Automated Reconnaissance

BashRecon– Ashley Nanni

Objective

The objective of the script is to perform a targeted reconnaissance and enumeration scan against a specified IP address. Serving as an extensible tool to simplify initial reconnaissance by automating steps to identify open ports, services, potential vulnerabilities with Metasploit module recommendations, and providing insights for penetration testing or vulnerability assessment.

Tools Used

Nmap for network scanning, discovering hosts, and identifying open ports.

Gobuster to enumerate directories and files on the web server

WhatWeb to fingerprint web applications and identify technologies or frameworks in use.

Metasploit an exploitation framework that is used for exploiting vulnerabilities.

Intended Use

* Ethical Hacking: Gather initial information about a target
* Vulnerability Assessment: To identify potential weaknesses or misconfigurations in a system.
* Learning: Practicing reconnaissance techniques

Required Tools/Info Needed

For the script to run properly user must have the following installed on their Kali machine: Nmap, Gobuster, Whatweb, and Metasploit. The user **must run a host discovery scan** on the entire network using cider notation to identify target machine.

Key Features of the Script

* **Port Scanning and Service Enumeration:**
* Utilizes nmap to scan the target for open ports and identify running services, capturing detailed information about versions and protocols.
* **HTTP Service Reconnaissance:**
* If HTTP services are detected (e.g., port 80), the script:
  + Runs **Gobuster** to identify hidden directories or files on the web server.
  + Executes **WhatWeb** to fingerprint web applications and determine underlying technologies.
* **Vulnerability Identification:**
* Checks for services commonly associated with vulnerabilities, and suggest a module in Metasploit that could be used (reference exploitations below)
* Logs exploit suggestions for manual follow-up.
* **Report Generation:**
* All findings are consolidated into a results HTML file for easy review, including:
  + Identified services and ports.
  + Reconnaissance tool outputs.
  + Exploit recommendations.

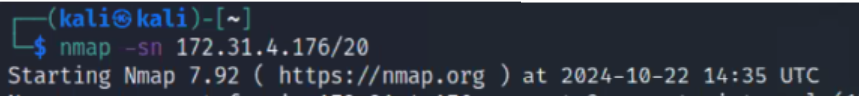
Loading Script for use

1. vim ./Xplor.sh
2. To enter insert mode -- Press Esc and then type I
3. Copy > paste script into Vim
4. To save and Exit: Press Esc and then type :x > enter
5. From the terminal: chmod +x Xplor.sh
6. To run the script, enter ./Xplor.sh 192.168.56.102 (note the IP address should match your target machine

