Security System Exploitation on Domains and Subdomains of UIN Syarif Hidayatullah Jakarta

Thoyyibah. T 1,*, Wasis Haryono1, Tomi Hardi 1

* Correspondence Author: e-mail: dosen01116@unpam.ac.id

1 Informatics Engineering, Computer Science Faculty, Universitas Pamulang; Jl. Raya Puspitek No. 46, Serpong, Kota Tangerang Selatan, Banten 15316, Indonesia; email: dosen01116@unpam.ac.id, wasish@unpam.ac.id, dosen01784@unpam.ac.id

Abstract

A computer is a machine that can be used to process any information. In the computer world, crime often occurs. Thus, security is needed, for computer systems to avoid various attacks. In the world of computers, especially on the Internet, virus attacks often occur, such as worms, trojans, software piracy and credit card theft problems. Despite the many offers of computer sophistication in processing information, there are still weaknesses that can be exploited by irresponsible parties. This can be detrimental to the rightful owner of the information. So that it can cause small-scale to large-scale damage. Therefore, it is very important for us to know about security exploits so that we can prevent such exploitation and avoid abuse from certain parties. Although no system is completely secure, at least we have minimized the possibility by knowing security exploits. Forms of security exploitation generally use various techniques; therefore a security system is needed that is able to overcome these forms of exploitation. This study discusses how to exploit a system and its techniques with the object used is a security system in the domain and subdomain of UIN Syarif Hidayatullah Jakarta. It is hoped that with this research the reader can know and understand the exploitation techniques used so that they can prevent or treat when this exploitation technique is used. The research method used consists of several paths, namely footprinting, scanning, DOOS, Access, Filtering, finally Covering tracks and creating a backdoor. The research output is the display of the University's network security and its exploitation process.

Keywords: Exploitation, Network, Security, University

1. Introduction

The sophistication of technology makes it easier for humans to complete activities in daily life. Because the computer is a machine that can be used to process any information to suit what we need. Then there is a need for security for computer systems in order to avoid crime events in the computer world, especially on the Internet network such as virus attacks, worms, Trojans, DoS, Web defacements, software piracy, to credit card theft problems.
Politics to use certain subjects arbitrarily for self-interest that can exploit others beyond the limits of propriety is an exploitation of security. The main target of exploitation is the control or use to dredge and exploit the potential of resources, both natural resources and human resources, as at the university level. The campus studied in this study is one of the State Universities in Banten. Where this university is the first Islamic university in Indonesia. The university is Syarif Hidayatullah State Islamic University, Jakarta. State Islamic University (UIN) is a form of state Islamic university in Indonesia that provides academic education in several scientific disciplines, including science outside Islamic studies. UIN is a form of state Islamic university in addition to the State Islamic Institute (IAIN) and the State Islamic College (STAIN).

This action causes harm to other parties, both to humans and the environment. Network security systems have the task of preventing and identifying unauthorized users on computer networks. This preventive measure serves to stop intruders from accessing through computer network systems. The solution is to improve the network security system. Because the nature of the network is to carry out two-way communication from the sender to the receiver and vice versa. So every communication sent on a computer network can be misused by irresponsible people. One other solution that needs to be known is to make sure the user is not familiar with network security issues. If they do not know about the network, then there will be potential network security holes that are easy to penetrate. So besides building a network security system, don’t forget to also educate users about network security. Despite the many offers of computer sophistication in processing information. but there are still weaknesses that can be exploited by irresponsible parties. which may harm the rightful owner of the information. that can cause small-scale to large-scale damage. Therefore, it is very important for us to know about security exploits so that we can prevent these exploitations and avoid abuse from certain parties. although no system is completely secure. at least we have minimized this possibility by knowing security exploits. Forms of security exploitation generally use various techniques, therefore a security system is needed that is able to overcome these forms of exploitation.

