Markitnus Morris

Katherine winters

Principles of information and security

4 September 2021

Assignment 2

. 1.

What is shoulder surfing and how can you protect against shoulder surfing?

a) Shoulder surfing is a model of a societal engineering method; used in cybersecurity to collect secrets about the individual.Thinsg such as identification numbers, passwords, and other private data are collected by peering over the victim's shoulder.

b) Researchers concentrate on assessing the shoulder surfing attack (SSA) susceptibility. We find empirical shoulder surfing research that meet a subset characteristics. We provide an analysis approach for the SSA experimental procedure predicated on the architectural attributes retrieved from the trials.Designers want to simplify and normalize testing procedures by demonstrating their influence on the original study outcomes, and to develop criteria for a more unbiased design of shoulder surfing research through extensive analysis.

https://www.sciencedirect.com/science/article/pii/S0167404820302960

A "shoulder-surfing" attack can compromise picture-based password schemes. A novel technique is presented that hides as much information about the login entities as feasible. Modern technology techniques seek to mitigate this risk by asking users to input their credentials explicitly by executing specific mental activities in order to generate the secondary password, therefore hiding the user's true password. However, accessibility and privacy concerns are introduced by flaws in the placement of experiment and passcode items. The right password seems to be arbitrary and could only be deduced using the entire collection of user account features.

https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4058474/

In a lab trial with 20 individuals, they were requested to shoulder surf between two PassfacesTM setups (mouse versus keypad information input) as well as complex and poor credentials. The susceptibility of the four authenticating network implementations to shoulder-surfing, as well as research participants' opinions of the same risk, were obtained. Further research looked at the link between research volunteers' actual and subjective shoulder-surfing success, as well as how the four identity verification setups were vulnerable to shoulder-surfing in any way.

https://dl.acm.org/doi/10.1145/1143120.1143128

2)

Packet sniffer questions.

A) What is a packet sniffer and how does it work?

A packet sniffer, also known as a packet analyzer, or networks procedure scanner, is a device that monitors system communications using technology or algorithms. Sniffers analyze ethernet frame patterns that move between systems on a channel, as well as between network infrastructures and the broader Web.

B) A tool commonly used as a packet sniffer is Wireshark. Go to https://en.wikipedia.org/wiki/Wireshark

C) Read the information and answer these questions:

i. Do you to have a wired connection to the network to use Wireshark?

YES

ii. Name and describe 3 features of Wireshark.

This is frequently the greatest tool for debugging network difficulties. Dropped packets, latency difficulties, and malicious network activity are all common issues that Wireshark may help you address. Thorough examination of thousands of protocols, for what's getting implemented all the time, realtime captures, offsite evaluation, and a typical three particle viewer for multi-platforms which are somemore of its capabilities.

iii. What does promiscuous mode mean?

Promiscuous mode is a configuration for a wired switch port or local wireless regulator in internet protocol that enables the device to send any traffic it obtains to the central processor unit instead of only the packets it is expressly intended to accept.

3.

One of the major avenues that hackers use to infiltrate a system is through a buffer overflow. The glossary in the back of the book defines a buffer overflow as “An application error that occurs when more data is sent to a program than it is designed to handle.” Use the Internet to research buffer overflows (There is an excellent explanation at https://searchsecurity.techtarget.com/definition/buffer-overflow#:~:text=A%20buffer%20overflow%20occurs%20when,buffer%20is%20allocated%20to%20hold.&text=If%20the%20excess%20data%20is,overwrites%20any%20data%20held%20there)

Do the following:

A) Using the textbook definition as a beginning, provide a comprehensive definition of a buffer overflow.

> A buffer overflow, also known as a buffer overload, happens when a fixed-length buffer is filled with more information than it can manage. The additional data, which must be stored someplace, might overflow into neighboring internal memory, damaging or resetting the data stored there.

B) Describe how a buffer overflow works.

> Whenever the amounts of information surpasses the ram buffer's internal storage, a buffer overflow develops. As a consequence, the application seeking to send information to the reservoir overwrites storage regions close to the buffer. All forms of technology can be affected by system vulnerabilities.

C) Describe how is a hacker can use a buffer overflow for an attack?

> Buffer overflowing have a significant sensitivity rating because they can culminate in illegal executable code; if an attacker has access of the overflowed memory area beyond the intended buffer and can reroute a functional reference to their malicious software.

D) Cite your sources

https://www.csoonline.com/article/3513477/what-is-a-buffer-overflow-and-how-hackers-exploit-these-vulnerabilities.html#:~:text=Buffer%20overflow%20attack%20examples,pointer%20to%20their%20malicious%20code.

https://resources.infosecinstitute.com/topic/ethical-hacking-buffer-overflow/

4.

For this portion of the assignment, you will be investigating the threats and attacks discussed in chapter 2. Use the internet to search for specifics on three different threats or attacks that are mentioned in the chapter. For each of the threats or attack, provide the name of the threat, details on how it works and the source of the information.

A) Financial Fraud

Computer fraud is a type of cybercrime that involves utilizing a computer to steal or manipulate digital information, as well as gaining unauthorized access to a computer or system. Cracking into electronic networks in order to get unauthorized access to personal data such as credit card details or Social Security numbers. As banks begin to adapt their procedures to the changing face of financial crime, they are confronted with the growing link between cybercrime and virtually all forms of financial crime. The cyber aspect isn't entirely new. Until recently, for instance, the majority of fraud was transactional, with criminals leveraging control flaws. Banks combat this type of fraud using simple, stream, point-based restrictions.

https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/financial-crime-and-fraud-in-the-age-of-cybersecurity

B) Password Sniffing

Password sniffing is a cyber method that employs a specific software program that permits a hacker to acquire login details by covertly monitoring network data and analyzing it. This is common on public Wireless connections, wherein poor or unsecured communication is relatively easy to intrude on.

https://cyberhoot.com/cybrary/password-sniffing/#:~:text=Password%20Sniffing%20is%20a%20hacking,on%20weak%20or%20unencrypted%20traffic.

C) Denial of service

A denial-of-service type of cyber in which the offender attempts to render a computer or network resource inaccessible to its target purposes by interrupting functionality of a hosts linked to the Web for a period of time or forever.

https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos#:~:text=A%20Denial%2Dof%2DService%20(,information%20that%20triggers%20a%20crash.&text=Buffer%20overflow%20attacks%20%E2%80%93%20the%20most%20common%20DoS%20attack.