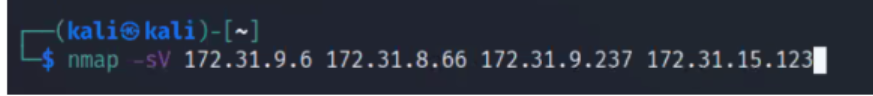
Running Nmap & Host Discovery Scan

Step 1: find your own IP using ip a or host name -I

Step 2: run a host discovery scan on the entire network using CIDER notation



Step 3: running service version scans on any machines of interest



Script Breakdown

1. Nmap Scans:
   * Aggressive mode (-A) enables OS detection, version detection, script scanning, and traceroute
     + OS Detection: Attempts to determine the target's operating system.
     + Version Detection: Tries to identify the versions of services running on open ports.
     + Traceroute: Maps the route packets take to the target.
     + Default Scripts: Runs a set of commonly used Nmap scripts (e.g., for banner grabbing, SSL/TLS analysis, etc.).
   * Timing template (-T4) set to aggressive level 4
     + Nmap has six timing templates ranging from T0 (Paranoid) to T5 (Insane).
     + T4 speeds up the scan by reducing delays between probes but may cause network congestion or be more easily detected by intrusion detection systems (IDS).
   * Stealth Scan (-sS)
     + Sends SYN packets to the target, trying to initiate a TCP connection but doesn't complete it.
     + If the target responds with a SYN-ACK, it means the port is open.
     + If it responds with RST, the port is closed.
     + This scan is fast and stealthier compared to a full TCP connect scan (-sT), as it does not complete the handshake
2. Gobuster is a tool used for directory and file brute-forcing. Often used in security assessments to discover hidden paths or files on a web server that might not be immediately visible or accessible through regular browsing.
   * Directory Enumeration (dir)
     + Directory Brute-forcing: Uses a wordlist to attempt to discover directories or files by appending names to the target URL.
   * Wordlist (-w)
     + Customizable Wordlist: Custom wordlists tailored to your target or rely on predefined lists (e.g., Seclists).
3. WhatWeb is a web application fingerprinting tool that helps to gather detailed information about websites.
   * WhatWeb works by sending HTTP requests to a target URL and analyzing the responses. Focused on HTTP Headers, HTML content, JavaScript, and Cookies.
     + Checking for unique signatures or patterns that correspond to specific technologies
4. Potential Exploits Identified with recommended Metasploit module and/or manual actions
   * **Potential TCP Exploit: Netgear TelnetEnable Command Injection (Port 23):** 
     + Telnet is a text-based network protocol that is used for accessing remote computers over TCP/IP networks like the Internet.
     + This vulnerability exists in devices that have the **Telnet** service enabled, and it allows attackers to execute arbitrary commands on the device via **command injection.**
     + **Metasploit Module:** exploit/linux/telnet/netgear\_telnetenable
   * **Potential FTP Exploit: vsftpd 2.3.4 Backdoor Command Execution (Port 21):**
     + an FTP server that contains a backdoor, which was inserted into the code by an unknown intruder.
     + This backdoor enables remote code execution, allowing an attacker to take control of the affected system.
     + **Metasploit Module:** exploit/unix/ftp/vsftpd\_234\_backdoor
   * **Potential Exploit: HTTP Related (Ports 80 & 8180)**
     + **Port 80:** General Web Server Vulnerabilities (e.g., Apache, Nginx, IIS)
       - Cross-Site Scripting (XSS): Attackers inject malicious scripts into web pages to steal cookies, perform actions on behalf of users, or spread malware.
       - SQL Injection: If a web application improperly validates user inputs, attackers can manipulate SQL queries to access or modify the database.
       - Remote File Inclusion (RFI): Malicious users can include remote files that may execute arbitrary code.
       - Denial of Service (DoS): Servers might be vulnerable to flooding or resource-exhausting attacks (e.g., HTTP flood, slowloris).
       - Unpatched Vulnerabilities: Known vulnerabilities in the web server or CMS (WordPress, Joomla, etc.) could be exploited if the system is not up to date.
       - Insecure HTTP Methods: HTTP methods such as PUT or DELETE may be enabled by default and can be exploited to upload or delete files.
       - **Metasploit Module:** exploit/unix/webapp/joomla\_sql\_injection
     + **Port 8180**:
       - Apache Tomcat is an open-source application server that executes Java servlets and JavaServer Pages. If misconfigured or running an outdated version, the following vulnerabilities may arise:
       - Remote Code Execution (RCE): Exploits targeting outdated versions of Tomcat can allow attackers to execute arbitrary commands on the server.
       - Directory Traversal: Attackers could access files outside of the web server’s root directory.
       - Default Credentials: services that have weak or default login credentials
       - Privilege Escalation: Flaws in the web application running on Tomcat might allow attackers to escalate privileges and access sensitive data.
       - **Metasploit Module:** exploit/multi/http/tomcat\_mgr\_upload
   * **SSH KEY Exploit (Port 22):** 
     + Weak or misconfigured SSH keys, improper access control, exposed/leaked SSH keys or weakness in the SSH protocol..
     + Manual enumeration recommended for credential brute-forcing or privilege escalation: **John the Ripper** or **Hashcat** tools with a .pem key file
     + **Metasploit Module (SSH Brute force):** auxiliary/scanner/ssh/ssh\_login
     + **Metasploit Module (SSH Keys):** auxiliary/scanner/ssh/ssh\_keyscan
   * **Potential IRC Exploit: UnrealIRCd 3.2.8.1 Backdoor Command Execution**
     + **Cause**: The source code was compromised and distributed with a backdoor, allowing remote attackers to execute system-level commands.
     + **Metasploit Module:** exploit/unix/irc/unreal\_ircd\_3281\_backdoor

**Script**

#!/bin/bash

# Check if a target IP is provided

if [ -z "$1" ]; then

    echo "Usage: ./Xplorr.sh <Target IP>"

    exit 1

fi

# Assign the target IP

TARGET=$1

# Initialize results file

RESULTS\_FILE="results"

