Student:	Email:
Sadam Hashi	smhashi@asu.edu

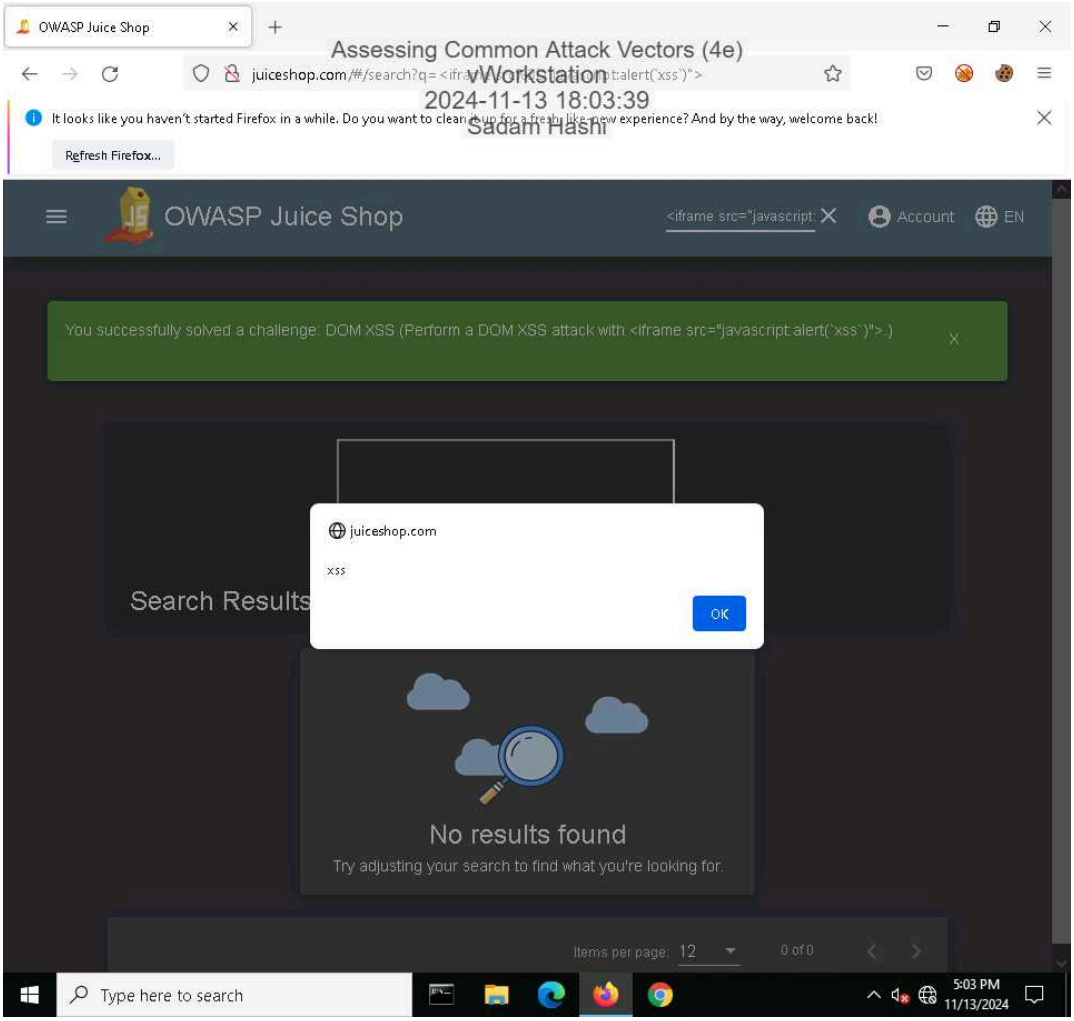
Time on Task:	Progress:
14 hours, 16 minutes	100%

