«host\_docx»

Reconnaissance Findings Report

Date: «current\_date\_docx»

Version: «version\_docx»

# **Assessment Overview**

## **Executive Summary**

«company\_name\_docx» evaluated «host\_docx» internal security posture through penetration testing on «current\_date\_docx». The following sections provide information based on reconnaissance or enumeration.

## **Testing Summary**

The network assessment evaluated «host\_docx»’s internal network security posture. From an internal perspective, the «company\_name\_docx» team performed vulnerability scanning against «host\_docx» to evaluate the overall patching health of the network. The team also performed «tools\_used\_docx».

The «company\_name\_docx» team discovered that «host\_docx» is using «os\_host\_docx» and based on the Nmap scan performed, the target has «total\_services\_docx» service(s) running. Those service(s) are «services\_docx».

## **Objective**

The objective of this report is to gather information about OS used, port(s) opened, service(s) opened, vulnerability assessment, and reconnaissance or enumeration of the services that were running in the target.

# **Reconnaissance Result**

## **Initial Data**

### Nmap

Nmap is used in the beginning of the reconnaissance to get the initial data needed, for instance port and services used in target, and vulnerability assessment using vulners as wordlist.

|  |
| --- |
| Nmap |
| «nmap\_docx» |

The target using «os\_host\_docx» and has «total\_services\_docx» service(s) running. Those service(s) are «services\_docx».

### DNS Lookup

The **dig** command in Linux is used to gather DNS information. It stands for Domain Information Groper, and it collects data about Domain Name Servers. Other than dig, the program used dnsenum to gather dns datas, for instance MX, mail exchange servers, NS, domain name servers, or the address record for a domain.

|  |
| --- |
| dig |
| «dig\_docx» |
| dnsenum |
| «dnsenum\_docx» |

### Google Dorking

Google Dork is a technique that utilizes the Google search engine to get various important or sensitive information that is not generally available on the web.

|  |
| --- |
| «gdorks\_docx» |

### VirusTotal

Using the VirusTotal API, the program will check «host\_docx»’s reputation based on the report from security vendor such as Avira, BitDefender, Fortinet, Kaspersky, and many more.

|  |
| --- |
| «virustotal\_docx» |

### Shodan

Using the Shodan API, the program will check «host\_docx»’s top five organizations, top 5 domains, top 5 ports, and top 5 countries that were related to the «host\_docx».

|  |
| --- |
| «shodan\_docx» |

## **FTP**

The **File Transfer Protocol (FTP**) is a standard network protocol used for the transfer of computer files between a client and server on a computer network. In this part, the program tries to brute-force the FTP login credentials using wget with “ftp-betterdefaultpasslist.txt” as the default wordlist.

|  |
| --- |
| «ftp\_docx» |

## **SSH**

**Secure Shell** or **Secure Socket Shell** is a network protocol that gives users a secure way to access a computer over an unsecured network. The program scans the service using nmap with ssh2-enum-algos, ssh-hostkey, and ssh-auth-methods as wordlists.

|  |
| --- |
| «ssh\_docx» |

## **HTTP or HTTPS**

### Directory Fuzzing

Performed by using gobuster and dirsearch to find some of the “hidden paths” the target has. Gobuster using “directory-list-2.3-medium.txt” as a default wordlist and dirbuster using their default wordlist.

|  |
| --- |
| Gobuster |
| «gobuster\_dir\_docx» |
| Dirsearch |
| «dirsearch\_docx» |

### Subdomain Fuzzing

Performed by using gobuster to find subdomain the target has. Gobuster using “subdomain-wordlist.txt” as a default wordlist and dirbuster using their default wordlist.

|  |
| --- |
| «gobuster\_subdomain\_docx» |

### Web Server Vulnerability Scan

|  |
| --- |
| Nikto |
| «nikto\_docx» |

1. Wordpress Vulnerability Scan

|  |
| --- |
| Wpscan |
| «wpscan\_docx» |

## **POP**

**Post Office Protocol (POP)** is a type of computer networking and internet standard protocol that extracts and retrieves email from a remote mail server for access by the host machine. The POP clients generally connect, retrieve all messages, store them on the client system, and delete them from the server. There are 3 versions of POP, but POP3 is the most used one.

|  |
| --- |
| «pop\_docx» |

## **Samba**

**Server Message Block (SMB)** is a client-server protocol that regulates **access to files** and entire directories and other network resources such as printers, routers, or interfaces released for the network. In this part, enum4linux will be used to do nmblookup, get password policy information, brute force share names, and get userlist(s).

|  |
| --- |
| «enum4linux\_docx» |

## **NetBios Name Service**

**The NetBIOS Name Service (NBNS)** is part of the **NetBIOS-over-TCP/IP (NBT/NetBT)** protocol suite that allows legacy computer applications relying on the NetBIOS Application Programming Interface (API) to be used on TCP/IP networks. For reconnaissance, the program will use nmblookup to check node status on the target and nmap with nbtstat as wordlist.

|  |
| --- |
| «netbios\_docx» |

## **LDAP**

**LDAP (Lightweight Directory Access Protocol)** is a software protocol for enabling anyone to locate organizations, individuals, and other resources such as files and devices in a network, whether on the public Internet or on a corporate intranet. Nmap will be used to scan the target, using ldap-rootdse as wordlist.

|  |
| --- |
| «ldap\_docx» |

## **Microsoft SQL**

**Microsoft SQL Server (MSSQL)** is a relational database management system developed by Microsoft. Nmap will be used to scan the target using ms-sql-info, ms-sql-empty-password, ms-sql-xp-cmdshell, ms-sql-config, ms-sql-ntlm-info, ms-sql-tables, ms-sql-hasdbaccess, ms-sql-dac, ms-sql-dump-hashes wordlists.

|  |
| --- |
| «mssql\_docx» |

## **MySQL**

**MySQL** is a freely available open-source Relational Database Management System (RDBMS) that uses **Structured Query Language (SQL)**. Nmap will be used to scan the target using mysql-audit, mysql-databases, mysql-dump-hashes, mysql-empty-password, mysql-enum, mysql-info, mysql-query, mysql-users, mysql-variables, mysql-vuln-cve2012-2122 as wordlists.

|  |
| --- |
| «mysql\_docx» |