This study discusses how to exploit a system and its techniques with the object used is a security system in the domain and subdomain of UIN Syarif Hidayatullah Jakarta. It is hoped that with this research the reader can know and understand the exploitation techniques used so that they can prevent or treat when this exploitation technique is used. Some research and terms in security exploits such as Security Exploits use software that attacks specific security vulnerabilities but does not always aim to carry out unwanted actions. Such as penetration testing to find out system weaknesses so that it can prevent unwanted actions (Rahardjo, 2005).

2. Research Method

System exploitation method with the uinjkt.ac.id domain and subdomain, the exploitation system can be described as follows:

The security exploitation process in Figure 1 consists of several stages, according to the book Hacking Exposed 7 the process consists of the stages of Footprinting, Scanning, Enumeration & Gaining Access, Pilfering, Covering Tracks & Creating Backdoor, and Denial Distributed of Services (DDoS) (Rahardjo, 2005). Foot Printing or footprints, in security exploitation, is a process to obtain information about the target destination carried out before an attack by a hacker or cracker (Mcclure S, Scambray J, Kurtz G (2012). Scanning is scanning. Enumeration is the process of exploiting security to find more information on the system that has been scanned. Distributed Denial of Service is an attempt (in the form of an attack) to disable the target system so that the system cannot provide its services (denial of service) or the service level drops drastically (Akhir, 2020). Imagine if a bank was attacked by a rival bank by crippling an ATM outlet (Automatic Teller Machine) owned by that bank. Or a credit card merchant server that was attacked so that it cannot accept payments via credit cards (Rahardjo B, 2005). Pilfering or can be interpreted as theft, is a process where
the access rights on the target system have been controlled by hackers or crackers in full (Mcclure S, Scambray J, Kurtz G, (2012)).

Figure 1. Exploitation Method

Covering Tracks is the process of deleting traces or known as system logs by hackers or crackers after completing their goals on the system. The purpose of deleting system logs is so that users and superusers/admins on the target system do not know if the system has been entered by someone without permission (Akhir, 2020). Sniffing is an enumerating process with a sniffing or tapping technique on packets moving towards the target system or originating from the target system (M. Ferdy Adiant & Is Mardianto, 2015).

Brute Force is a method of gaining access that aims to hack the password used by trying all possible combinations in a wordlist (Pramaditya, 2016). IP Spoofing is a complex technical attack that consists of several components. This is a security exploit that works by tricking a computer into pretending someone else is using it. Several attacks that use changing the source IP Address or forging the attacker's IP so that the target assumes the attacker's IP address is the IP address of the original host not from outside the network. Simply put, IP Spoofing can be explained as a way to hide the identity of the attacker so that it is not tracked by the destination computer (Zuli et al., 2017).
3. Results and Analysis

In this study, criteria and alternative choices were used in accordance with those formulated in the background of the problem above. While the data used is data obtained from the results of questionnaires distributed to respondents. Discussion In the exploitation of the security system in the uinjkt.ac.id domain and sub domain, 2 tests will be taken, namely the uinjkt.ac.id domain and the subdomain, namely ais.uinjkt.ac.id

A). Foot Printing, In this process the initial information search is carried out using the SamSpade program installed on the Windows 10 operating system. It is known that the SamSpade program has not been able to find information about the uinjkt.ac.id or ais.uinjkt.ac.id domains, this is due to the agreement on the "id" domain. " which is in RIPE format cannot be loaded or filtered.

B). Scanning, Scanning process to look for security holes or Vulnerability of the uinjkt.ac.id and ais.uinjkt.ac.id domains using Nmap and Nikto.

a. Scanning with Nmap

From Figure 2, it is known that the scanning results show that in the uinjkt.ac.id domain there are 6 ports or entrances in open status and one port with closed status. A port with an open status is the port used by the uinjkt.ac.id system to interact with outside connections and this port can be passed by us as hackers to enter the uinjkt.ac.id system, while ports that have a closed status cannot be used as a way enter exploitation.