Report Generated: Thursday, November 14, 2024 at 10:13 PM

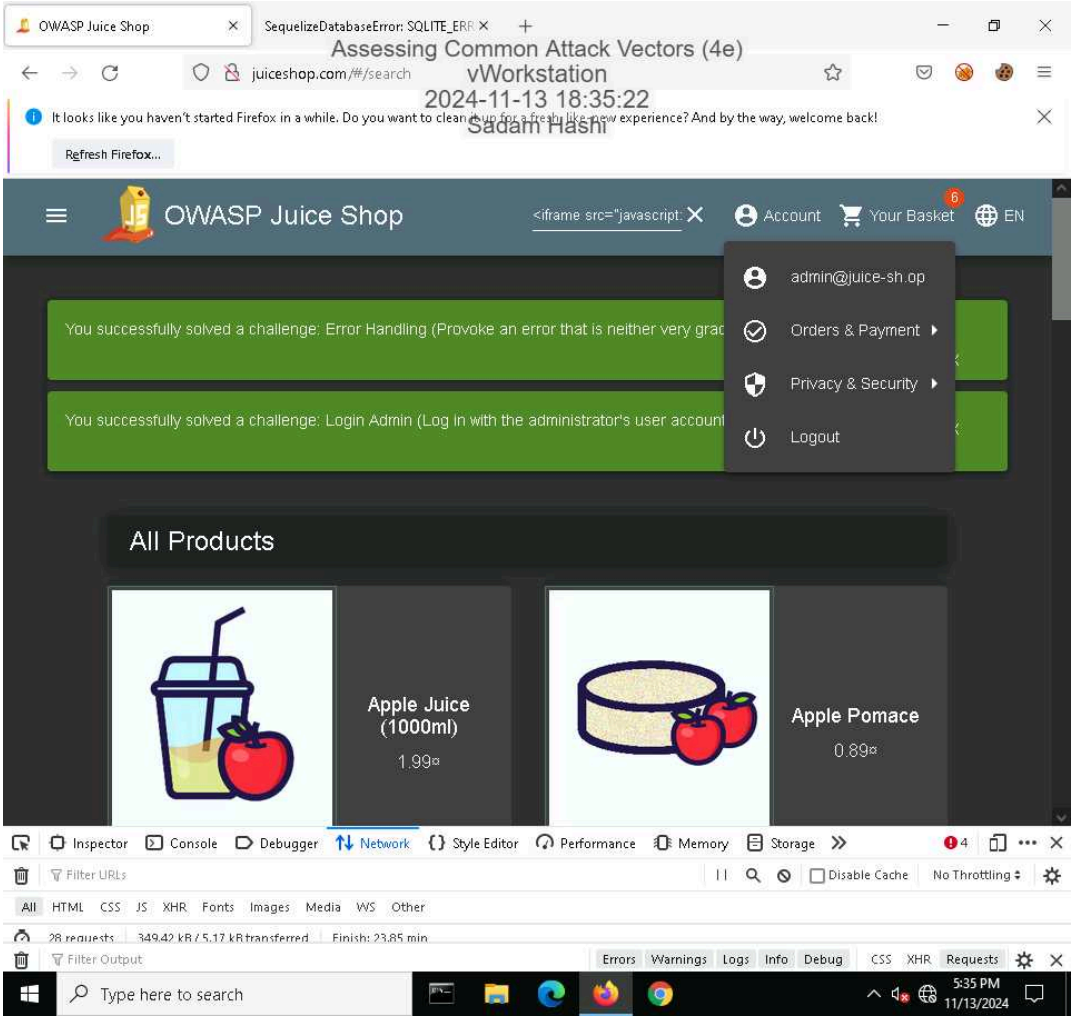
Section 1: Hands-On Demonstration

Part 1: Perform an Injection Attack

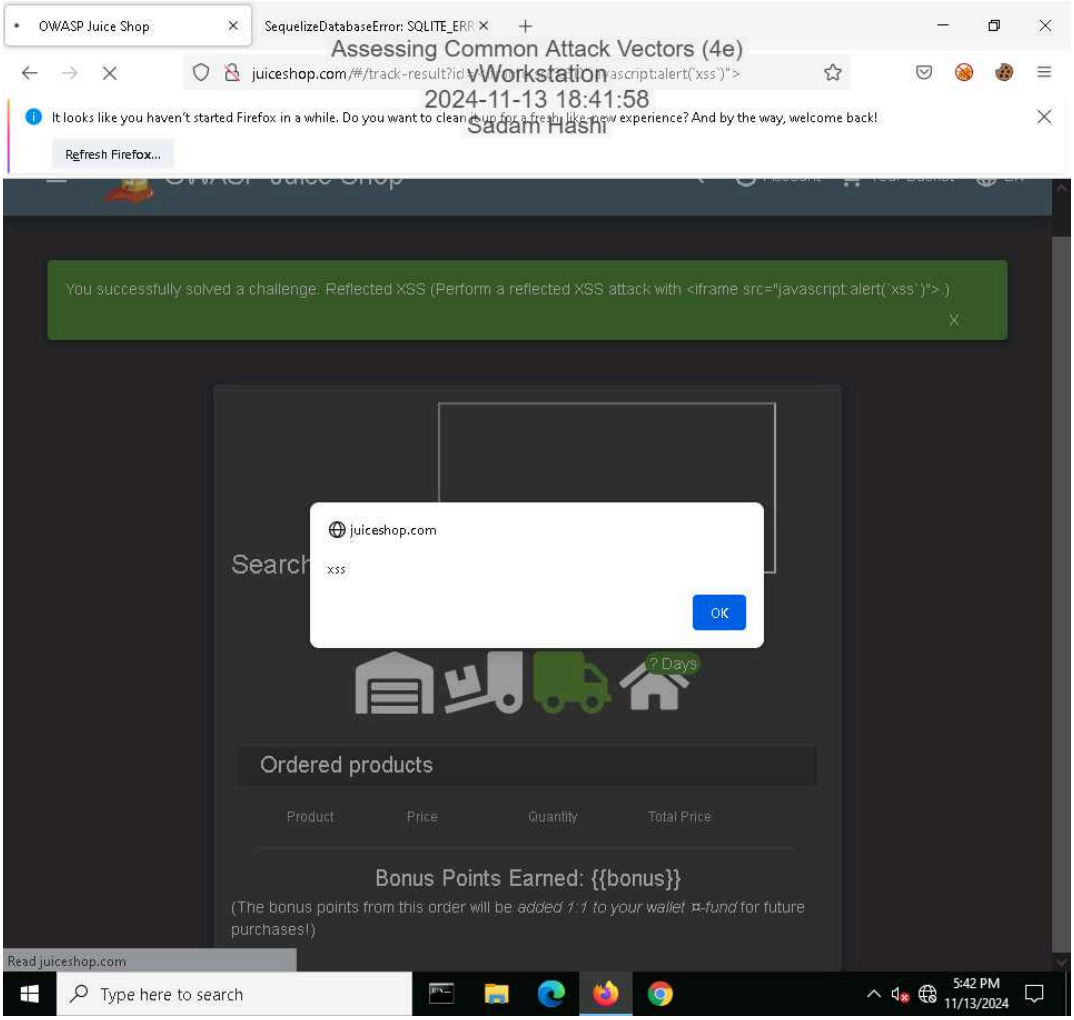
11. **Make a screen capture** showing the **DOM XSS dialog box**.



