Exploiting DNS Server Vulnerabilities Using Linux Operating System

Aysar A. Abdulrahman, Alaa K. Jumaa
University of Sulaimani, Computer Science, Kurdistan Region of Iraq
aysar.abdulrahman@univsul.edu.iq
Sulaimani Polytechnic University, Technical College of Informatics, Kurdistan Region of Iraq
alaa_alhadithy@yahoo.com

ABSTRACT
Today, the world is using many modern Information Technology (IT) systems to gather, store, and manipulate important information. On the other hand, hackers are trying to gain access to any computer or system for viewing, copying, or creating data without the intention of destroying data or maliciously harming the computer. Exploiting domain name system (DNS) vulnerabilities have resulted in a range of high profile disruptions and outages for major internet sites around the world. DNS attack is an exploit in which an attacker takes advantage of vulnerabilities is the (DNS). This paper will present the vulnerabilities and the weak points of the DNS server and how attackers (black hat hacker) can exploit those vulnerabilities to attack and gain access to the server machine. In conclusion, presenting and implementing this project make users understand the hazard of hackers. Then, will lead to build secure and protected systems and applications.

Indexing terms/Keywords
Vulnerabilities; black hat hacker; DNS server; exploiting

Academic Discipline And Sub-Disciplines
Computer Science; Network Security; Computer Security;

SUBJECT CLASSIFICATION
Network Security Classification

TYPE (METHOD/APPROACH)
Experimental

INTRODUCTION
Network Security is the process of taking physical and software preventative measures to protect the underlying networking infrastructure from unauthorized access, misuse, malfunction, modification, destruction, or improper disclosure, thereby creating a secure platform for computers, users and programs to perform their permitted critical functions within a secure environment. Hacking is the art of exploiting computers to get access to otherwise unauthorised information. Nowadays, the world is using IT systems to gather, store and manipulate important information there is also a need to make sure that data is secure. However, no system is without its problems. Holes are often present within security systems which, if exploited, allow hackers to gain access to this otherwise restricted information. This paper aims to give you the information required to think like hackers, so as to be able to secure your systems and keep your information safe. Hacking and security is a constantly updated and fast moving sector of the computing industry and, as such, it is vital that you are up to date with all the details (including the latest exploits, patches and more).

HACKERS AND HACKING TOOLS
In a cyber security world, the person who is able to discover weakness in a system and managed to exploit it to accomplish his goal referred as a Hacker, and the process is referred as Hacking. Traditionally, a hacker is someone who likes to tinker with software or electronic systems. Hackers enjoy exploring and learning how computer systems operate. They love discovering new ways to work electronically. The good-guy (white-hat) hackers don’t like being in the same category as the

bad-guy (black-hat) hackers. Whatever the case, most people give hacker a negative connotation. Many malicious hackers claim that they don’t cause damage but instead are altruistically helping others. Hackers use some tools and techniques to attack or hack any system or victim, such us, Kali Linux.

Linux Hacking
Linux is extremely popular operating system for hackers. There are two main reasons behind this. The first reason is that Linux is freely available because it is an open source operating system; which make it so easy to modify or customize. The second reason is there are countless Linux security tools available that can double as Linux hacking software. Generally, there are two types of Linux hacking: hacking done by hobbyists and hacking done by malicious actors. Hobbyists are often hackers looking for new solutions to software problems or tinkerers looking for new uses for their software/hardware. Malicious actors use Linux hacking tools to exploit vulnerabilities in Linux applications, software, and networks. This type of Linux hacking is done in order to gain unauthorized access to systems and steal data [1].
LINUX HACKING TOOLS

Malicious actors typically use tools such as password crackers, network and vulnerability scanners, and intrusion detection software. These Linux hacking tools all serve different purposes and are used for a wide range of attacks. Password crackers are software developed for decoding passwords in a variety of formats, such as encrypted or hashed passwords. Many cracking tools offer additional functionality such as network detectors and wireless packet sniffing. Malicious actors use these Linux hacking tools because they offer a simple way to gain access to an organization’s network, databases, directories, and more. Password cracking distros are commonly used in Linux wifi hacking (Linux hacking that targets wireless networks) [2].

Linux network scanners are used to detect other devices on a network. In doing so, attackers are able to develop a virtual map of the network. In addition to discovering other devices, many network scanners are capable of gathering details about devices such as which operating systems, software, and firewalls are being used. For example, network scanners are used to discover network security holes in Linux wifi hacking. They also can be used to gather information useful for Linux distro hacking (Linux hacking that targets software, applications, operating systems, etc) [5].

Linux vulnerability scanning software is used to detect vulnerabilities in systems and applications. Malicious parties often use vulnerability scanners as Linux hacking software in order to detect exploitable vulnerabilities, gather simple passwords, discover configuration issues, and perform denial of service attacks. Vulnerability scanners are frequently used for Linux distro hacking because of these capabilities [4].