RESULTS\_HTML="results.html"

printf "\n----- SCAN RESULTS FOR $TARGET -----\n\n" > "$RESULTS\_FILE"

# Add formatted headers

add\_header() {

    printf "\n\n=====  $1  =====\n\n" >> "$RESULTS\_FILE"

}

# Run Nmap for detailed port scan and service detection

echo "Running Nmap... curiosity may get you into trouble, but with Nmap, at least it will show you what kind of trouble..."

nmap -sV -A  -T4 "$TARGET" > nmap\_temp

add\_header "NMAP RESULTS"

cat nmap\_temp >> "$RESULTS\_FILE"

# Extract OS details

OS=$(grep "OS details" nmap\_temp | cut -d: -f2 | xargs)

printf "\nDetected OS: $OS\n" >> "$RESULTS\_FILE"

# Process Nmap results

while read -r line; do

    if [[ $line == \*open\* ]]; then

        # Extract port number

        PORT=$(echo "$line" | grep -oE '^[0-9]+')

        # HTTP services on port 80 and 8180

        if [[ $line == \*http\* ]]; then

            add\_header " HTTP Service detected on port $PORT "

            echo "- Potential Apache Tomcat Exploitation (Metasploit: exploit/multi/http/tomcat\_mgr\_upload)" >> "$RESULTS\_FILE"

            echo " -Potential HTTP Server Exploitation (Metasploit: exploit/unix/webapp/joomla\_sql\_injection)" >> "$RESULTS\_FILE"

            # Run Gobuster for directory enumeration

            gobuster dir -u http://"$TARGET" -w /usr/share/seclists/Discovery/Web-Content/big.txt -qz > gobuster\_temp 2>/dev/null

            if [ -s gobuster\_temp ]; then

                printf "\n----- GOBUSTER RESULTS (Port $PORT) -----\n\n" >> "$RESULTS\_FILE"

                cat gobuster\_temp >> "$RESULTS\_FILE"

            else

                printf "\n----- GOBUSTER RESULTS (Port $PORT) -----\nNo directories found.\n\n" >> "$RESULTS\_FILE"

            fi

            rm gobuster\_temp

            # Run WhatWeb for web fingerprinting

            whatweb -v http://"$TARGET" > whatweb\_temp 2>/dev/null

            if [ -s whatweb\_temp ]; then

                printf "\n----- WHATWEB RESULTS (Port $PORT) -----\n\n" >> "$RESULTS\_FILE"

                cat whatweb\_temp >> "$RESULTS\_FILE"

            else

                printf "\n----- WHATWEB RESULTS (Port $PORT) -----\nNo web application data found.\n\n" >> "$RESULTS\_FILE"

            fi

            rm whatweb\_temp

        fi

        # SSH services on port 22

        if [[ $line == \*ssh\* ]] && [[ $line == \*22/tcp\* ]]; then

            printf "\nSSH service detected on port $PORT\n" >> "$RESULTS\_FILE"

            ssh-keyscan -H $TARGET > ssh\_keys\_temp 2>/dev/null

            echo " -Potential SSH Brute Force (Metasploit: auxiliary/scanner/ssh/ssh\_login)" >> "$RESULTS\_FILE"

            echo " -Potential SSH Keys (Metasploit: auxiliary/scanner/ssh/ssh\_keyscan)" >> "$RESULTS\_FILE"

            add\_header "SSH KEYS (Port $PORT)"

            printf "\n----- SSH KEYS -----\n\n" >> "$RESULTS\_FILE"

            cat ssh\_keys\_temp >> "$RESULTS\_FILE"

        fi

        # IRC services (detects potential backdoors)

        if [[ $line == \*irc\* ]]; then

            printf "\nIRC backdoor service detected on port $PORT\n" >> "$RESULTS\_FILE"

            echo "- Potential IRC Exploit: UnrealIRCd 3.2.8.1 Backdoor Command Execution (Metasploit: exploit/unix/irc/unreal\_ircd\_3281\_backdoor)" >> "$RESULTS\_FILE"

        fi

        # FTP services on port 21

        if [[ $line == \*ftp\* ]] && [[ $line == \*21/tcp\* ]]; then

            printf "\nFTP service detected on port $PORT\n" >> "$RESULTS\_FILE"