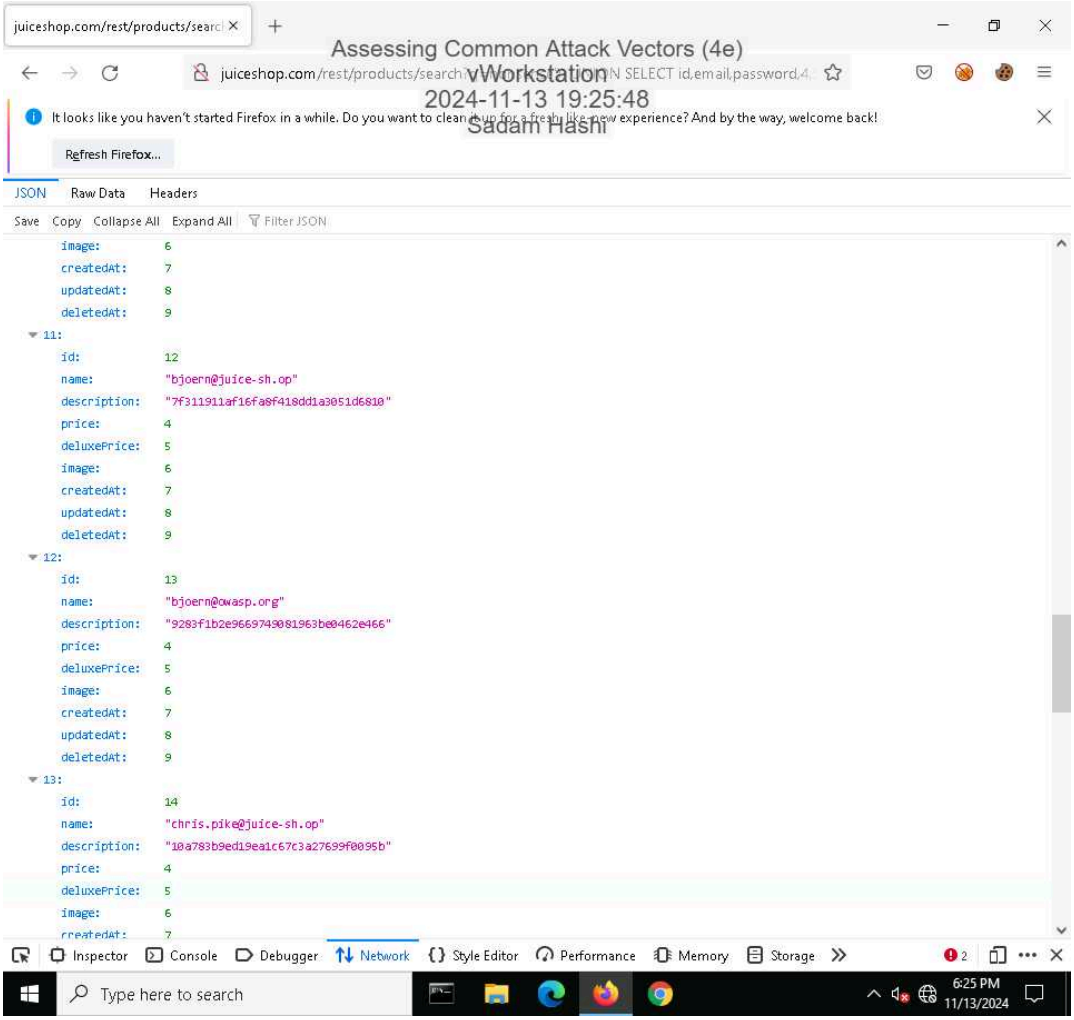
21. **Make a screen capture** showing the **successful admin login**.



