIGHTING OR FOCUSING ON RELEVANT DATA.

EXAMPLES:

1: USING A DISPLAY FILTER IN WIRESHARK TO SHOW ONLY HTTP TRAFFIC TO ANALYZE WEB ACTIVITY.

2: FILTERING PACKETS BY IP ADDRESS TO FOCUS ON TRAFFIC BETWEEN A PARTICULAR HOST AND AN EXTERNAL SERVER SUSPECTED OF MALICIOUS ACTIVITY.

TECHNIQUES AND TOOLS:

TOOLS: WIRESHARK, TCPDUMP (WITH FILTERS), IPTABLES (FOR REAL-TIME PACKET FILTERING).

WEBSITES: [WIRESHARK FILTER SYNTAX] (HTTPS://WWW.WIRESHARK.ORG/DOCS/DFREF/), [TCPDUMP EXAMPLES] (HTTPS://HACKERTARGET.COM/TCPDUMP-EXAMPLES/).

ADVANCED PROTOCOL ANALYSIS

DEFINITION:

ADVANCED PROTOCOL ANALYSIS INVOLVES A DEEPER EXAMINATION OF NETWORK PROTOCOLS BEYOND THE BASIC ANALYSIS, INCLUDING UNDERSTANDING PROTOCOL BEHAVIORS, DETECTING ANOMALIES, AND ANALYZING ENCRYPTED OR PROPRIETARY PROTOCOLS.

EXAMPLES:

1: ANALYZING SSL/TLS HANDSHAKE PACKETS TO ENSURE PROPER ENCRYPTION PROTOCOLS ARE USED AND TO IDENTIFY ANY ANOMALIES THAT COULD INDICATE A MAN-IN-THE-MIDDLE ATTACK.

2: EXAMINING VOIP (VOICE OVER IP) TRAFFIC TO IDENTIFY ISSUES SUCH AS JITTER, LATENCY, OR PACKET LOSS THAT COULD AFFECT CALL QUALITY.

TECHNIQUES AND TOOLS:

TOOLS: WIRESHARK, ZEEK, ETTERCAP (FOR ANALYZING AND MANIPULATING NETWORK PROTOCOLS).

WEBSITES: [WIRESHARK WIKI](HTTPS://WIKI.WIRESHARK.ORG/), [ZEEK DOCUMENTATION](HTTPS://DOCS.ZEEK.ORG/EN/CURRENT/).

PACKET DECRYPTION TECHNIQUES

DEFINITION:

PACKET DECRYPTION TECHNIQUES INVOLVE DECRYPTING ENCRYPTED NETWORK TRAFFIC TO ANALYZE THE CONTENTS FOR SECURITY OR TROUBLESHOOTING PURPOSES. THIS REQUIRES ACCESS TO THE ENCRYPTION KEYS OR EXPLOITING WEAKNESSES IN THE ENCRYPTION PROTOCOL.

EXAMPLES:

1: DECRYPTING SSL/TLS TRAFFIC BY IMPORTING THE SERVER'S PRIVATE KEY INTO WIRESHARK, ALLOWING FULL VISIBILITY INTO HTTPS TRAFFIC.