            echo "- Potential FTP Exploit: vsftpd 2.3.4 Backdoor Command Execution (Metasploit: exploit/unix/ftp/vsftpd\_234\_backdoor)" >> "$RESULTS\_FILE"

        fi

        # Telnet services on port 23 (backdoor exploitation)

        if [[ $line == \*telnet\* ]] && [[ $line == \*23/tcp\* ]]; then

            printf "\nTelnet service detected on port $PORT\n" >> "$RESULTS\_FILE"

            echo "- Potential TCP Exploit: Netgear TelnetEnable Command Injection (Metasploit: exploit/linux/telnet/netgear\_telnetenable)" >> "$RESULTS\_FILE"

        fi

    fi

done < nmap\_temp

rm nmap\_temp

# Generate HTML output

echo "<html><body><h1>Scan Results for $TARGET</h1><pre>" > "$RESULTS\_HTML"

cat "$RESULTS\_FILE" >> "$RESULTS\_HTML"

# Display final results

cat "$RESULTS\_FILE"

HTML Output Results

**Scan Results for 192.168.56.102**

----- SCAN RESULTS FOR 192.168.56.102 -----

===== NMAP RESULTS =====

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-25 12:48 EST

Nmap scan report for 192.168.56.102

Host is up (0.00051s latency).

Not shown: 977 closed tcp ports (reset)

PORT STATE SERVICE VERSION

21/tcp open ftp vsftpd 2.3.4

|\_ftp-anon: Anonymous FTP login allowed (FTP code 230)

| ftp-syst:

| STAT:

| FTP server status:

| Connected to 192.168.56.103

| Logged in as ftp

| TYPE: ASCII

| No session bandwidth limit

| Session timeout in seconds is 300

| Control connection is plain text

| Data connections will be plain text

| vsFTPd 2.3.4 - secure, fast, stable

|\_End of status

22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)

| ssh-hostkey:

| 1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)

|\_ 2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)

23/tcp open telnet Linux telnetd

25/tcp open smtp Postfix smtpd

| sslv2:

| SSLv2 supported

| ciphers:

| SSL2\_RC2\_128\_CBC\_WITH\_MD5

| SSL2\_RC2\_128\_CBC\_EXPORT40\_WITH\_MD5

| SSL2\_DES\_192\_EDE3\_CBC\_WITH\_MD5

| SSL2\_RC4\_128\_WITH\_MD5

| SSL2\_RC4\_128\_EXPORT40\_WITH\_MD5

|\_ SSL2\_DES\_64\_CBC\_WITH\_MD5

|\_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN

| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX

| Not valid before: 2010-03-17T14:07:45

|\_Not valid after: 2010-04-16T14:07:45

|\_ssl-date: 2024-11-25T17:48:47+00:00; 0s from scanner time.

53/tcp open domain ISC BIND 9.4.2

| dns-nsid:

|\_ bind.version: 9.4.2

80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)

|\_http-title: Metasploitable2 - Linux

|\_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2

111/tcp open rpcbind 2 (RPC #100000)

| rpcinfo:

| program version port/proto service

| 100000 2 111/tcp rpcbind

| 100000 2 111/udp rpcbind

| 100003 2,3,4 2049/tcp nfs

| 100003 2,3,4 2049/udp nfs

| 100005 1,2,3 37131/tcp mountd

| 100005 1,2,3 54660/udp mountd

| 100021 1,3,4 43431/udp nlockmgr

| 100021 1,3,4 51810/tcp nlockmgr

| 100024 1 38335/udp status

|\_ 100024 1 41080/tcp status

139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

445/tcp open netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)

512/tcp open exec netkit-rsh rexecd

513/tcp open login OpenBSD or Solaris rlogind

514/tcp open shell Netkit rshd

1099/tcp open java-rmi GNU Classpath grmiregistry

1524/tcp open bindshell Metasploitable root shell

2049/tcp open nfs 2-4 (RPC #100003)

2121/tcp open ftp ProFTPD 1.3.1

3306/tcp open mysql MySQL 5.0.51a-3ubuntu5

| mysql-info:

| Protocol: 10

| Version: 5.0.51a-3ubuntu5

| Thread ID: 26

| Capabilities flags: 43564

| Some Capabilities: Support41Auth, SupportsTransactions, ConnectWithDatabase, SupportsCompression, Speaks41ProtocolNew, SwitchToSSLAfterHandshake, LongColumnFlag

| Status: Autocommit

|\_ Salt: \*UOn[\;Tq^bRR'hXbbDk

5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7

| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX

| Not valid before: 2010-03-17T14:07:45

|\_Not valid after: 2010-04-16T14:07:45

|\_ssl-date: 2024-11-25T17:48:47+00:00; 0s from scanner time.

