ASSIGNMENT 1

EHA 361

NOVEMBER 9, 2024

Pieter Johannes Swart

Table of Contents

Section A:

Question 1:

1.1 Xfce is a lightweight, open-source desktop environment designed for UNIX-like operating systems. Created to be fast and efficient, it provides a basic yet practical visual layout that is popular in different Linux distributions, particularly on devices with restricted resources.

It comes with important utilities such as the Xfce terminal, known for its speed and ability to be personalized. Ethical hackers use terminals extensively to operate command-line tools such as Nmap, Metasploit, and Wireshark.

- **Penetration Testing Environments**: Several ethical hacking systems, like Parrot OS and certain versions of Kali Linux, provide Xfce as a choice. The low resource usage of Xfce enables hackers to operate several virtual machines for conducting penetration testing simulations.
- **Development and automation of scripts**: Ethical hackers can easily alternate between terminal windows, IDEs, and browser tabs on Xfce, enhancing productivity during script writing and testing.
- **Monitoring network and system**: Xfce allows monitoring tools to run efficiently with other applications, allowing ethical hackers to observe network traffic or system performance in real time without causing any system slowdown.

1.2 Zone Walking is a method employed in ethical hacking and penetration testing to collect data on a target's domain through exploiting vulnerabilities in the Domain Name System (DNS). It focuses on DNS zones and the format of domain names in order to reveal subdomains, servers, and other domain-related data.

Ethical hackers use Zone Walking to discover subdomains and IP addresses linked to a target domain. This data is essential for preparing thorough tests or attacks, as it aids in pinpointing possible access points. Ethical hackers can identify vulnerable systems in a network by understanding the unique layout of a domain and its corresponding records.

Zone Walking lead to examining the DNS namespace of a specific target in order to collect details about the domain structure. This could expose subdomains, mail servers, and other domain resources that are typically not easily reachable or publicly promoted. It is frequently utilized during the reconnaissance stage in penetration testing to identify the target's network and understand its layout.

Question 2:

2.1 Buffers are commonly used to store data, such as user input or file contents, temporarily in memory. If a program fails to check the size of incoming data and that data exceeds the allocated buffer size, it can lead to a buffer overflow.

When an overflow occurs, the excess data may overwrite critical areas in memory, including return addresses, function pointers, or other control structures. This can allow attackers to inject and execute malicious code by manipulating the overwritten memory locations.

Types of Buffer Overflows:

Stack-based Buffer Overflow: Happens when too much data is written to a local variable on the stack in the stack memory. This can write over the return address, which could result in code execution.

Heap-based Buffer Overflow: happens in heap memory, utilized for dynamically allocated data. In this case, excess data could overwrite different elements in the heap, leading to unforeseen actions or vulnerability.

Example:

- The 1988 Morris Worm exploited a stack buffer overflow in the fingerd program to spread across UNIX systems. This attack overwrote the return address to execute injected code.

- In Adobe Flash Player, a heap-based buffer overflow vulnerability allowed attackers to exploit the application and execute arbitrary code by tricking Flash into loading a malicious SWF file. This type of overflow typically corrupts metadata in the heap, leading to code execution.

- In WU-FTPD (a UNIX FTP daemon), a format string vulnerability was exploited by using specially crafted input that triggered a buffer overflow, allowing attackers to execute code with elevated privileges.

- The OpenSSH 3.4 vulnerability exploited an off-by-one overflow, allowing attackers to execute code remotely on affected systems.

Section B:

Question 3:

3.1

Vertical escalation and horizontal escalation are two methods of privilege escalation used in hacking and penetration testing to achieve unauthorized access or elevate privileges on a system. Both techniques allow malicious actors to exceed their intended permissions, but vary in their strategy and desired level of access.

	Vertical Privilege Escalation	**Horizontal Privilege Escalation**
Definition	Vertical escalation, also called privilege escalation, happens when a user or attacker attains higher-level privileges beyond their initial authorization. In this scenario, the assailant progresses "up" the permission ladder, frequently aiming to acquire administrative or root-level privileges.	Horizontal escalation, also referred to as lateral movement, happens when a cyberattacked obtains entry to accounts or resources that are at the same privilege level as their own, but are owned by different users. In this scenario, the hacker does not acquire increased privileges but instead obtains more data or capabilities.
Purpose	The objective is to obtain enhanced access privileges that enable the attacker to carry out critical tasks like altering system settings, accessing secure information, or installing harmful programs.	The goal is frequently to collect additional information, obtain sensitive user data, or breach more accounts at the same privilege level, possibly resulting in broader attacks or chances for vertical escalation.
Examples	Taking advantage of software vulnerabilities: An attacker could exploit a software application's vulnerability to run code with administrator privileges. One possible scenario would be exploiting a buffer overflow in a privileged program to obtain root privileges.	Taking advantage of Application Vulnerabilities: In multi-user applications, weak access controls can allow attackers to exploit an IDOR (Insecure Direct Object Reference) vulnerability and access data from other users with the same level of privilege.

Comparing Vertical and Horizontal Escalation

Vertical escalation refers to the act of advancing through the privilege order to obtain greater permissions, such as transitioning from a regular user to an administrator or root user. This type of escalation usually allows for greater control over the system.

Horizontal Escalation refers to the act of accessing extra accounts or resources within the same privilege level without elevating privileges. This category primarily broadens the range of entry rather than the extent of authority.

Question 4:

The EternalBlue exploit, a widely recognized exploit and vulnerability, gained notoriety for its use in the WannaCry ransomware attack. EternalBlue exploited a flaw in Microsoft's Server Message Block (SMB) protocol, enabling hackers to run code from a remote location and obtain unauthorized entry into systems.