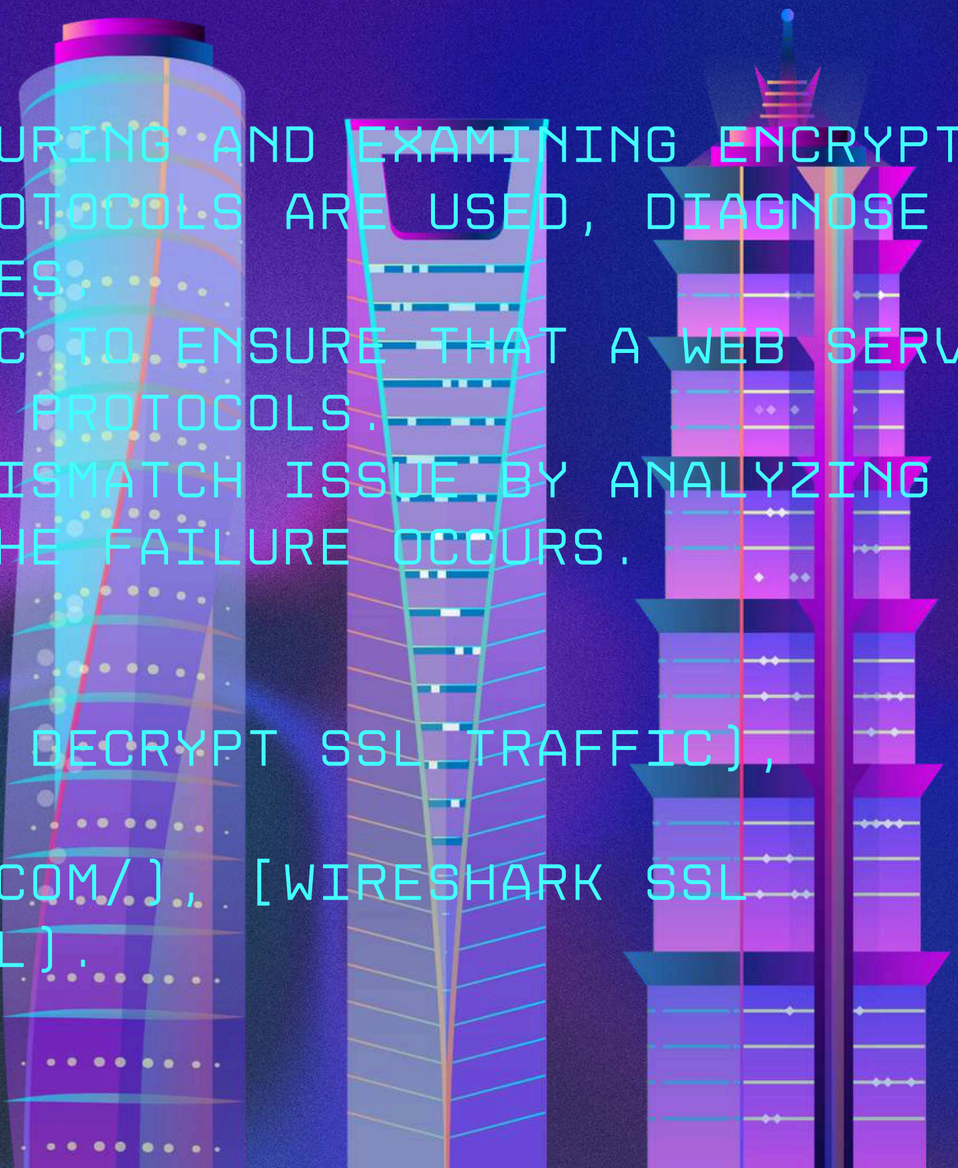
2: USING BRUTE-FORCE OR DICTIONARY ATTACKS TO DECRYPT WEAKLY ENCRYPTED WI-FI TRAFFIC CAPTURED OVER A WPA NETWORK.

TECHNIQUES AND TOOLS:

TOOLS: WIRESHARK (WITH KEYS), AIRCRACK-NG (FOR WI-FI DECRYPTION), OPENSSL (FOR SSL/TLS DECRYPTION).

WEBSITES: [WIRESHARK DECRYPTION](HTTPS://WIKI.WIRESHARK.ORG/SSL), [AIRCRACK-NG](HTTPS://WWW.AIRCRACK-NG.ORG/).

CAPTURING AND ANALYZING SSL/TLS TRAFFIC



DEFINITION:

SSL/TLS TRAFFIC ANALYSIS INVOLVES CAPTURING AND EXAMINING ENCRYPTED TRAFFIC TO ENSURE SECURE COMMUNICATION PROTOCOLS ARE USED, DIAGNOSE ISSUES, OR DETECT POTENTIAL VULNERABILITIES.

