Unit III
Techniques Used by Hackers

The Reconnaissance

In the context of cybersecurity, reconnaissance is the practice of covertly discovering and collecting information about a system. This method is often used in ethical hacking or penetration testing.

Like many cybersecurity terms, reconnaissance derives from military language, where it refers to a mission with the goal of obtaining information from enemy territory.

How Reconnaissance Works

Reconnaissance generally follows seven steps:

1. Collect initial information
2. Determine the network range
3. Identify active machines
4. Find access points and open ports
5. Fingerprint the operating system
6. Discover services on ports
7. Map the network

One of the most common techniques involved with reconnaissance is port scanning, which sends data to various TCP and UDP (user datagram protocol) ports on a device and evaluates the response.

Differences Between Passive and Active Reconnaissance

There are two main types of reconnaissance: active and passive reconnaissance.

- With *active reconnaissance*, hackers interact directly with the computer system and attempt to obtain information through techniques like automated scanning or manual testing and tools like ping and netcat. Active recon is generally faster and more accurate, but riskier because it creates more noise within a system and has a higher chance of being detected.

- *Passive reconnaissance* gathers information without directly interacting with systems, using tools such as Wireshark and Shodan and methods such as OS fingerprinting to gain information.

Passive Scanning Techniques

In passive reconnaissance, data are gathered without interacting with the framework or application we are trying to comprehend. Data is collected through web searches and free reports. The framework is unlikely to know the IP address when we use passive reconnaissance. Conduction of passive recon is done without directly interacting with the target. By doing so, no request is sent to the target and, therefore, they have no idea that information is being gathered about them.

- One of the easiest things a hacker can do is check the target organization's websites. It is common for businesses to put information up that can be very useful to an attacker. For example, let's assume company XYZ lists John Doe as its IT manager. An enterprising hacker scans bulletin boards and discussion groups for references to John Doe at XYZ.

That attacker might find information useful in spear phishing attacks, or the attacker might find information useful in social engineering.

- It is also possible for an attacker to scan bulletin boards, chat rooms, discussion groups, and more looking for questions from IT staff at the target organization. For example, if an administrator posts in a discussion group asking about a particular server problem, this can give the attacker valuable information about that target network.
- Another way attackers can use the Web to find out information about a target is through job ads. For example, if a company routinely advertises for ASP.NET developers and never for PHP or Perl, then it is likely that the company's web applications are developed with ASP.NET running on a Windows web server (Internet Information Services). This can allow the attacker to focus only on a small group of possible attacks (those against ASP.NET/Windows).
- There are also specific websites that provide information an attacker may find useful. The first such website is **netcraft.com**,. This website provides information about websites. For example, you can find out what kind of server a site is running, and in some cases how long it has been since it was last rebooted.

Active Scanning Techniques

The previously mentioned techniques are all considered passive, as they do not require the attacker to connect to the target system. Since the attacker is not actually connecting to the target system, it is impossible for an intrusion detection system (IDS) to detect the scan. Active scans are far more reliable but may be detected by the target system. There are a few types of active scans.

Port Scanning

Port scanning is the process of attempting to contact each network port on the target system and see which ones are open. There are 1,024 well-known ports that are usually associated with specific services.

Some of the most popular and most frequently used ports include:

1. Port 20 (UDP): File Transfer Protocol (FTP) used for transferring data
2. Port 22 (TCP): Secure Shell (SSH) protocol used for FTP, port forwarding, and secure logins
3. Port 23 (TCP): The Telnet protocol used for unencrypted communication
4. Port 53 (UDP): The Domain Name System (DNS), which translates internet domain names into machine-readable IP addresses
5. Port 80 (TCP): The World Wide Web Hypertext Transfer Protocol (HTTP)

The most common types of scans are listed here:

- **Ping scan:** This scan simply sends a ping to the target port. Many network administrators block incoming ICMP packets for the purpose of stopping ping scans.