5900/tcp open vnc VNC (protocol 3.3)

| vnc-info:

| Protocol version: 3.3

| Security types:

|\_ VNC Authentication (2)

6000/tcp open X11 (access denied)

6667/tcp open irc UnrealIRCd

8009/tcp open ajp13 Apache Jserv (Protocol v1.3)

|\_ajp-methods: Failed to get a valid response for the OPTION request

8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1

|\_http-favicon: Apache Tomcat

|\_http-title: Apache Tomcat/5.5

|\_http-server-header: Apache-Coyote/1.1

MAC Address: 08:00:27:E0:96:05 (Oracle VirtualBox virtual NIC)

Device type: general purpose

Running: Linux 2.6.X

OS CPE: cpe:/o:linux:linux\_kernel:2.6

OS details: Linux 2.6.9 - 2.6.33

Network Distance: 1 hop

Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux\_kernel

Host script results:

| smb-os-discovery:

| OS: Unix (Samba 3.0.20-Debian)

| Computer name: metasploitable

| NetBIOS computer name:

| Domain name: localdomain

| FQDN: metasploitable.localdomain

|\_ System time: 2024-11-25T12:48:38-05:00

|\_smb2-time: Protocol negotiation failed (SMB2)

|\_clock-skew: mean: 1h14m59s, deviation: 2h30m00s, median: 0s

|\_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: , NetBIOS MAC: (unknown)

| smb-security-mode:

| account\_used:

| authentication\_level: user

| challenge\_response: supported

|\_ message\_signing: disabled (dangerous, but default)

TRACEROUTE

HOP RTT ADDRESS

1 0.50 ms 192.168.56.102

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 22.85 seconds

Detected OS: Linux 2.6.9 - 2.6.33

===== FTP Backdoor Vulnerability Detected on port 21 =====

- Potential FTP Exploit: vsftpd 2.3.4 Backdoor Command Execution (Metasploit: exploit/unix/ftp/vsftpd\_234\_backdoor)

-Potential SSH Brute Force (Metasploit: auxiliary/scanner/ssh/ssh\_login)

-Potential SSH Keys (Metasploit: auxiliary/scanner/ssh/ssh\_keyscan)

===== SSH KEYS (Port 22) =====

# 192.168.56.102:22 SSH-2.0-OpenSSH\_4.7p1 Debian-8ubuntu1

|1|5QNZNR+4GHxeK7Bn4oSYCxyOwnw=|eaps8WtBoOp6wI6QIqWxrXqpOUY= ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAstqnuFMBOZvO3WTEjP4TUdjgWkIVNdTq6kboEDjteOfc65TlI7sRvQBwqAhQjeeyyIk8T55gMDkOD0akSlSXvLDcmcdYfxeIF0ZSuT+nkRhij7XSSA/Oc5QSk3sJ/SInfb78e3anbRHpmkJcVgETJ5WhKObUNf1AKZW++4Xlc63M4KI5cjvMMIPEVOyR3AKmI78Fo3HJjYucg87JjLeC66I7+dlEYX6zT8i1XYwa/L1vZ3qSJISGVu8kRPikMv/cNSvki4j+qDYyZ2E5497W87+Ed46/8P42LNGoOV8OcX/ro6pAcbEPUdUEfkJrqi2YXbhvwIJ0gFMb6wfe5cnQew==

# 192.168.56.102:22 SSH-2.0-OpenSSH\_4.7p1 Debian-8ubuntu1

# 192.168.56.102:22 SSH-2.0-OpenSSH\_4.7p1 Debian-8ubuntu1

# 192.168.56.102:22 SSH-2.0-OpenSSH\_4.7p1 Debian-8ubuntu1

# 192.168.56.102:22 SSH-2.0-OpenSSH\_4.7p1 Debian-8ubuntu1

===== TELENET Vulnerability Detected on port 23 =====

- Potential TCP Exploit: Netgear TelnetEnable Command Injection (Metasploit: exploit/linux/telnet/netgear\_telnetenable)