1: CAPTURING AND ANALYZING SSL/TLS TRAFFIC TO ENSURE THAT A WEB SERVER IS USING UP-TO-DATE AND SECURE ENCRYPTION PROTOCOLS.

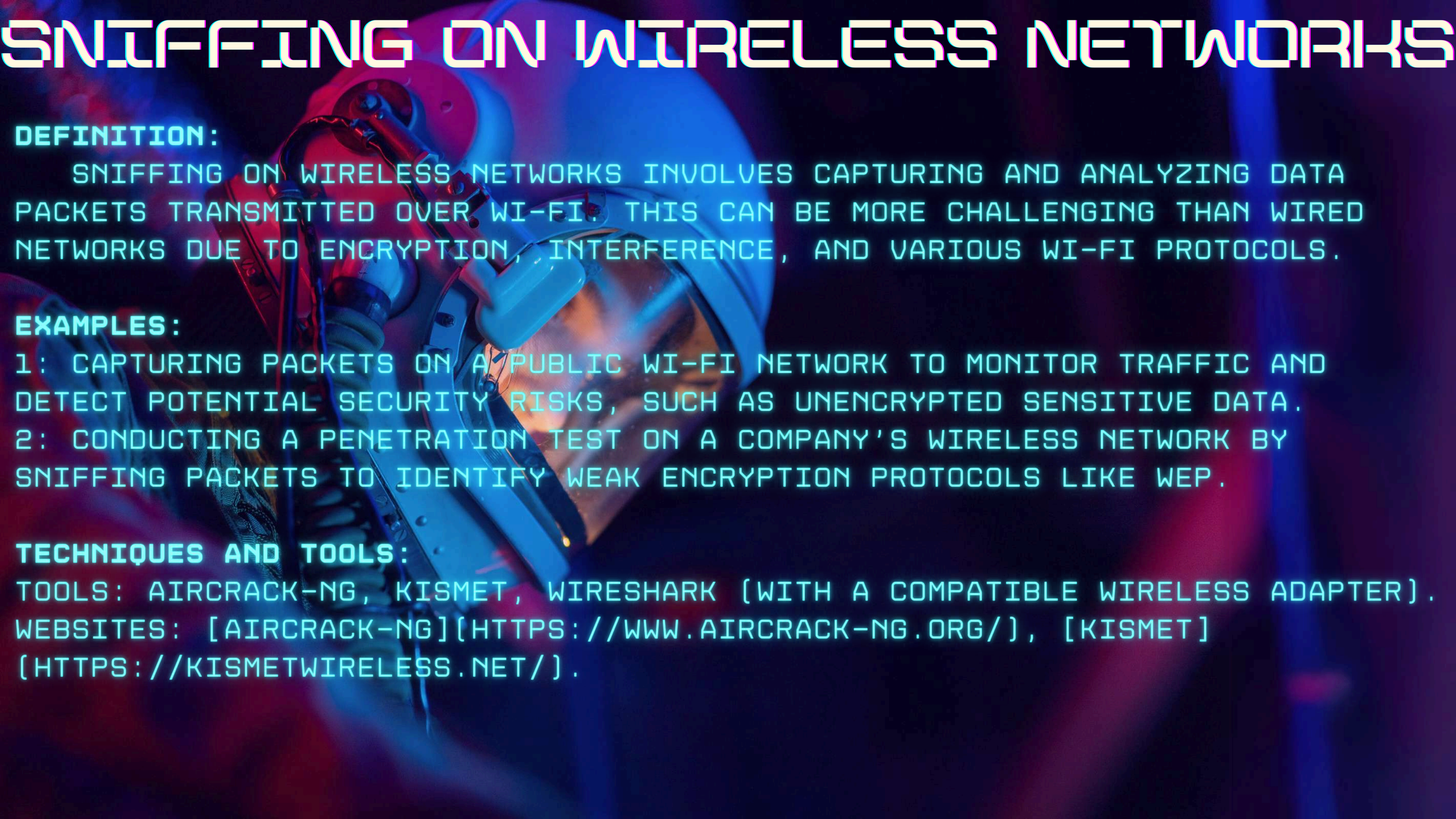
2: INVESTIGATING AN SSL/TLS CERTIFICATE MISMATCH ISSUE BY ANALYZING THE HANDSHAKE PROCESS TO IDENTIFY WHERE THE FAILURE OCCURS.