- **Connect scan:** This is the most reliable scan, but also the most likely to be detected. With this type of scan a complete connection is made with the target system.
- **SYN scan:** This scan is very stealthy. Most systems accept SYN (Synchronize) requests. This scan is similar to the SYN flood DoS attack described in Chapter 4, "Denial of Service Attacks." In this scan you send a SYN packet but never respond when the system sends a SYN/ ACK. However, unlike the DoS SYN flood, you only send one packet per port. This is also called the *half-open scan*.
- **FIN scan:** This scan has the FIN flag, or connection finished flag set. This is also not an un- usual packet for systems to receive, so it is considered stealthy.

Each of these scans provokes a different response on the target machine and thus provides different information to the port scanner:

- With a FIN scan or an XMAS scan, if the target port is closed, the system sends back an RST flag packet (RST means reset). If it is open, there is no response.
- With a SYN scan, if the port is closed, the response is an RST; if it is open, the response is a SYN/ACK.
- ACK scans and NULL scans only work on UNIX systems.

Example of Nmap:

Nmap also lets you set a number of flags (either with the command-line version of Nmap or the Windows version) that customize your scan. The allowed flags are listed here:

-O	Detects operating system
-sP	Is a ping scan
-sT	TCP connect scan
-sS	SYN scan
-sF	FIN scan

Actual Attacks

Now that we have discussed how attackers scan a target system, let's look at a few attacks that are commonly used. Obviously this won't be an exhaustive list, but it will provide you some insight into the attack methodologies used. In Chapter 4 we discussed denial of service (DoS) attacks and some tools used to cause these attacks. In this section we will look at other sorts of attacks and the techniques and tools used to make them happen.

SQL Script Injection

This may be the most popular attack on websites. In recent years, more websites have taken steps to ameliorate the dangers of this attack; unfortunately, all too many websites are susceptible. This attack is based on passing structured query language commands to a web application and getting the website to execute them.

Relational databases are based on relations between various tables. The structure includes tables, primary and foreign keys, and relations. A basic description can be summarized with the following points:

- Each row represents a single entity.
- Each column represents a single attribute.
- Each record is identified by a unique number called a *primary key*.
- Tables are related by foreign keys. A *foreign key* is a primary key in another table.

Many websites/applications have a page where users enter their username and password. That username and password will have to be checked against some database to see if they are valid. Regardless of the type of database (Oracle, SQL Server, MySQL), all databases speak SQL. SQL looks and functions a great deal like English. For example, to check a username and password, you might want to query the database and see if there is any entry in the users table that matches that username and password that was entered. If there is, then you have a match. The SQL statement might look something like this:

*'SELECT * FROM tblUsers WHERE USERNAME = 'jdoe' AND PASSWORD = 'letmein'*

Now if there is a username jdoe in tblUsers, and the password for it is letmein, then this user will be logged on. If not, then an error will occur.

SQL injection works by putting some SQL into the username and password block that is always true. For example, suppose you enter 'OR X=X' into the username and password boxes. This will cause the program to create this query:

*SELECT * FROM tblUsers WHERE USERNAME = "OR X=X' AND PASSWORD = "OR X=X'*

So what we are telling the database is to log us in if the username is blank, or if X=X, and if the password is blank, or if X=X. If you think about this for a second, you will see that X always equals x, so this will always be true,

There is no significance to 'OR X=X'; it is simply a statement that will always be true. Attackers try other similar statements, such as the following:

' or 'a'='a

' or '1'='1

' or (1=1)

Cross-Site Scripting

With cross-site scripting, an attacker injects client-side script into web pages viewed by other users. The key is that the attacker enters scripts into an area that other users interact with. When they go to that part of the site, the attacker's script is executed rather than the intended website functionality.

