TIMOTHY SEWE OGODE(CSSA0423076)

CYBER SHUJAA

WEEK 3

PASSIVE RECONNAISSANCE

Table of Contents

[1. INTRODUCTION 2](#_Toc136535198)

[2. PASSIVE VS ACTIVE 2](#_Toc136535199)

[3. WHOIS 2](#_Toc136535200)

[4. NSLOOKUP and DIG 2](#_Toc136535201)

[5. DNSDUMPSTER 2](#_Toc136535202)

[6. SHODAN.IO 3](#_Toc136535203)

[7. CONCLUSION 3](#_Toc136535204)

# INTRODUCTION

Passive reconnaissance in cybersecurity is a crucial initial phase of information gathering, where attackers employ non-intrusive methods to gather intelligence about a target network or system. By passively observing and analysing publicly available data, such as network configurations, domain information, and employee details, adversaries aim to identify vulnerabilities and potential attack vectors, thereby laying the groundwork for a successful breach. This covert approach allows cyber defenders to proactively assess their security posture, anticipate threats, and fortify defences against potential incursions.

# PASSIVE VS ACTIVE

Passive reconnaissance involves accessing publicly available data without direct engagement. Examples include checking DNS records, reviewing job ads, and reading news articles. In contrast, active reconnaissance requires direct interaction with the target, such as connecting to servers or employing social engineering tactics.

# WHOIS

WHOIS is a request and response protocol specified by RFC 3912, where a WHOIS server listens on TCP port 43 to handle incoming requests. Domain registrars maintain WHOIS records for the domains they lease, providing valuable information. By querying a WHOIS server, one can learn the registrar responsible for the domain, registrant contact details (unless privacy services are in place), creation, update, and expiration dates of the domain, as well as the name server associated with it. Accessing the WHOIS client locally, such as through the AttackBox or a Linux machine, allows for convenient and speedy retrieval of this information by using the syntax "whois DOMAIN\_NAME" in the terminal.

# NSLOOKUP and DIG

Nslookup and dig are powerful command-line tools used in networking and DNS troubleshooting. Nslookup is a traditional utility available on most operating systems that allows users to query DNS servers for information about domain names, IP addresses, and other DNS records. By typing "nslookup" followed by the domain or IP address, users can obtain details such as the corresponding IP address, hostname, and even perform reverse DNS lookups. Dig, short for "domain information groper," is a more advanced tool commonly found on Unix-like systems. It provides comprehensive DNS information, including querying specific DNS record types, specifying the DNS server to query, and displaying detailed response headers. Both nslookup and dig are indispensable tools for network administrators, system engineers, and anyone working with DNS-related tasks, aiding in troubleshooting and gaining insights into DNS configurations.

# DNSDUMPSTER

DNSDumpster is a popular online tool used for DNS reconnaissance and information gathering. It allows users to perform various queries on a target domain to gather details such as DNS records, subdomains, and associated IP addresses. By entering the domain name in DNSDumpster, users can retrieve a comprehensive report containing information like DNS server information, mail server details, open ports, and even visualize the domain's infrastructure.

# SHODAN.IO

This a powerful search engine that specializes in internet-connected devices and services. Unlike traditional search engines that focus on website content, Shodan.io allows users to search for specific types of devices, such as webcams, routers, servers, and even industrial control systems. By leveraging various scanning techniques, Shodan.io collects information about these devices, including open ports, banners, and other metadata. This enables users to discover potentially vulnerable or misconfigured devices that may be exposed to the internet.

# CONCLUSION

In conclusion, the various tools and techniques discussed in this report highlight the importance of reconnaissance and information gathering in cybersecurity. Passive reconnaissance, utilizing publicly available data, allows for a non-intrusive assessment of target systems, while active reconnaissance involves direct engagement and interaction with the target. Tools such as WHOIS, nslookup, dig, and platforms like DNSDumpster and Shodan.io provide valuable insights into domains, DNS records, IP addresses, and internet-connected devices.

A screenshot of a computer

Description automatically generated with medium confidence