EternalBlue was created as a cyber weapon by the NSA and then released by the hacking group Shadow Brokers in April 2017. It became a commonly utilized vulnerability because numerous systems had not been updated to fix it, despite Microsoft issuing a security update (MS17-010) in March 2017.

Step 1: Scanning for Vulnerable Systems

-Attackers first scanned networks for machines with port 445 open (used by SMB). They looked for systems that had not applied the MS17-010 patch, making them vulnerable to EternalBlue.

-Tool Used: Tools like Nmap and Metasploit were commonly used for scanning networks to detect unpatched systems with SMBv1 enabled.

Step 2: Exploiting the SMB Vulnerability with EternalBlue

Once a vulnerable system was identified, the attacker would use EternalBlue to send maliciously crafted SMB packets. These packets exploited the vulnerability by overflowing the buffer, enabling the attacker to execute code remotely.

-Tool Used: The Metasploit Framework contained an EternalBlue module, allowing attackers to execute the exploit easily. It also allowed attackers to set up payloads that would be executed on the target machine after successful exploitation.

Step 3: Deploying the WannaCry Ransomware

-After gaining control, attackers deployed WannaCry ransomware onto the compromised systems. WannaCry encrypted files on the system, adding a .wncry extension, and demanded a Bitcoin payment for decryption.

-WannaCry had a worm-like behavior, using EternalBlue to propagate itself to other unpatched systems within the network. This rapid spread led to a global ransomware crisis.

-Tool/Technology Used: WannaCry ransomware was the primary malware payload, and it included its own spreading mechanism, making it highly effective at infecting large numbers of computers.

Step 4: Holding Data for Ransom

-After encrypting files, WannaCry displayed a ransom note demanding payment in Bitcoin. If the ransom wasn't paid, it threatened to delete the decryption key, effectively locking the files permanently.

-Technology Used: The ransom note and encryption/decryption keys were hard-coded into WannaCry, using asymmetric encryption to make decryption nearly impossible without the attacker's private key.

Tools and Technologies Used in the Attack

-*EternalBlue Exploit*: Originally a cyber-weapon from the NSA, it exploited SMBv1 to execute remote code.

-*WannaCry Ransomware*: Malware that encrypted files and demanded Bitcoin payments. WannaCry's worm-like propagation was critical to its widespread impact.

-*Metasploit Framework*: Used for network scanning, finding SMB vulnerabilities, and deploying EternalBlue in a controlled penetration testing or malicious hacking scenario.

-*Bitcoin*: Used for ransom payments due to its pseudonymous nature, making it difficult to trace the attackers.

References

Bhartiya, S., 2019. Kali Linux Ethical Hacking OS Switches to Xfce Desktop, Gets New Look and Feel. 27 Nov, pp. https://www.linux.com/news/kali-linux-ethical-hacking-os-switches-to-xfce-desktop-gets-new-look-and-feel/.

Bohacek, .., 2019. Zone-Hopping!. 10 Jan, pp. https://datatracker.ietf.org/meeting/120/materials/slides-120-dnsop-zone-hopping-a-practical-solution-to-zone-walking-00#:~:text=What%20is%20Zone%2DWalking%3F,be%20identified%20within%20a%20domain..

Both, D., 2018. 8 reasons to use the Xfce Linux desktop environment. 25 June, pp. https://opensource.com/article/18/6/xfce-desktop.

Grossman, N., 2017. EternalBlue – Everything There Is To Know. 29 Sep, pp. https://research.checkpoint.com/2017/eternalblue-everything-know/.

Kanbach, B., 2023. Subdomain enumeration with DNSSEC. 17 Jan, pp. https://blog.apnic.net/2023/01/17/subdomain-enumeration-with-dnssec/.

Mr.MG, 2023. Horizontal Privilege Escalation Attack. 17 Jul, pp. https://maulikgoti.medium.com/horizontal-privilege-escalation-attack-delete-sub-agent-accounts-pocs-824454e6183b.

Newman, L. H., 2018. The Leaked NSA Spy Tool That Hacked the World. 7 Mar, pp. https://www.wired.com/story/eternalblue-leaked-nsa-spy-tool-hacked-world/.

Rezos, 2022. Buffer Overflow Attack. 12 Sep, pp. https://owasp.org/www-community/attacks/Buffer_overflow_attack.

SentinelOne, 2019. EternalBlue Exploit: What It Is And How It Works. 27 May, pp. https://www.sentinelone.com/blog/eternalblue-nsa-developed-exploit-just-wont-die/.

Shivanandhan, M., 2023. EternalBlue Explained – An In-Depth Analysis of the Notorious Windows Flaw. 11 Sep, pp. https://www.freecodecamp.org/news/eternalblue-explained-an-analysis-of-the-windows-flaw/.

Tran, L., 2018. EternalBlue Exploit. 20 Aug, p. https://www.cs.toronto.edu/~arnold/427/18s/427_18S/indepth/EternalBlue/EternalBlue_report.pdf.

Unknown, 2018. The Morris Worm. 2 November, pp. https://www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218.

Unknown, 2023. Access control vulnerabilities and privilege escalation. 10 Feb, pp. https://portswigger.net/web-security/access-control.

Unknown, 2023. Buffer Overflow Attack. 14 Aug, pp. https://www.imperva.com/learn/application-security/buffer-overflow/.

Unknown, 2023. What are Privilege Escalations? Attacks, Understanding its Types & Mitigating Them. 29 March, pp. https://www.eccouncil.org/cybersecurity-exchange/penetration-testing/privilege-escalations-attacks/.