For example, assume a shopping site allows users to review products. Rather than typing in a review, the attacker types in JavaScript that redirects the user to a phishing website. When another user views that "review," the script will execute and take him to the new site. Again, this can be prevented by simply filtering all user input. As of this writing, all the major online shopping portals, such as Amazon.com, do filter input and are not susceptible to this attack. However, many smaller sites are still susceptible.

Let's look at another hypothetical scenario. Let's assume that ABC online book sales has a website. In addition to shopping, users can have accounts with credit cards stored, post reviews, and more. The attacker first sets up an alternate web page that looks as close to the real one as possible. Then the attacker goes to the real ABC online book sales website and finds a rather popular book. He goes to the review section, but instead of typing in a review he types in this:

<script> window.location = "http://www.fakesite.com"; </script>

Now when users go to that book, this script will redirect them to the fake site, which looks a great deal like the real one. The attacker then can have the website tell the user that his session has timed out and to please log in again. That would allow the attacker to gather a lot of accounts and passwords. That is only one scenario, but it illustrates the attack.

Password Cracking

Doing password cracking is easiest when one can actually get physical access to a machine. This is not as difficult as it sounds. Many organizations (such as universities) have kiosk machines where someone can use the system with minimal/guest privileges. A skilled hacker can use this access to gain further access. Password Cracking can be cracked in three popular ways-*Brute force attack, Dictionary Attack and Rainbow Table attack.*

Brute force Attack: A brute force attack (exhaustive search) is a cryptographic hack that relies on guessing possible combinations of a targeted password until the correct password is discovered. This attack uses trial-and-error to guess login info, encryption keys, or find a hidden web page. Brute force attacks don't employ an intellectual strategy. These attacks simply try using different combinations of characters until the correct combination is found. The length of the password causes that hacker needs to the more guessing to understand the password.

Dictionary attack: In this attack, the attacker works through a dictionary of possible passwords and tries them all. Of course, these attacks tend to be somewhat outdated because often require a large number of attempts against possible targets.

Rainbow table attack: A rainbow table is a precomputed table for reversing cryptographic hash functions. It can be used to guess a function up to a certain length consisting of a limited set of characters.

Windows Hacking Techniques

Given the ubiquitous nature of Microsoft Windows, it should be no surprise that there are a wide range of attacks specifically aimed at Windows operating System. Most popular Windows Hacking are- Pass the Hash, Net User Script and

Pass the Hash

Many systems store passwords as a cryptographic hash. This is done because it is impossible to "unhash" something. The pass the hash attack essentially realizes that the hash cannot be reversed; rather than trying to find out what the password is, the attacker just sends over the hash. If the attacker can obtain a valid username and user password hashes values (just the hash—the attacker does not know the actual password), then the hacker can use that hash, without ever knowing the actual password.

Net User Script

This particular exploit first requires access to the target machine with at least guest-level privileges. It is based on the fact that many organizations put the technical support personnel in the domain admin's group.

The attacker writes the following two-line script (obviously the word *localaccountname* is replaced with an actual local account name.):

```
net user /domain /add localaccountname password
net group /domain "Domain Admins" /add Domain
```

Save that script in the All Users startup folder. The next time someone with domain admin privileges logs on to the machine, it will execute and that *localaccountname* will now be a domain admin. The only problem is that it may be quite some time before someone with such privileges logs onto that machine. To make this happen, the attacker will cause a problem with the system that would necessitate technical support fixing it, such as by disabling the network card. The next user to log in will not be able to access the network or Internet and will call technical support. There is a reasonably high chance that the person in technical support is a member of the domain administrators group. When that person logs on to the computer to fix the problem, unbeknownst to her the script will execute.

Login as System

This particular attack requires physical access to one machine on your network. It does not require domain or even computer login credentials. To understand this attack, think about the last time you logged into any Windows computer, even a Windows server. Next to the login text boxes (Username and Password), there is an accessibility button that allows you to launch various tools to aid those users with disabilities. For example, you can launch the magnifier class in order to magnify text.