Source: Research Result (2023)

Figure 2. The results of port scanning using Nmap on the uin.jkt.ac.id domain
Basicall all systems must have an open port, for example, port 80 or HTTP port which is a protocol so that data can go out and enter the system. In Figure 2 it is known that the uinjkt.ac.id domain has port 21 for ftp with vsftpd version 2.0.8 or below and port 88 http with apache http server version. Knowing the version of the port we can reduce the subject of how to disable the system with that version of the port. Furthermore, scanning as many as 11 ports on the subdomain ais.uinjkt.ac.id, where there are 3 ports with filtered status. The port with filtered status is an ambiguous port because the program cannot determine whether the port is open or closed because the port itself only provides a little information from the program request, while it is known that port 80 with http service on the subdomain ais.uinjkt.ac.id runs with type nginx 1.10.2 server.

b. Scanning with Owasp ZAP

The uin.jkt.ac.id domain only has 2 weaknesses that are classified as low, and there are no high or medium weaknesses. This proves that the security in the uinjkt.ac.id domain in terms of coding to the database is very good, making it difficult to penetrate in general. There are 2 weaknesses at the intermediate level that can be used as an attack method against the subdomain. It can be seen that the attack method can be done with the "Click Jacking attack", and it can also be seen how the solution to solve the security problem is.

C). Distributed Denial of Service (DDoS) Attack, The Distributed Denial of Service (DDoS) process is generally not mandatory, because without this process an attacker can enter a target system. However, if the security system of the target is too difficult and troublesome for the attacker, the attacker can perform the DDoS process to disable the security of the target system. The DDoS process also requires an IP spoofing program so that the origin of the attack is difficult to know or trace. The DDoS programs used are Zombie DDoS attack, High Orbit Ion Cannon (HOIC), Low Orbit Ion Cannon (LOIC), DdoS.

Attacker, and for ip spoofing program using Psiphon.

a. Ip Spoofing with Platinum Hide IP, IP Spoofing explained that the attacker had changed his ip where the attacker's ip was originally 180.252.202.27 with Indonesia's location being 181.174.79.53 which was located in America.

b. Distributed Denial of Service Attack, Testing the DDoS process cannot be assumed by having to drop or make the uinjkt.ac.id domain or subdomain system out of service, but this cannot be done because to bring down a system requires a minimum of dozens of PCs/laptops as an attacker. The testing process is carried out on the ais.uinjkt.ac.id subdomain, because the uinjkt.ac.id domain is not receiving the ping request status at all or Request Time Out. The testing process can be seen by the packet transfer speed by making a ping request domain and subdomain and the status packet.
Table 1. Results of Testing Requests for ping packets before and during an attack

<table>
<thead>
<tr>
<th>Ping Time</th>
<th>Max Time</th>
<th>Min Time</th>
<th>Average Time</th>
<th>Package Status</th>
<th>Max Time</th>
<th>Min Time</th>
<th>Average Time</th>
<th>Package Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>75ms</td>
<td>5ms</td>
<td>31ms</td>
<td>100%</td>
<td>114ms</td>
<td>9ms</td>
<td>59ms</td>
<td>100%</td>
</tr>
<tr>
<td>2</td>
<td>9ms</td>
<td>5ms</td>
<td>34ms</td>
<td>100%</td>
<td>23ms</td>
<td>6ms</td>
<td>11ms</td>
<td>75%</td>
</tr>
<tr>
<td>3</td>
<td>85ms</td>
<td>5ms</td>
<td>33ms</td>
<td>100%</td>
<td>230ms</td>
<td>7ms</td>
<td>63ms</td>
<td>100%</td>
</tr>
</tbody>
</table>

Source: Research Result (2023)

From Table 1 above, it is known that there is a difference in the time received on the ping request before an attack using DDoS is carried out and when a DDoS attack is carried out where during a DDoS attack the time received tends to be longer, namely in schemes 1 and 3, in scheme 2 the time received by DDoS attacks tends to shorter because there is a failure of received ping packets (RTO) so that the number of packets received is only 75% and if the packets received are 100%, the probability of receiving time is the same as in schemes 1 and 3.