===== HTTP Service detected on port 80 =====

- Potential Apache Tomcat Exploitation (Metasploit: exploit/multi/http/tomcat\_mgr\_upload)

-Potential HTTP Server Exploitation (Metasploit: exploit/unix/webapp/joomla\_sql\_injection)

----- GOBUSTER RESULTS (Port 80) -----

[2K/.htpasswd (Status: 403) [Size: 296]

[2K/.htaccess (Status: 403) [Size: 296]

[2K/cgi-bin/ (Status: 403) [Size: 295]

[2K/dav (Status: 301) [Size: 319] [--> http://192.168.56.102/dav/]

[2K/index (Status: 200) [Size: 891]

[2K/phpMyAdmin (Status: 301) [Size: 326] [--> http://192.168.56.102/phpMyAdmin/]

[2K/phpinfo (Status: 200) [Size: 48008]

[2K/server-status (Status: 403) [Size: 300]

[2K/test (Status: 301) [Size: 320] [--> http://192.168.56.102/test/]

[2K/tikiwiki (Status: 301) [Size: 324] [--> http://192.168.56.102/tikiwiki/]

[2K/twiki (Status: 301) [Size: 321] [--> http://192.168.56.102/twiki/]

----- WHATWEB RESULTS (Port 80) -----

WhatWeb report for [1m[34mhttp://192.168.56.102[0m

Status : 200 OK

Title : [1m[33mMetasploitable2 - Linux[0m

IP : 192.168.56.102

Country : [1m[31mRESERVED, ZZ[0m

Summary : [1mApache[0m[[1m[32m2.2.8[0m], [1mHTTPServer[0m[[1m[31mUbuntu Linux[0m][[1m[36mApache/2.2.8 (Ubuntu) DAV/2[0m], [1mPHP[0m[[1m[32m5.2.4-2ubuntu5.10[0m], [1mWebDAV[0m[[1m[32m2[0m], [1mX-Powered-By[0m[[0m[22mPHP/5.2.4-2ubuntu5.10[0m]

Detected Plugins:

[ [1mApache[0m ]

The Apache HTTP Server Project is an effort to develop and

maintain an open-source HTTP server for modern operating

systems including UNIX and Windows NT. The goal of this

project is to provide a secure, efficient and extensible

server that provides HTTP services in sync with the current

HTTP standards.

Version : [1m[32m2.2.8[0m (from HTTP Server Header)

Google Dorks: (3)

Website : http://httpd.apache.org/

[ [1mHTTPServer[0m ]

HTTP server header string. This plugin also attempts to

identify the operating system from the server header.

OS : [1m[31mUbuntu Linux[0m

String : [1m[36mApache/2.2.8 (Ubuntu) DAV/2[0m (from server string)

[ [1mPHP[0m ]

PHP is a widely-used general-purpose scripting language

that is especially suited for Web development and can be

embedded into HTML. This plugin identifies PHP errors,

modules and versions and extracts the local file path and

username if present.

Version : [1m[32m5.2.4-2ubuntu5.10[0m

Google Dorks: (2)

Website : http://www.php.net/

[ [1mWebDAV[0m ]

Web-based Distributed Authoring and Versioning (WebDAV) is

a set of methods based on the Hypertext Transfer Protocol

(HTTP) that facilitates collaboration between users in

editing and managing documents and files stored on World

Wide Web servers. - More Info:

http://en.wikipedia.org/wiki/WebDAV

Version : [1m[32m2[0m

[ [1mX-Powered-By[0m ]

X-Powered-By HTTP header

String : [1m[36mPHP/5.2.4-2ubuntu5.10[0m (from x-powered-by string)

HTTP Headers:

HTTP/1.1 200 OK

Date: Mon, 25 Nov 2024 17:48:55 GMT

Server: Apache/2.2.8 (Ubuntu) DAV/2

X-Powered-By: PHP/5.2.4-2ubuntu5.10

Content-Length: 891

Connection: close

Content-Type: text/html

===== FTP Backdoor Vulnerability Detected on port 2121 =====

- Potential FTP Exploit: vsftpd 2.3.4 Backdoor Command Execution (Metasploit: exploit/unix/ftp/vsftpd\_234\_backdoor)

