



Information Gathering

Introduction

Alexis Ahmed

Senior Penetration Tester @HackerSploit
Offensive Security Instructor @INE



aahmed@ine.com



@HackerSploit



@alexisahmed

Course Topic Overview

- + Introduction To Information Gathering
- + Passive Information Gathering
- + Active Information Gathering

- + Basic familiarity with Linux
- + Basic familiarity with web technologies

Prerequisites



Learning Objectives:

- Students will learn about the difference between active and passive information gathering.
- Students will learn how to perform passive information gathering by leveraging various tools and resources.
- Students will perform active information gathering.

Disclaimer

In this module you will see some examples of tools and techniques used on realistic IP addresses and hosts.

Never run any of these tools and techniques on those addresses or on any machine and network without proper authorization!



Let's Get Started!



Introduction To Information Gathering

What is Information Gathering?

- Information gathering is the first step of any penetration test and involves gathering or collecting information about an individual, company, website or system that you are targeting.
- The more information you have on your target, the more successful you will be during the latter stages of a penetration test.
- Information gathering is typically broken down into two types:
 - Passive information gathering - Involves gathering as much information as possible without actively engaging with the target.
 - Active information gathering - Involves gathering as much information as possible by actively engaging with the target system. (You will require authorization in order to perform active information gathering)

What Information Are We Looking For?

Passive Information Gathering

- + Identifying IP addresses & DNS information.
- + Identifying domain names and domain ownership information.
- + Identifying email addresses and social media profiles.
- + Identifying web technologies being used on target sites.
- + Identifying subdomains.

Active Information Gathering

- + Discovering open ports on target systems.
- + Learning about the internal infrastructure of a target network/organization.
- + Enumerating information from target systems.



Website Recon & Footprinting

What are we looking for

- + IP addresses
- + Directories hidden from search engines
- + Names
- + Email addresses
- + Phone Numbers
- + Physical Addresses
- + Web technologies being used



Practical Demo



Whois Enumeration



Practical Demo



Website Footprinting With Netcraft



Practical Demo



DNS Recon



Practical Demo



WAF Detection With wafw00f



Practical Demo



Subdomain Enumeration With Sublist3r



Practical Demo



Google Dorks



Practical Demo



Email Harvesting With theHarvester



Practical Demo



Leaked Password Databases



Practical Demo



DNS Zone Transfers

DNS

- + Domain Name System (DNS) is a protocol that is used to resolve domain names/hostnames to IP addresses.
- + During the early days of the internet, users would have to remember the IP addresses of the sites that they wanted to visit, DNS resolves this issue by mapping domain names (easier to recall) to their respective IP addresses.
- + A DNS server (nameserver) is like a telephone directory that contains domain names and their corresponding IP addresses.
- + A plethora of public DNS servers have been set up by companies like Cloudflare (1.1.1.1) and Google (8.8.8.8). These DNS servers contain the records of almost all domains on the internet.

DNS Records

- + A - Resolves a hostname or domain to an IPv4 address.
- + AAAA - Resolves a hostname or domain to an IPv6 address.
- + NS - Reference to the domains nameserver.
- + MX - Resolves a domain to a mail server.
- + CNAME - Used for domain aliases.
- + TXT - Text record.
- + HINFO - Host information.
- + SOA - Domain authority.
- + SRV - Service records.
- + PTR - Resolves an IP address to a hostname

DNS Interrogation

- + DNS interrogation is the process of enumerating DNS records for a specific domain.
- + The objective of DNS interrogation is to probe a DNS server to provide us with DNS records for a specific domain.
- + This process can provide with important information like the IP address of a domain, subdomains, mail server addresses etc.

DNS Zone Transfer

- + In certain cases DNS server admins may want to copy or transfer zone files from one DNS server to another. This process is known as a zone transfer.
- + If misconfigured and left unsecured, this functionality can be abused by attackers to copy the zone file from the primary DNS server to another DNS server.
- + A DNS Zone transfer can provide penetration testers with a holistic view of an organization's network layout.
- + Furthermore, in certain cases, internal network addresses may be found on an organization's DNS servers.



Practical Demo



Host Discovery With Nmap



Practical Demo



Port Scanning With Nmap



Practical Demo



Information Gathering

Conclusion



Learning Objectives:

- Students will learn about the difference between active and passive information gathering.
- Students will learn how to perform passive information gathering by leveraging various tools and resources.
- Students will perform active information gathering.



Thank You!