ICSI MODULE 13:

Hacking Preparation

13.1 Hacking Preparation

Skilled hackers rarely simply start an attack. They first want to gather information about the target before attacking. This is similar to a skilled bank robber first casing the bank to learn all he can before actually trying to rob it. A skilled hacker wants to understand everything he can about the target organisation and its system. This preparation phase is important. It is also a reason why a security-conscious organisation should be very careful about what information is allowed in public.

13.1.1 Passive Information Gathering

The first step in any computer attack is a passive search. This is any attempt to gather information that does not actually involve connecting to the target system. If the target system has firewall logs, an intrusion detection system (IDS), or similar capabilities, then an active scan might alert the company. The first step is to simply search the web for the organisation in question.

You might discover that it has an announcement stating a move to a new router model, or that it uses IIS 7.0 for its web server. Any information about the target system enables the attacker to narrow his search for vulnerabilities. In the second example, he can now simply search for "security flaws in IIS 7.0" or some similar search term.

The possibility also exists that the attacker will learn about people in the organisation. Knowing actual names, phone numbers, office locations, and so on can aid in a social engineering attack. The more information one has on a target organisation, the easier the attack will be.

Several websites can help with this. Websites such as www.netcraft.com, www.shodan.io and www.censys.io can provide information about a target web server or what ports are open on the public IP address of the organisation in question.

13.1.2 Active Scanning

Although passive scanning can yield a lot of useful information, at some point the attacker needs to do an active scan, which involves some level of actual connection to the target system. It is the most likely to be detected, but also the most likely to yield actionable information. Several types of active scanning exist:

- **Port scanning:** This is a process of scanning the 1024 well-known ports or even all the ports (there are 65,535) to see which ports are open. This can tell an attacker a great deal of information. For example, port 161 indicates the target is using Simple Network Management Protocol, which might provide a vulnerability that can be exploited. Port 88 tells an attacker that the target system uses Kerberos authentication.
- **Enumeration:** This is a process whereby the attacker tries to find out what is on the target network. Items such as shared folders, user accounts, and similar items are sought after. Any of these can provide a point of attack.
- **Vulnerability assessment:** This is the use of some tool to seek out known vulnerabilities. The attacker might also try to manually assess vulnerabilities. The latter can be done in many ways.

A number of tools are freely available on the Internet for active scanning. They range from the very simple to the complex. Anyone involved in preventing computer crimes or investigating computer crimes should be familiar with a few of these.

When you are doing a port scan, you have a number of options. The most common types of scans and their limitations are as follow:

- **Ping scan:** This scan sends a ping packet to the target IP address. This is to check to see whether a given port is open. The problem with ping scanning is that many firewalls block ICMP packets. Internet Control Message Protocol (ICMP) is the protocol used by ping and tracert (traceroute for Unix/Linux users).
- **Connect scan:** This type of scan actually tries to make a full connection to the target IP address at a given port. This is the most reliable type of scan. It will not yield false positives or false negatives. However, it is the scan most likely to be detected by the target network.
- **SYN scan:** This scan is based on knowledge of how network connectivity works. Any time you connect to any server an exchange of packets negotiates the connection. Your machine sends a packet with a SYN flag, which means synchronize. Basically, you are asking permission to connect. The server responds with a packet that has a SYN-ACK flag, a synchronize-acknowledge.

That is the server saying "ok, you can connect." Your computer then sends a packet with an ACK flag, acknowledging the new connection. A SYN scan simply sends a connection request to each port. This is to check to see whether the port is open. Because servers and firewalls routinely get SYN packets, this is unlikely to trigger any alarms on the target system.

- **FIN scan:** This scan has the FIN flag, or connection finished flag, set. This is also usually not going to attract unwanted attention at the target network because connections are being closed routinely, so packets with the FIN flag set are not unusual.

Other scans include the Null scan, with no flags set, and the XMAS scan, with several flags set. Whatever the specific scan used, most will leave some trace of the attack in the server or firewall logs.

