5.1.9 Scanning Considerations Facts

This lesson covers the following topics:

- Scanning considerations
- Evasion
- Vulnerability scans
- Preventing banner grabbing

Scanning Considerations

You want to be strategic when you select which scanning tools and methods to use. Carefully consider the strengths and weaknesses of each scan type. Selecting the wrong method not only takes up valuable time, it also increases the chances that you will get caught.

Consider the time of day that you'll be doing your scans. Do you want to scan when there's a lot of network traffic in hopes that you'll blend in with the crowd? Or do you want to attempt to access the system in the middle of the night, or on the weekends when no one's around? There isn't necessarily a right or wrong answer to these questions, and your decisions could vary from one company to another depending on their operations.

Evasion

Even the stealthiest of ethical hackers are going to come across a few obstacles. After all, firewalls and security measures are typically in place to keep people like you out of the network. So, what can you do when you find that your scanning attempts are being blocked? A few options include scanning with ACK, fragmenting packets, spoofing IP addresses, and using a proxy.

Method	Description
Scan with ACK	This scan will help you determine whether the firewall is stateful or stateless and whether or not the ports are open. In an ACK scan, only the ACK flag is set. If a port is unfiltered, both open and closed ports return an RST packet. If a port is filtered, it either returns an error message or no response at all.
Fragment packets	Fragmenting is probably one of the most commonly used methods to avoid detection. You're still sending packets, you're just breaking them apart so intrusion detection systems don't know what they are. As long as you're not bombarding the system, the packet segments float by without concern.
Spoof IP addresses	Many scanning tools have the functionality to recraft the packet so that the source address reflects a different IP address. The scan is sent to the recipient, the feedback is returned to the fake IP address, and there is no record of your IP address sending the requests.
Use a proxy	A proxy serves as a less vulnerable access point to a network. Typically, proxies are placed in networks to keep external users from accessing the internal network. Hackers like proxies because they filter incoming and outgoing traffic, provide you with anonymity, and shield you from possible detection.

Vulnerability Scans

All organizations should perform regular vulnerability scans. Various tools have been designed to scan ports, banners, coding, and other high-target areas within a network for vulnerabilities. Similar to virus scanners and malware detectors, though, a vulnerability scan is only as good as its data. If a vulnerability is not included in the current database of issues that are being scanned for, an "all clear" result could be misleading. In addition to keeping your scanning tools up to date, you will want to use a variety of tools to be sure you're covering as much ground as possible. Also, keep in mind that if these tools are available to the companies you're working for, they are also available for hackers. Remind your clients that even if they aren't running these scans on a regular basis, someone else may be.

The following are a few of the vulnerability scanning tools available:

Tool	Description
Nessus	Nessus is often considered the industry standard for vulnerability scanning. The software helps to identify software flaws, malware, missing or outdated patches, and configuration errors across a network.
OpenVAS	OpenVAS provides authentication testing, protocol testing, and performance tuning for large-scale networks.
Beyond Trust	Beyond Trust provides a network security scanner that helps to identify vulnerabilities and prioritize solutions. This software is available as a standalone application or part of their larger vulnerability management solution.
InsightVM	Saint provides enterprise level vulnerability management tools.

Preventing Banner Grabbing

A few banner grabbing prevention options are available. One option is to disable the banners, or at least portions of the banner. Several utilities help to change or even remove the banner contents. Second, they'll want to hide file extensions. File extensions tell everyone what software is being used to create a web page. Hiding the file extension gives one less bit of information to an intruder. A third option to banner grabbing prevention is to enable custom error pages. This way, you have full control over what scanners can and cannot see when they trigger an error message.