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

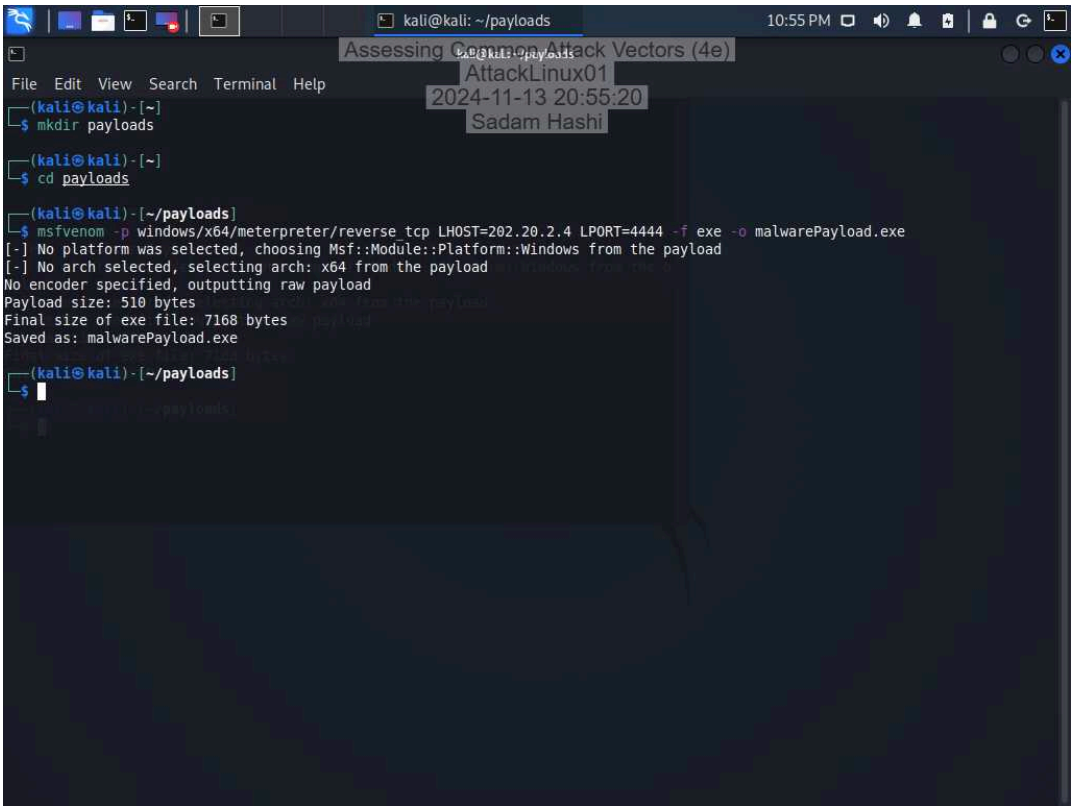


42. **Make a screen capture** showing the **user with the @owasp.org email**.

