Whitepaper Study Questions

Samuel E Barrionuevo

Trevecca Nazarene University

ITI-4070-01: Network Security/Cryptography

Dr. Kendrix

5th March 2024

Whitepaper Study Questions

The purpose of Craig Wright's research project is to determine the attractiveness of each system to attackers (Wright, 2011). With the null hypothesis for the experiment being that there is no difference in the number of attacks on both servers, the posited claim that the experiment is testing is that one server is more attractive to attackers than another (Wright, 2011). This was evaluated by investigating the individual attackers per system, which refers to the web server and the OS (Wright, 2011). This experiment does not include the reasons that attackers prefer a specific system, but rather uses corporate web server honeypots to attract attackers to test the claim that one system is more likely to be attacked than another (Wright, 2011).

Demonstrated security of the software

In the initial test phase of the experiment, the headers of the servers were not obscured making the server and operating system information available to possible attackers. This allowed for network reconnaissance and probing to take place for attackers to gauge which server to attack. Though this specific experiment did not directly measure the security of each software, the number of attacks on the Linux and Microsoft server software could lead to claims that the server less attacked is more secure because attackers are likely to target less secure servers (Wright, 2011). Additionally, based on the project results, the claim can be made that Apache Linux servers are more secure because they are attacked by less individuals than Microsoft IIS servers (Wright, 2011). Additionally, it was found that attacks on Apache Linux servers are less intense and stop when the server identity is found which both prove the active avoidance of Linux systems (Wright, 2011). The premise that attackers are more likely to attack Microsoft IIS servers and stop attacking when the discover Linux servers can lead to the conclusion that

Microsoft IIS servers are less secure. Though this is not conclusive proof, both servers are both highly secure despite the differences in sourcing and development.

Credibility Detraction

To start, the difference in vulnerabilities used could be a variable that directly affects the results of the experiment. Though similar vulnerabilities and levels were selected, the difference in the software and therefore vulnerabilities could affect the number and levels of the attacks. Depending on the vulnerability, it could directly affect the number of attack attempts (Wright, 2011). This subtracts credibility because the vulnerabilities that are selected affect the number of attackers, leading results to be inaccurate. Additionally, botnet attacks were not tracked or determined which could skew attack results. Tracking attacks by IP address rather than attack can lead to skewed results if the botnet source was being coordinated by the same attacker. Another source of doubt can be cast when using the attack time metric to measure server attractiveness because higher attack time can be credited both the number of attackers and the difficulty of the vulnerability. The reason for higher attack time can lead it to be a misleading metric when measuring server attractiveness. Lastly, it is possible that the deployments of the servers could be skewing the attack numbers if a certain server has further vulnerabilities, this experiment would better be supported with an experiment using multiple versions of Apache Linux and Microsoft Windows servers to better test the attractiveness of the servers. These factors could lead to skewed results because they are more dependent on the server version and selected vulnerability.

Main Findings of the study

To start, it was found that the average time spent attacking the server vulnerabilities was higher on Microsoft IIS software during the first phase of the project, which is when the headers

were not obscured (Wright, 2011). It scored higher in both the medium and high vulnerability category in mean seconds and showed that attackers spend more time attacking Microsoft servers regardless of the vulnerability (Wright, 2011). Additionally, Microsoft servers scored higher on the average number of attacking hosts daily (Wright, 2011). Meaning that higher effort was spent attacking Microsoft networks, though this can be attributed to the attack difficulty, it can also show preference (Wright, 2011). Lastly, it was found that Linux servers with Apache are less attractive to attackers based on the mean attacks per day and the lowered intensity of attack against Linux servers (Wright, 2011). This leads to the conclusion that attackers will likely avoid Linux servers when the header is unobscured (Wright, 2011). Rather than leading to the conclusion that attackers are specifically attracted to windows, it is better to posit the idea that attackers shy away from Linux based systems and are more in favor of attacking other servers (Wright, 2011).