TECHNIQUES AND TOOLS:

TOOLS: WIRESHARK, SSLDUMP (TO CAPTURE AND DECRYPT SSL TRAFFIC), OPENSSL.

WEBSITES: [SSL LABS](HTTPS://WWW.SSLLABS.COM/), [WIRESHARK SSL DECRYPTION](HTTPS://WIKI.WIRESHARK.ORG/SSL).

SNIFFING ON WIRELESS NETWORKS



DEFINITION:

SNIFFING ON WIRELESS NETWORKS INVOLVES CAPTURING AND ANALYZING DATA PACKETS TRANSMITTED OVER WI-FI. THIS CAN BE MORE CHALLENGING THAN WIRED NETWORKS DUE TO ENCRYPTION, INTERFERENCE, AND VARIOUS WI-FI PROTOCOLS.

EXAMPLES:

1: CAPTURING PACKETS ON A PUBLIC WI-FI NETWORK TO MONITOR TRAFFIC AND DETECT POTENTIAL SECURITY RISKS, SUCH AS UNENCRYPTED SENSITIVE DATA.
2: CONDUCTING A PENETRATION TEST ON A COMPANY'S WIRELESS NETWORK BY SNIFFING PACKETS TO IDENTIFY WEAK ENCRYPTION PROTOCOLS LIKE WEP.

TECHNIQUES AND TOOLS:

TOOLS: AIRCRACK-NG, KISMET, WIRESHARK (WITH A COMPATIBLE WIRELESS ADAPTER).
WEBSITES: [AIRCRACK-NG](HTTPS://WWW.AIRCRACK-NG.ORG/), [KISMET](HTTPS://KISMETWIRELESS.NET/).

SNIFFING ON SWITCHED NETWORKS

DEFINITION:

SNIFFING ON SWITCHED NETWORKS IS MORE CHALLENGING THAN ON HUBS BECAUSE SWITCHES DIRECT TRAFFIC TO SPECIFIC PORTS, MAKING IT HARDER TO CAPTURE PACKETS NOT ADDRESSED TO THE SNIFFER'S PORT. TECHNIQUES LIKE ARP SPOOFING OR PORT MIRRORING ARE OFTEN USED TO CAPTURE TRAFFIC IN SUCH ENVIRONMENTS.

1. USING ARP SPOOFING TO TRICK A SWITCH INTO SENDING TRAFFIC TO THE ATTACKER'S MACHINE, ALLOWING THE CAPTURE OF SENSITIVE DATA SUCH AS LOGIN CREDENTIALS.
2. CONFIGURING PORT MIRRORING ON A NETWORK SWITCH TO SEND ALL TRAFFIC TO A SPECIFIC PORT WHERE IT CAN BE CAPTURED AND ANALYZED BY WIRESHARK.

TECHNIQUES AND TOOLS:

TOOLS: ETTERCAP (FOR ARP SPOOFING), WIRESHARK (WITH PORT MIRRORING), CAIN & ABEL.

WEBSITES: [ETTERCAP](HTTPS://WWW.ETTERCAP-PROJECT.ORG/), [WIRESHARK WIKI](HTTPS://WIKI.WIRESHARK.ORG/CAPTURESETUP/ETHERNET).


HAPPY HACKING
MUHAMMAD BILAL