D). Enumeration & Gaining Access

In this process, a password guessing experiment is carried out with Brute Force Attack and wiretapping using Sniffing Tools. The Brute Force Attack process can be done directly without Sniffing, but usually the Attacker does Sniffing first in order to get a clue or clue to do a Brute Force Attack. Sniffing process using Cain & Abel and for Brute Force Attack using Hydra.

a. Sniffing Process

Some hosts are connected to the uinjkt.ac.id network, for example, a target with a local IP of 192.168.1.5 is determined to be intercepted of their activities. Thus, it can be seen the activities carried out by someone with a local IP 192.168.1.5, the activity is visiting social media pages, which basically can be retrieved more information about the username and password. However, the process of tapping the user ID and password cannot be done because the security system carried out by all web browsers and other web browsers is currently using HTTPS where S is Secure, so that any process that is indicated to be irregular, the browser will not carry out the work process.

b. Brute Force Attack Process

To carry out the Brute Force Attack process, we must know beforehand which port is used as the entrance of the attack, from the previous Scanning process we already know that the uinjkt.ac.id domain has port 21 with an open ftp service and a subdomain ais.uinjkt.ac.id has
port 80 with an open HTTP service. These two ports can be used as the entrance to BruteForce Attack.

It is known that the Brute Force Attack experiment for the uinjkt.ac.id domain using the FTP port did not get the appropriate password, while the experiment for the ais.uinjkt.ac.id subdomain resulted in an appropriate password and could be used to enter the ais.uinjkt.ac system. en.

E). Pilfering

In this process no testing is carried out because this process is a process of data theft, as well as system destruction, so the process at this stage depends on a person's intentions and goals when he can control and occupy the system.

F). Covering Tracks & Creating Backdoor

The Covering Tracks process is not carried out because the Pilfering process is not carried out, and for the Creating Backdoor process a Trojan exploit is used other than as an exit and re-entry door to the system, besides that Trojan exploit can also be used to monitor what the target system is doing or other processes such as accessing the system. target system from a distance.

![Trojan Exploit]

Source: Research Result (2023)

Figure 3. Trojan Exploit

The Trojan Build menu is a trojan program known as a virus, and the Start Listener is a menu that is used to exploit the target system when the Trojan application is run, in the form of monitoring, keylogger, to system access using the terminal or Command Prompt. Figure 3 is the result of monitoring the target system in the form of a screenshot of the target system, and the image is the result of monitoring input data/keylogger in the form of a text file.
4. Conclusion

Conclusion In the process of exploiting the system domain uinjkt.ac.id and subdomain ais.uinjkt.ac.id several weaknesses or security holes were found. The most security holes are in the ais.uinjkt.ac.id subdomain, which means that there are two mid-level loopholes so that attacks can still be carried out on the system, while in the uinjkt.ac.id domain system, the security gaps tend to be small. Unfortunately, the Distributed Denial of Service process has not been able to disable the uinjkt.ac.id domain system or the ais.uinjkt.ac.id subdomain system, but can only slow down the system process. The process of Enumeration and Gaining Access with Sniffing did not get maximum results and with BruteForce Attack obtained a username and password on the subdomain ais.uinjkt.ac.id, and at the end of the process a Trojan exploit was used to monitor the target system after completing security exploits on the system.

Acknowledgements

The authors thank Piksel journal editorial team for providing the opportunity to submit and carry out a review related to the journal.

Author Contributions

Thoyyibah proposed the topic; Thoyyibah, Haryono and Tomi conceived models and designed the experiments as well as conducted reporting and analysis.

Conflicts of Interest

The authors declare no conflict of interest.

References


https://doi.org/10.28932/jutisi.v4i1.770
https://doi.org/10.26905/jtmi.v2i1.615
https://doi.org/10.24246/ai.ti.v17i2.143-158