Automated and Manual attacks against Web Servers

Based on the results of the study, it can be found that the active avoidance of Apache Linux systems can point to the rise of manual attacks rather than automated attacks (Wright, 2011). This is further supported by the observance of stopped of attacks that happened against systems that were too challenging (Wright, 2011). Furthermore, it was found that automated system scans are being replaced by manual processes to gain network information to maximize success by avoiding Linux systems (Wright, 2011). This manual scanning and purposeful attack proves that manual attacks are being used to specifically target systems rather than automated attacks. Though this information can be gleaned from the test results, it must be noted that denial of service (DOS) and distributed denial of service (DDOS) attacks were blocked through Snort software to mainly test for network intrusion techniques. This causes a number of automated

attacks to be omitted from this experiment that would otherwise be present in a normal network environment.

Policies and Procedures for Web Security

When having servers that provide services to both external and internal users, it is important to properly secure access and infrastructure (Scarfone, Jansen, & Tracy, 2008). Because some servers can hold sensitive network and client information, they will face many attackers. Properly installing, configuring, maintaining, and securing the system is important (Scarfone, Jansen, & Tracy, 2008). The underlying operating system, server software, and its services must be tested, logged, monitored, and backed up (Scarfone, Jansen, & Tracy, 2008). This goes for both Windows IIS and Linux Apache servers and policies must be put in place to accomplish these objectives.

Windows IIS Security Measures

Windows Web Servers must be primarily managed by securing, updating, and patching the system, using required services, and restricting user accounts (Weaver, Weaver, & Farwood, n.d.). This can be accomplished through a few security measures. Having Windows Web Server authentication is vital for web users and even verifying anonymous users can lead to both user and server safety (Weaver, Weaver, & Farwood, n.d.). Additionally using SSL encryption and implementing access controls for specific IP addresses can allow for safe access to files and safe internet access (Weaver, Weaver, & Farwood, n.d.). Lastly, separating web servers from other critical servers can allow for isolated and safe systems (Weaver, Weaver, & Farwood, n.d.).

Linux Apache Security Measures

Apache servers also require proper hardening to ensure web security. This includes many of the same things as Windows servers. A few vital measures include hardening the OS by

downloading the code and disabling unnecessary services (Weaver, Weaver, & Farwood, n.d.). Others include dividing users into web groups made up of closely watched user accounts (Weaver, Weaver, & Farwood, n.d.). Limiting privileges and protecting administrative rights can lead to the safe deployment of a Linux Apache server (Weaver, Weaver, & Farwood, n.d.).

Operating System Analysis

Based on the research of the project, attackers are more likely to target Microsoft IIS Servers running on a Windows operating system rather than Apache web servers running on the Linux operating system (Wright, 2011). Though there is no specific evidence that points to one operating system being easier to attack than the other, the information leads to the conclusion that attackers more frequently favored attacking the Windows operating system over Linux operating systems (Wright, 2011). If it were the case that Linux servers were easier to attack, the evidence would state otherwise, so it can be posited that Windows operating systems are easier to attack. This is further supported by the fact that attackers spent more time attacking windows servers more frequently (Wright, 2011). Though the argument can be made that Linux servers had less attack time because they are easier, it can be rebutted by the more frequent attacks against Windows servers which leads to the conclusion that Windows systems are easier to attack (Wright, 2011). They were more frequently the target of directed attacks with a higher average attack time (Wright, 2011).

References

Weaver, R., Weaver, D., & Farwood, D. (n.d.). Guide to Network Defense and Countermeasures. Retrieved from https://platform.virdocs.com/read/2415359/310/#/4/2[FWWM7ASARDLRK90D3989]/6[KGJV6PPZKV6Q6HJDP392]/8[VQDMDRYYYHCVX11XC771]/4[QGFMH8YAS9YUK0Y2T828]/2[SRTCRKMVQ86EN80V5011],/1:77,/1:77

Scarfone, K., Jansen, W., & Tracy, M. (2008). Guide to general server security. NIST Special Publication, 800(123).

Wright, C. (2011). A comparative study of attacks against corporate IIS and Apache web servers21. SANS Institute