Network Scanner

Network scanners can be used to discover hosts on the network, find out what ports and services might be open were exposed on a host, to fingerprint operating systems, and to identify versions of services that are running.

Web Vulnerability Scanner

Web vulnerability scanners have some different flavors. Web server scanners examine web server software, such as Apache, looking for misconfigurations. Web application scanners look at the applications themselves, sometimes focusing on a particular types of vulnerabilities such as cross site scripting (XSS) or SQL injection (Sqli) vulnerabilities.

Exploitation Tools

Exploitation tools are usually not used to find vulnerabilities but rather just to exploit them clearly they could be used as true hacker tools but they can also be used to prove that particular vulnerabilities are real and exploitable, such as metasploit and armitage.

Nmap

Nmap ("Network Mapper") is an open source tool for network exploration and security auditing. It was designed to rapidly scan large networks, although it works fine against single hosts. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. While Nmap is commonly used for security audits, many systems and network administrators find it useful for routine tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. The output from Nmap is a list of scanned targets, with supplemental information on each depending on the options used. Key among that information is the “interesting ports table”. That table lists the port number and protocol, service name, and state. The state is either open, filtered, closed, or unfiltered. Open, means that an application on the target machine is listening for connections/packets on that port. Filtered, means that a firewall, filter, or other network obstacle is blocking the port so that Nmap cannot tell whether it is open or closed. Closed, ports have no application listening on them, though they could open up at any time. Ports are classified as unfiltered. In addition to the interesting ports table, Nmap can provide further information on targets, including reverse DNS names, operating system guesses, device types, and MAC addresses.

OUR WORK

The main operating system, which is used in this project, is Kali Linux. It is a Debian-based Linux distribution aimed at advanced penetration testing and security auditing. Kali Linux was released on the 13 March, 2013 as a complete, and it contains several hundred tools aimed at various information security tasks, such as penetration testing, forensics and reverse engineering. The other tool that we used in this paper is the Metasploit. Metasploit is an open source penetration tool used for developing and executing exploit code against a remote target machine. It is a powerful tool used for penetration testing, which can be used to test the vulnerability of computer system in order to protect them and on the other hand it can also be used to break into remote systems.

Metasploit can be used to make simple powerful Trojans for windows operating systems, which allow hackers complete access and control over the target system. In this project, we scan a target machine to find out the vulnerabilities of it. Then, we use metasploit to make a Trojan and hack a victim machine which use windows server as an operating system.
The first stage of this paper is scanning the whole network to find and detect the list of the live hosts on the network. Then, select one of those hosts to be our victim machine. In this step we can know details of the victim machine such as opened ports, services, and operating system.

The second stage is logging into the victim machine using “shell” command. In this step, we login to the victim machine and modify the “host” file which saved in windows directory.

The third stage of our project is creating a “facebook” fake website and force the victim to login to our fake sit by modifying victim’s host file.

Then, the last stage is stealing and grabing the facebook account of the user’s victim machine.

**Network Scanning**

The first step of our scan, as shown in the figure 1 and figure 2, is scanning the network to find out all the host machines.
The next step, as shown in figure 3, is scanning the specific host as a victim machine. In this step, we will get all the details about the victim machine such as the open ports, services, operating system, etc.

Creating a Host File

The host file is a computer file used by the operating system to map hostnames to IP addresses. The host file is a plain text file, and is conventionally named hosts. It is a text file which contains the hostnames and address of hosts as contributed for inclusion by member organizations. The host file is saved on the Windows operating system in the following directory: C:\Windows\System32\Drivers\etc\hosts. In this step, we create a fake host file to use later for modifying the victim’s host file. First, we will need to find the IP of our Kali Linux IP address. As shown in figure 4, we can use “ifconfig” command to find out the IP.

Figure 3 Scan a Victim Machine

Figure 4 Kali Linux (Attacker) IP Address
The next step is creating a fake host file as shown if the following figure 5

![Creating a Fake Host File](image)

**Figure 5 Creating a Fake Host File**

**Attacking and Modifying a Victim’s Host File**

In this step, as shown in figure 6, we use the “command shell” attack to login into the victim’s host file:

![Login into Victim’s Host File](image)

**Figure 6 Login into Victim’s Host File**
The next step is removing the original victim’s host file and upload our host file which we created in the previous section, as shown in the following figure 7:

Figure 7 Removing and Uploading the Fake Host File

Creating Fake “Facebook” website.

The Social-Engineer Toolkit (SET) was created and written by the founder of TrustedSec. It is an open-source Python-driven tool aimed at penetration testing around Social-Engineering. SET has been presented at large-scale conferences including Blackhat, DerbyCon, Defcon, and ShmooCon. With over two million downloads, SET is the standard for social-engineering penetration tests and supported heavily within the security community. The Social-Engineer Toolkit has over 2 million downloads and is aimed at leveraging advanced technological attacks in a social-engineering type environment. TrustedSec believes that social-engineering is one of the hardest attacks to protect against and now one of the most prevalent.