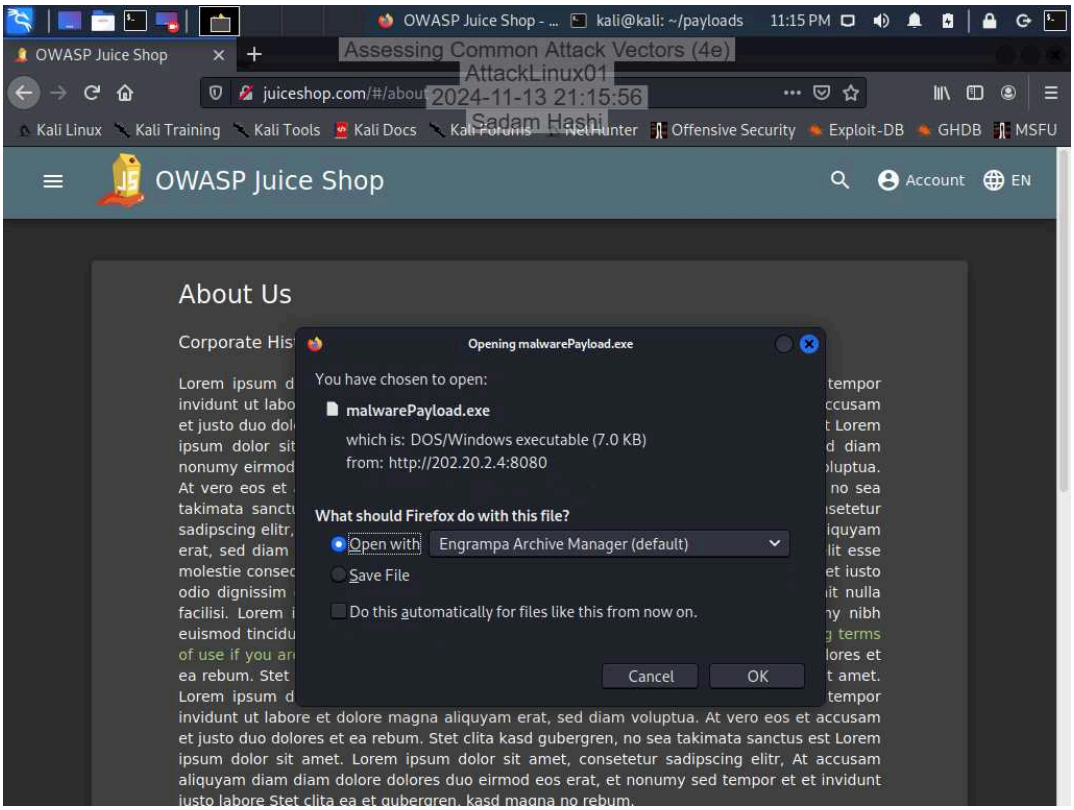


Part 2: Perform a Malware Attack

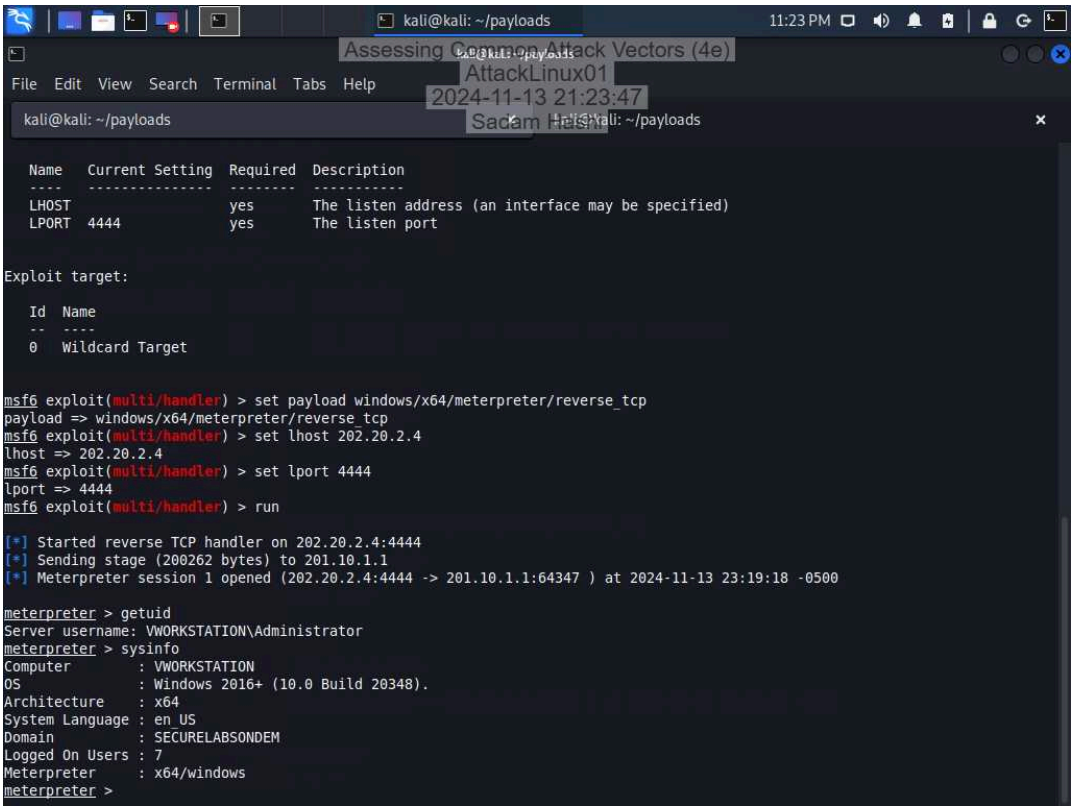
6. **Make a screen capture** showing the **msfvenom output**.