In this attack, the perpetrator will boot the system to any Linux live CD. Then, using the FDISK utility, the attacker will locate the Windows partition. Navigating to the Windows\System32 directory, the attacker can first take magnify.exe and make a backup, perhaps naming the backup magnify.bak. Then she can take command.exe (the command prompt) and rename it magnify.exe.

Now the attacker reboots to Windows. When the login screen appears, the perpetrator clicks Acces- sibility and then Magnify. Since command.exe was renamed to magnify.exe, this will actually launch the command prompt. No user has logged in yet, so the command prompt will have system privileges. At this point the attacker is only limited by her knowledge of commands executed from the command prompt.

This particular attack illustrates the need for physical security. If an attacker can get even 10 minutes alone with your Windows computer, she will likely find a way to breach the network.

Penetration Testing

As was mentioned at the beginning of this chapter, these techniques can also be conducted as part of a penetration test. However, a penetration test is not simply the random application of a variety of hacking techniques. Usually, a penetration test is done along with or subsequent to a vulnerability assessment.

The process is a methodical probing of a target network in order to identify weaknesses in the network. The theory behind penetration testing is that the only way to objectively determine the security level of a given network is to have a competent penetration tester attempt to breach security. There are a variety of standards that one can use to guide a penetration test.

NIST 800-115

NIST 800-115 is the National Institute of Standards and Technology guideline for security assessments for Federal Information Systems. Assessments include penetration tests. NIST 800-115 describes security assessments and has four phases:

- **Planning:** During this phase the tester needs to set specific testing goals. Often these will be related to previous risk assessment evaluations of the target network.
- **Discovery:** This phase involves using a variety of tools, including port scanners, vulnerability scanners, and manual techniques to identify or discover any issues with the target network.
- **Attack:** Now the attacker can attempt to compromise the target network by exploiting the vulnerabilities found during the discovery phase. It is in this phase that the penetration tester applies the hacking techniques we have discussed in this chapter.
- **Reporting:** The final step is to prepare a detailed report and to deliver it to the person who hired the penetration tester. The report should provide details on what vulnerabilities were exploited, how they were exploited, and what remediation steps are recommended.

National Security Agency Information Assessment Methodology

The National Security Agency (NSA) has primary responsibility for information security throughout the United States Federal government. For this reason, it formulated a methodology to be applied to any information systems assessment to include security audits, vulnerability tests, and penetration tests. That methodology is briefly described here:

- Pre-Assessment
  - Determine and manage the customer's expectations.
  - Gain an understanding of the organization's information criticality.
  - Determine customer's goals and objectives.
  - Determine the system boundaries.
  - Coordinate with customer.
  - Request documentation.

- On-Site Assessment
  - Conduct opening meeting.
  - Gather and validate system information (via interview, system demonstration, and document review).
  - Analyze assessment information.
  - Develop initial recommendations.
  - Present out-brief.
- Post-Assessment
  - Give additional review of documentation.
  - Get help understanding what you learned.
  - Report coordination (and writing).

PCI Penetration Testing Standard

The Payment Card Industry Data Security Standards (PCI DSS) are standards used by companies that process credit cards. We will look at PCI standards in general in Chapter 10, "Security Policies." In this section we will briefly examine the penetration testing portion of those standards. PCI DSS Requirement mandates penetration testing to validate that segmentation controls and methods are operational, effective, and isolate all out-of-scope systems from systems in the cardholder data environment.

PCI standards recommend testing a separate environment, not on the live production environment during normal business hours.

It is recommended that pen testing include social engineering tests.

Per PCI DSS Requirements, penetration testing must be performed at least annually and after any significant change—for example, infrastructure or application upgrade or modification— or new system component installations. As with the previous models we examined, PCI DSS has some specific steps:

- Pre-engagement: Defining scope, documents, rules of engagement, success criteria, and re- view of past issues
- The actual penetration test: Where you apply the hacking techniques
- Post-Engagement: Reporting and recommending remediation steps