===== IRC Backdoor Vulnerability Detected on port 6667 =====

- Potential IRC Exploit: UnrealIRCd 3.2.8.1 Backdoor Command Execution (Metasploit: exploit/unix/irc/unreal\_ircd\_3281\_backdoor)

===== HTTP Service detected on port 8180 =====

- Potential Apache Tomcat Exploitation (Metasploit: exploit/multi/http/tomcat\_mgr\_upload)

-Potential HTTP Server Exploitation (Metasploit: exploit/unix/webapp/joomla\_sql\_injection)

----- GOBUSTER RESULTS (Port 8180) -----

[2K/.htaccess (Status: 403) [Size: 296]

[2K/.htpasswd (Status: 403) [Size: 296]

[2K/cgi-bin/ (Status: 403) [Size: 295]

[2K/dav (Status: 301) [Size: 319] [--> http://192.168.56.102/dav/]

[2K/index (Status: 200) [Size: 891]

[2K/phpMyAdmin (Status: 301) [Size: 326] [--> http://192.168.56.102/phpMyAdmin/]

[2K/phpinfo (Status: 200) [Size: 48008]

[2K/server-status (Status: 403) [Size: 300]

[2K/test (Status: 301) [Size: 320] [--> http://192.168.56.102/test/]

[2K/tikiwiki (Status: 301) [Size: 324] [--> http://192.168.56.102/tikiwiki/]

[2K/twiki (Status: 301) [Size: 321] [--> http://192.168.56.102/twiki/]

----- WHATWEB RESULTS (Port 8180) -----

WhatWeb report for [1m[34mhttp://192.168.56.102[0m

Status : 200 OK

Title : [1m[33mMetasploitable2 - Linux[0m

IP : 192.168.56.102

Country : [1m[31mRESERVED, ZZ[0m

Summary : [1mApache[0m[[1m[32m2.2.8[0m], [1mHTTPServer[0m[[1m[31mUbuntu Linux[0m][[1m[36mApache/2.2.8 (Ubuntu) DAV/2[0m], [1mPHP[0m[[1m[32m5.2.4-2ubuntu5.10[0m], [1mWebDAV[0m[[1m[32m2[0m], [1mX-Powered-By[0m[[0m[22mPHP/5.2.4-2ubuntu5.10[0m]

Detected Plugins:

[ [1mApache[0m ]

The Apache HTTP Server Project is an effort to develop and

maintain an open-source HTTP server for modern operating

systems including UNIX and Windows NT. The goal of this

project is to provide a secure, efficient and extensible

server that provides HTTP services in sync with the current

HTTP standards.

Version : [1m[32m2.2.8[0m (from HTTP Server Header)

Google Dorks: (3)

Website : http://httpd.apache.org/

[ [1mHTTPServer[0m ]

HTTP server header string. This plugin also attempts to

identify the operating system from the server header.

OS : [1m[31mUbuntu Linux[0m

String : [1m[36mApache/2.2.8 (Ubuntu) DAV/2[0m (from server string)

[ [1mPHP[0m ]

PHP is a widely-used general-purpose scripting language

that is especially suited for Web development and can be

embedded into HTML. This plugin identifies PHP errors,

modules and versions and extracts the local file path and

username if present.

Version : [1m[32m5.2.4-2ubuntu5.10[0m

Google Dorks: (2)

Website : http://www.php.net/

[ [1mWebDAV[0m ]

Web-based Distributed Authoring and Versioning (WebDAV) is

a set of methods based on the Hypertext Transfer Protocol

(HTTP) that facilitates collaboration between users in

editing and managing documents and files stored on World

Wide Web servers. - More Info:

http://en.wikipedia.org/wiki/WebDAV

Version : [1m[32m2[0m

[ [1mX-Powered-By[0m ]

X-Powered-By HTTP header

String : [1m[36mPHP/5.2.4-2ubuntu5.10[0m (from x-powered-by string)

HTTP Headers:

HTTP/1.1 200 OK

Date: Mon, 25 Nov 2024 17:49:12 GMT

Server: Apache/2.2.8 (Ubuntu) DAV/2

X-Powered-By: PHP/5.2.4-2ubuntu5.10

Content-Length: 891

Connection: close

Content-Type: text/html