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



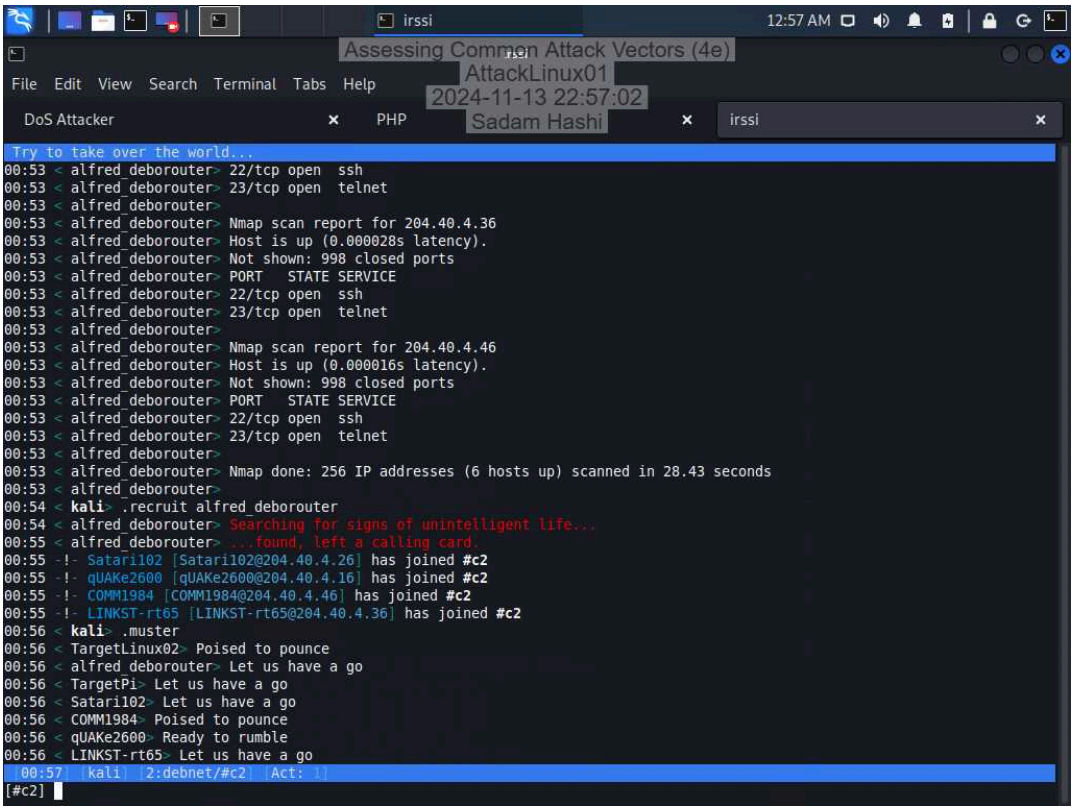
36. **Make a screen capture** showing the **output of the sysinfo command**.



