Chapter 8
Protecting Against Social Engineering Using Wireshark: Effective Strategies With Real-World Examples

Manvi Mishra
SRMS College of Engineering and Technology, Bareilly, India

Md Shadab Hussain
SRMS College of Engineering and Technology, Bareilly, India

Sudheer Kumar Singh
Galgotias University, Noida, India

ABSTRACT

In the domain of cybersecurity, defending against social engineering attacks remains a critical challenge. This abstract explores effective strategies and real-world examples of using Wireshark—a powerful network protocol analyzer—to mitigate the risks posed by social engineering tactics. Social engineering attacks exploit human psychology rather than technical vulnerabilities, making them difficult to detect through conventional security measures alone. This chapter delves into various strategies for leveraging Wireshark in defense against social engineering. Key aspects include configuring Wireshark for optimal security monitoring, setting up filters and profiles to capture relevant traffic, and decrypting SSL/TLS communications to uncover malicious intent hidden within encrypted data. Detection techniques encompass monitoring DNS and HTTP traffic for signs of phishing attempts, identifying malware communications, and conducting behavioral analysis to spot

DOI: 10.4018/979-8-3693-6665-3.ch008

anomalies in network behavior

I. INTRODUCTION

Social engineering attacks use psychology to trick people into sharing sensitive information or compromising security. Unlike technical hacking, these attacks rely on manipulation and persuasion (Abu and Eleyan, 2023). Tactics include phishing, where fake emails deceive victims; spear phishing, which customizes messages for specific targets; vishing, using phone calls for data extraction; and smishing, deceptive text messages. These attacks bypass technical defenses by exploiting human vulnerabilities, highlighting the need for awareness and training to combat these threats effectively. Social engineering attacks might trick a user into clicking on a link that downloads malware onto their computer. Conversely, malware can facilitate social engineering by providing attackers with access to personal information or enabling them to control compromised systems (Sobur et al, 2023).

One of the biggest dangers in cybersecurity is malware, also called malicious software. Malware is made to sneak into, harm, or stop computers, networks, and the information they have. Cybercriminals use many types of harmful software, like viruses, worms, Trojan horses, ransomware, and spyware. Each type of malware does something different bad. Viruses and worms can mess up files and spread by themselves. Trojans pretend to be real software to get illegal access. Ransomware locks up important data and asks for money to unlock it. Spyware quietly watches what users do and takes important info.

Malware is a serious problem because it can lead to data breaches, money lost, and stop work from getting done. To fight these attacks, good cybersecurity strategies are a must. This includes using strong antivirus and anti-malware software, keeping systems updated to fix problems, and using firewalls to block unwanted access. Teaching people to spot fake emails (phishing) and not download suspicious stuff is also really important. Adding extra protections like backing up data often, using strong passwords, and checking identities in more than one way can help a lot. As malware gets tricky, it’s crucial to use smart cybersecurity plans to keep info safe and keep computer systems working well. To overcome this problem an opensource tool wireshark is used (Tuli, 2023).

Wireshark is a powerful tool used to detect malware by analyzing network traffic. It captures data packets in real-time, allowing experts to examine details of transmitted information. By studying this data, suspicious patterns that might indicate malware can be identified. Wireshark also analyzes packet payloads, where malware signatures may hide (Yusuf at al, 2024). It checks communication protocols for any unusual activity that could be caused by malware. If there's a sudden increase in