Guided Exercise: Passive Information Gathering

13.2 Guided Exercise: Passive Information Gathering

Resources	
Files	None
Machines	None

In this exercise you are required to search and find publicly available information for the domain hackthissite.com. You will need to use a web browser for this exercise not in the lab environment.

Go to the link https://www.netcraft.com/ and in the text box under What's that site running enter https://www.hackthissite.org and press Enter.

1. Once the results are revealed identify the IP address.
2. Which is the Nameserver of the domain?
3. Which is the Nameserver organisation?
4. Which is the Hosting country?
5. What is the Reverse DNS?

The Attack Phase

13.3 The Attack Phase

After passive scanning, port scanning, enumerating, and gathering information about the target site, the attacker will be ready to attack the target system. This is the part where he or she applies the knowledge gained in the scanning phases.

13.3.1 Physical Access Attacks

If an attacker can physically sit in front of any machine connected to your network, there are a number of ways he can use that to gain access to your entire network. His first step is simply to be able to log on to that machine. He need not be able to log on to the network yet, just that machine.

13.3.1.1 Bypassing the Password

One exciting way to break into Windows computers is to simply bypass the password all together. You don't find out what the password is; you just skip it. It requires about 5 minutes at the workstation with a Linux live CD.

13.3.2 Remote Access Attacks

Obviously, physical access to a workstation on the target network is not always possible. Although remote attacks are far less likely to succeed, they still have the potential to succeed. A number of possible remote attack methods exist, but this section focuses on a couple of the most common: SQL injection and cross-site scripting.

13.3.2.1 SQL Injection

SQL injection is a popular attack against web applications. A login screen requires a username and password, which must be checked against a database to see whether they are valid. All databases speak Structured Query Language (SQL). If the programmer who created the login is not careful it might be susceptible to SQL injection. Here is how that attack works. SQL looks a lot like English. For example, to check a username and password an intruder might want to query the database and see whether any entry in the users table matches the username and password that was entered. If there is, then a match exists.

13.3.2.2 Cross-Site Scripting (XSS)

An attacker injects a client-side script into web pages viewed by other users. The term cross-site scripting originally referred to the act of loading the attacked, third-party web application from an unrelated attack site, in a manner that executes a fragment of JavaScript prepared by the attacker in the security context of the targeted domain.

Essentially, an attacker enters scripts into an area that other users interact with, so that when they go to that part of the site, the attacker's script runs, rather than the intended website functionality. This can include redirecting users.

Hacking Wi-Fi

13.4 Hacking Wi-Fi

Wi-Fi is obviously a target for attack. Given its easy accessibility, it is likely that any attacker will at least attempt to breach your Wi-Fi. There are several common attacks you should be familiar with. Each of these can present a danger to your network.

- **Jamming:** This involves simply attempting to jam the Wi-Fi signal so that users cannot get on the wireless network. This is essentially a denial of service attack on the wireless access point.
- **De-authentication:** This is sending a de-authentication or logoff packet to the wireless access point. The packet will spoof the

user’s IP address. This can be done in order to trick the user into then logging in to the rogue access point.

- **WPS attack:** Wi-Fi Protected Setup (WPS) uses a PIN to connect to the wireless access point. The WPS attack attempts to intercept that PIN in transmission, connect to the WAP, and then steal the WPA2 password.
- **Cracking the password:** Actually, breaking the encryption is usually not something that is likely to succeed. However, cracking bad Wi-Fi passwords is certainly possible.

QUIZ:

- 1.Which of the following is the most reliable type of scan?
- 2.From a port scanning you identified that port 88 is open. What does this tell you?
- 3.If you send a SYN to an open port what is the correct response?
- 4.Trying to identify machines on a target network is called?
- 5.Julie has been hired to perform a penetration test on xyz.com. She begins by looking at IP address ranges owned by the company and details of domain name registration. She then goes to news groups and financial websites to see whether any of the company’s sensitive information or technical details are online. What is Julie doing?