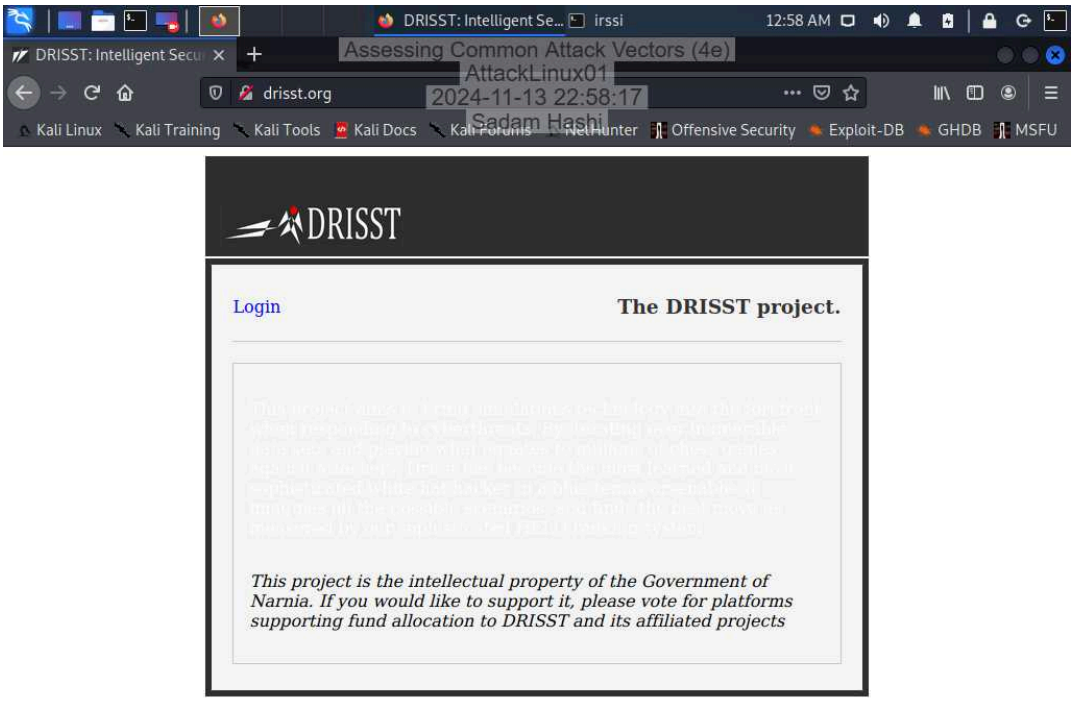
Section 2: Applied Learning

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

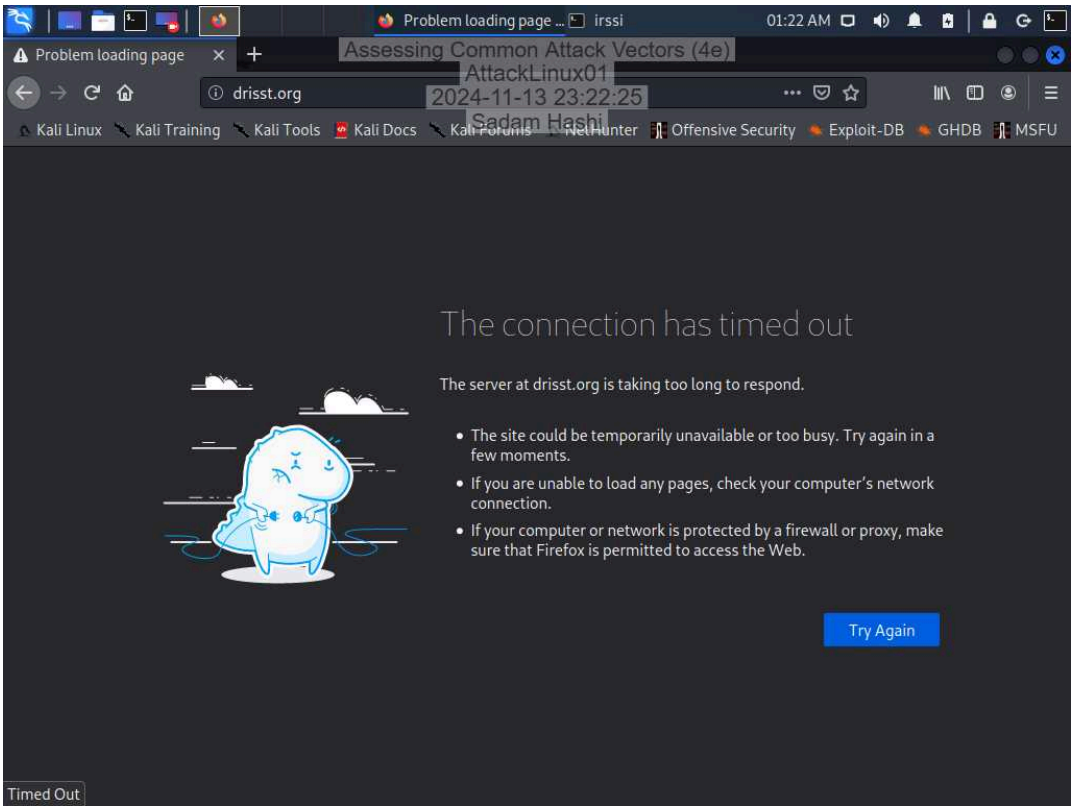
25. **Make a screen capture** showing