|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name: Nishchal Sreevathsa |  |  |  |  |

Crafting and Deploying Malware Using a

Remote Access Trojan (RAT)

Ethical Hacking & Lab 6

Table of Contents

1. [Executive Summary 2](#_Toc409378035)

[Highlights](#_Toc409378036)

[Objectives](#_Toc409378037)

1. [Lab Description Details 3](#_Toc409378038)

[Include Steps Taken, Notes, & Screen Shots demonstrating completion of lab objectives](#_Toc409378039)

1. [Supporting Evidence 15](#_Toc409378040)
2. [Conclusion & Wrap-Up 17](#_Toc409378041)

[Summary with observations, Success & Failures, Challenges](#_Toc409378042)

# Executive Summary

## Highlights

|  |  |
| --- | --- |
|  | Our goal in this lab session is to penetrate and seize control of a host that is connected to the network. To find the open ports on the pfSense firewall from outside, use the scanning software nmap/Zenmap in the first stage. The lab then uses Bruter, a Windows-based GUI program for network brute-forcing, to conduct a dictionary attack in order to find the administrator password. The attacker can use the credentials to access the administrator account over an RDP session after Bruter successfully determines the password.  **Breaching the System:** The demand for more complicated passwords is a current problem in information technology systems. The simplicity of passwords makes it possible for hackers to utilize password dictionaries—lists of frequently used passwords—to launch a brute-force assault against your systems and discover login information. A breach may involve the theft of intellectual property, which could harm an organization's reputation or cause financial loss.  **Bruter:** Bruter is a brute force tool that helps hackers try logins using a dictionary of frequently used passwords until the tool is consistently successful and reports the password that it identified as being valid. Using Bruter, you were able to discover the administrator account's login information in this lab.  **Malware:** The term "malicious software" is short for "malicious software," which refers to computer programs that have been created with evil intentions. Here are a few prevalent forms of malware:Trojan horses, rootkits, ransomware, viruses, worms, and backdoors. |

## Objectives

|  |  |
| --- | --- |
|  | Scan a network with nmap or Zenmap.  Malware is installed on a system.  Utilize Bruter to take advantage of a system weakness.  To break into a system, use remote desktop. |

# Lab Description Details

## Include Steps Taken, Notes, & Screen Shots demonstrating completion of lab objectives

**Launching an Attack**

**Step 1:** Select external Windows 8.1 machine and launch the command prompt. Now the firewall's open ports should be identified.

Command: **nmap 203.0.113.100**

A computer screen shot of a computer

Description automatically generated

**Step 2:** Launch Zenmap, enter the target host with IP Address **203.0.113.100**, and run a thorough scan. The open ports and associated banner messages can be seen by selecting the Ports / Hosts tab when the scan is finished. Then exit Zenmap.

A screenshot of a computer

Description automatically generated

**Step 3:** Launch the **Bruter.exe** application on an external Windows machine. Enter the IP Address **203.0.113.100** in the Target field, Set the protocol to **FTP** and enter **21** in the port number field. In the User option type **administrator** as the User. Click Browse the button next to Dictionary and select and open the **Wordlist.txt file**. Press the **Start** button to launch the attack.

A screenshot of a computer

Description automatically generated

After a few minutes, once the attack gets completed, the password would be displayed (**P@ssw0rd**) for the user administrator with the Target IP address 203.0.113.100 using the FTP service.

**Building and Deploying the Malware**

**Step 4:** Open the Malware Folder on Windows machine and extract sampleflag.7z file and open the file to see the **sample flag: 999818**.

A screenshot of a computer

Description automatically generated

**Step5:** Open **flag2.txt** and see the **flag number: 343434** for **Challenge 1**.

A screenshot of a computer

Description automatically generated

**Step 6:** Extract the DarkComet.7z zip file and open the DarkComet folder and search for flag3.txt and open it. We see **Flag number:** **717999** for **challenge 2**.

A screenshot of a computer

Description automatically generated

**Step 7:** Launch DarkComet.exe application and select Listen to new port and enter **443** in Listen port number field and then press Listen button.

A computer screen shot of a computer

Description automatically generated

**Step 8:** Select Full editor (Expert) from the Server module menu in the DarkComet-RAT menu bar. Next, select Network Settings. When this opens, type **443** (almost always allowed out) for Port and **175.45.176.200** (the IP address of the external Windows 8.1 machine) for IP/DNS. Next, select ADD.

A computer screen shot of a computer

Description automatically generated

**Step 9:** In the chose icon windows select custom icon and select firefox icon.

A screenshot of a computer

Description automatically generated

**Step 10:** Select the executable file as **UPX (Ultimate Packer Executable)** by clicking on Stud Finalization then click on Build the Stub.

A screenshot of a computer

Description automatically generated

**Step 11:** Save the firefox on the Desktop and then you would be able to see **firefox.exe** malware on the Desktop.

A screenshot of a desktop

Description automatically generated

**Step 12:** Open the command prompt and check whether the RDP is open on the firewall.

Command: **nmap 203.0.113.100 –p 3389**

A computer screen shot of a computer screen

Description automatically generated

**Step 13:** Launch the Microsoft Service client and enter IP Address **203.0.113.100** in the computer field on Remote Desktop Connection Window and then click on Connect button.

