11.2.8 Reconnaissance Facts

Reconnaissance, also known as footprinting, is the process of gathering as much information about a target before beginning any penetration test or security audit. The more information we know about the target, the more prepared we can be for anything that may come up.

This lesson covers the following topics:

- Passive reconnaissance
- Active reconnaissance
- Reconnaissance tools

Passive Reconnaissance

Passive reconnaissance involves gathering information on the target with no direct interaction with that target. Valuable information can be gathered using passive reconnaissance. The following table shows some of the common passive reconnaissance methods:

Passive Reconnaissance Method	Description
Packet sniffing	Packet sniffing is the process of capturing data packets that are flowing across the network and analyzing them for important information. Modern networks should have good protection against network sniffing attacks, but there are occasional circumstances that allow an attacker to gather sensitive information from the data packets. Packet sniffing is most easily performed on open wireless networks. Because the attacker is not sending data or actively interacting with the target, this is considered passive reconnaissance. Scanning for open wireless networks needs to be done before packets can be sniffed. Two common methods are war driving and war flying: ▪ War driving is driving around with a wireless device looking for open, vulnerable wireless networks. ▪ War flying uses drones or unmanned aerial vehicles to find open wireless networks.
Eavesdropping	Eavesdropping is the act of covertly listening in on a communication between other people. This can include: ▪ Listening to employees conversations without them knowing. ▪ Shoulder surfing, which is an eavesdropping technique where the listener obtains passwords or other confidential information by looking over the shoulder of the target as the target logs on or types information. ▪ Dumpster diving, which is also considered eavesdropping. When dumpster diving, the attacker goes through the trash to find important information that may have accidentally been thrown away.
Open-source	Open-source intelligence is any data that is collected from publicly available sources.

intelligence (OSINT)	The goal is to gather as much personal identifiable information (PII) as possible. This includes information found from resources such as: ▪ Search engines (Google, Bing) ▪ Social media (Facebook, LinkedIn) ▪ Company websites (About sections of websites, company directories) ▪ Media sources (news sites, interviews, articles) ▪ Public government sources (property appraisal sites, public records)

Active Reconnaissance

After an attacker has gained as much information as possible through passive reconnaissance, the next step is the active reconnaissance phase.

Active reconnaissance is the process of gathering information by interacting with the target in some manner. Because there is direct interaction with the target, there is also a risk of exposure.

There are many different methods to perform active reconnaissance, but the goal is to gather additional information on the target, including:

- Network information
  - IP configurations
  - Domains and sub-domains
  - DNS information
- System information
  - Operating systems
  - Software versions
  - Usernames and passwords
  - Physical server locations
  - Additional organizational information

Performing reconnaissance provides the attacker with the information needed to perform a successful attack on the target. The goal is to know and understand the following information about the target:

- Security posture (this includes both network and physical security)
- How to narrow the focus for attack
- Potential vulnerabilities
- How to best create a network map

Reconnaissance Tools

There are many tools and resources available to assist in the reconnaissance phase. The below table covers some of the popular tools used:

Reconnaissance Tool	Description
OSINT framework	The OSINT framework is a collection of resources and tools that are separated by common categories. The OSINT Framework makes it easy to gather all sorts of information, making the initial reconnaissance process much more efficient. Documentation can be found at https://osintframework.com/

theHarvester	theHarvester is a passive reconnaissance tool that is used to gather information from a variety of public sources. The tool gathers emails, names, subdomains, IPs, and URLs using multiple public data sources. These sources include search engines, social media sites, and Shodan. theHarvester does have some options, such as brute-forcing DNS and taking screenshots, that would fall under active reconnaissance.
Shodan	Shodan is a popular search engines for internet-connected devices. Users are able to search for specific types of devices and locations. This information can be used to see if a target has any online devices without proper security.
Dnsenum	Dnsenum is a program that performs DNS enumeration and can find the DNS servers and entries for an organization. This information can help find other information such as usernames, computer names, IP addresses, and more.
Curl and wget	Curl and wget are two common command line programs that can be used to download or upload files. An example of using these tools is to download an entire website for offline analysis. Because these tools actively engage with the target, they are considered active reconnaissance tools.
scanless	scanless is used for port scanning. Instead of scanning ports from the hacker machine, scanless uses exploitation websites to perform port scans. This means the attacker is able to maintain anonymity while scanning the target.
Sn1per	Sn1per is a automated scanner that can be used to enumerate and scan for vulnerabilities. Sn1per combines the functions of many tools and can be used to find information such as DNS information, open ports, running services, and more.
Nessus	Nessus is a proprietary vulnerability scanner that is developed by Tenable. Nessus can be used to scan the target for any known vulnerabilities, which can be exploited to gain access to the target.

Selecting the right tool allows the attacker to gain the necessary information on the target. Network defenders can also use these tools to discover what information is out there and take the necessary steps to remove or hide anything that should not be available.