The first thing we have to do is update both Metasploit framework and the social engineering toolkit to make sure that we have the latest version. Now, from the menu we select number “1-Social Engineering Attacks” as shown in the following figure 8:

Figure 8 Social Engineering Toolkit
The next step is selecting “2-Website Attack Vectors” as shown in the following figure 9:

![Figure 9 SET (Website Attack Vectors)](image)

Then, we use the third option, which is “3-Credential Harvester Attack Method” as shown below in figure 10:

![Figure 10 SET (Credential Harvester Attack)](image)
We now have three options as shown in figure 11, and we use the third option, which is “3-Custom Import” to import our facebook face website.

![Figure 11 SET (Custom Import)](image)

Now, as shown in figure 12, we have to enter the IP of our Kali Linux machine, which can be obtained by using the terminal with “ifconfig” command. The IP of the Kali machine is 192.168.1.111

![Figure 12 SET (Attacker IP Address)](image)

The next step is specifying the path of the fake facebook web site that we already created, which is /root/Facebook. Then, we have to chose the second options to copy all the entire folder. Then entering the URL of the facebook as https://www.facebook.com. Now, we can see as shown in figure 13 that our fake web server is started.
Hacking Victim’s Facebook Account

We are created a fake Facebook web server and modified the victim’s host file. When the victim machine tries to login to www.facebook.com, the victim machine will login to our web server. Now, when the victim’s user enters his/her user name and password, we will get a copy of them and find it in the following path: var/www, as shown in the following figure 14 and 15:

Figure 13 SET (Fake Web Server Starter)

Figure 14 victim’s Facebook Login Page
As shown above, when the victim logs in to his/her Facebook account, our fake server will get a copy of that account and save it in a specific directory, which is: var/www.

**CONCLUSION AND FUTURE WORK**

The most important points concluded throughout the planning and the implementing of this project are:

1. Scanning a network to find the live victims.
2. Scanning a specific target and find vulnerabilities and the type of the OS which is running on it.
3. Creating a fake “host” file using Kali Linux.
4. Hacking a victim machine and uploading the fake host file into the victim’s machine.
5. Creating a fake “facebook” web server and force the victim to use it by modifying its host file.
6. Grab the user name and password of the victim’s Facebook account.

The future works can be progress to include many new parts using updated technologies and tools. The main future work can be summarized as the following:

1. Scan networks and victims using Zombie’s scan tool.
2. Find the vulnerabilities of victim machine using undirected methods.
3. Creating fake web servers for hacking yahoo mail and google mail account.

**REFERENCES**

[1] Maynor, D., & Mookhey, K. (2007). Metasploit toolkit for penetration testing, exploit development, and vulnerability research. Burlington, MA: Syngress.

[2] Lakshman, S. (2011). Linux Shell Scripting Cookbook. Birmingham: Packt Pub.

[3] Hutchens, J. (2014). Kali Linux network scanning cookbook over 90 hands-on recipes explaining how to leverage custom scripts and integrated tools in Kali Linux to effectively master network scanning. Birmingham, UK: Packt Pub.

[4] Chirillo, J. (2001). Hack attacks revealed: A complete reference with custom security hacking toolkit. New York: Wiley.

[5] Pritchett, W. (2013). Kali Linux Cookbook. Packt Publishing.
[6] Valade, J. (2005). Linux. Upper Saddle River, NJ: Addison-Wesley.

[7] Broad, J., & Bindner, A. (2014). Hacking with Kali practical penetration testing techniques. Waltham, MA: Elsevier Science.

[8] Kennedy, D. (2011). Metasploit the penetration tester's guide. San Francisco, CA: No Starch Press.

[9] Lyon, G. (2008). Nmap network scanning: Official Nmap project guide to network discovery and security scanning. Sunnyvale, CA: Insecure.Com, LLC.

[10] Pardoe, T. D., & Snyder, G. F. (2005). Network security. Clifton Park, NY: Thomson/Delmar Learning.

[11] Huang, S. C., MacCallum, D., & Du, D. (2007). Network security. New York: Springer.

[12] Savasgard, E. (2015). Hacking: The essential hacking playbook for beginners, secret techniques you need to know before you start hacking. North Charleston, SC: CreateSpace Independent Publishing Platform.

[13] Gregory, M. A., & Glance, D. (2013). Security and the networked society. Cham: Springer.

Author' biography with Photo

Aysar A. Abdulrahman received his B.Sc. in Information and Communication Engineering from University of Baghdad, in 2003. In 2008, he received the M.Sc. degrees in Computer Science from University of Sulaimani. During 2008-2010, he worked as an assist lecturer at University of Sulaimani\ College of Science\ Computer Department. In Dec 2013, he got his Ph.D. in Computer Engineering from Southern Illinois University. Now, he is working as a lecturer in the University of Sulaimani\ College of Science\ Computer Department.