A computer screen with a computer code

Description automatically generated

**Step 14:** Enter the username as **administrator** and password as **P@ssw0rd** in the credential’s windows to login into remote windows 2008 server.

A computer screen with a login box

Description automatically generated

**Step 15:** Paste the firefox.exe malware file on the Windows desktop server and open the malicious file.

A computer screen shot of a blue screen

Description automatically generated

**Step 16:** After clicking on Firefox, the user's reflection appeared on the Darkcomet application's users panel. The DarkComet-RAT console will show the connection to the victim. You may view the victim's internal IP address by expanding the IP Wan/[Lan]: Port tab on the right. This address is now known to the attacker!

A screenshot of a computer

Description automatically generated

**Step 17:** Open the victim machine and launch the Control Server. On the list on the left, select System Info. To examine the computer information, choose Computer Information and press the Refresh button at the program's bottom.

A screenshot of a computer

Description automatically generated

**Step 18:** Double-click on the Explorer files in the list after opening the Files manager by clicking on the arrow. It will show up the File Manager. The perpetrator is on the left, and the victim is on the right. On the victim machine, access the C drive folder.

A screenshot of a computer

Description automatically generated

**Step 19:** On Victim Machine, Open the **DeathStar** folder, **4 Blueprint pictures** were discovered. Open the C drive on the Attack machine and open Users folder and open Document folder which is in Public Folder which is under Users Folder. Choose all four blueprint files on the victim machine, then use the Receive button to send them to the attack machine. Then click the Refresh Button on the attack machine to view the transferred file from the victim machine.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

**Step 20:** Open the File Explorer and open the C drive -> Users -> Public Folder -> Public Documents.

Open the **Blueprint1.jpg** and record the **sample flag: 999818**.

A computer screen shot of a blueprint

Description automatically generated

**Step 21:** Opened the **Blueprint2.jpg** and captured the flag for **Challenge 3** and the **flag number is 111222**.

A screenshot of a computer

Description automatically generated

**Step 22:** Opened **Blueprint3.jpg** and captured the flag for **Challenge 4** and the **flag number is 777558**.

A screenshot of a computer

Description automatically generated

**Step 23:** Opened **Blueprint4.jpg** and captured the flag for **Challenge 5** and the **flag number is 655913**.

A screenshot of a computer

Description automatically generated

# Supporting Evidence

**Screenshots, Research, Etc.**

**Screens screenshot of a computer

Description automatically generated**

**A screenshot of a computer

Description automatically generated**

**Screens screenshot of a computer

Description automatically generated**

# Conclusion & Wrap-Up

## Summary with observations, Success & Failures, Challenges

In this lab, an attacker made an attempt to infiltrate and compromise a host on a network. The attacker used a variety of techniques, including network scanning with nmap/zenmap, system vulnerability exploration with bruter, malware deployment (in this case, the DarkComet Remote Access Trojan), and remote desktop access and data exfiltration. Let's look at the lab's accomplishments, setbacks, and difficulties.

**Successes:**

* **Scanning the Network:** The experiment effectively illustrated the value of extensive network scanning using programs like nmap and zenmap to find open ports and potential security holes in the target machine.
* **Attack via Brute Force:** The administrator account's login information was successfully determined by the brute-force tool Bruter, underscoring the dangers of using weak or pre-generated passwords.
* **Deployment of Malware:** The lab demonstrated how simple it is to install malware, in this case the DarkComet RAT, on a compromised system. Because the malware was camouflaged as a genuine application, it was more difficult to find.
* **Exfiltration of Data:** The attacker was able to exfiltrate private information after successfully compromising the target system, highlighting the possible repercussions of a breach for an organization.

**Challenges:**

* In Zenmap it took too long for an intense Scan to complete.
* It took some time to understand the DarkComet.exe application first then proceeded with the usage of this application.

**Risks:**

* Firewalls have to be set up such that sensitive data and computers can only be accessed by approved connections, ports, and addresses. In our instance, the external computer established a limitable remote session with the server computer.
* To prevent malware from being installed and executed, all computers connected to the network need to have up-to-date antivirus software and malware detection tools installed and operational.
* To stay current with malware signatures, both the antivirus and malware must be updated on a regular basis.
* Administrators are required to investigate whether any services or components operating on the network are using default passwords, and if so, they must change them right away.
* Additionally, administrators must avoid using less complex or widely used passwords for any crucial, sensitive accounts or services.

**Remediations:**

* To prevent brute-force attacks, administrators must set exceedingly complex passwords for sensitive accounts and machines.
* Additionally, the password cannot be used on more than one machine or account.
* In order to improve security, the passwords must also be changed every thirty days.
* Need to make sure that every default password is modified.
* Improved intrusion detection and prevention tools and rules need to be implemented on firewalls in order to stop and identify malicious or unauthorized activity.
* Allow only the ports that are in use, keep an eye on all incoming and outgoing traffic, and build a baseline map of the network that you can use to flag any questionable activity. Since the most frequently used ports are the ones that permit traffic to flow, they are also the most susceptible to attacks; for this reason, the ports need to be properly configured using the firewall and also need to be monitored.