the **newly recruited hosts**.



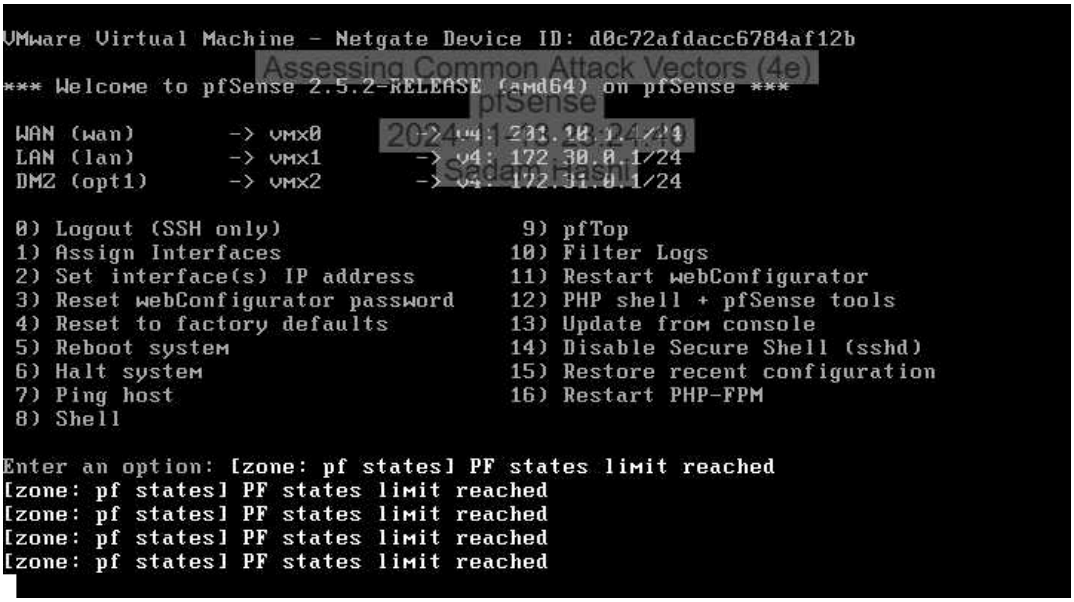
28. **Make a screen capture** showing the **drisst.org webpage**.



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

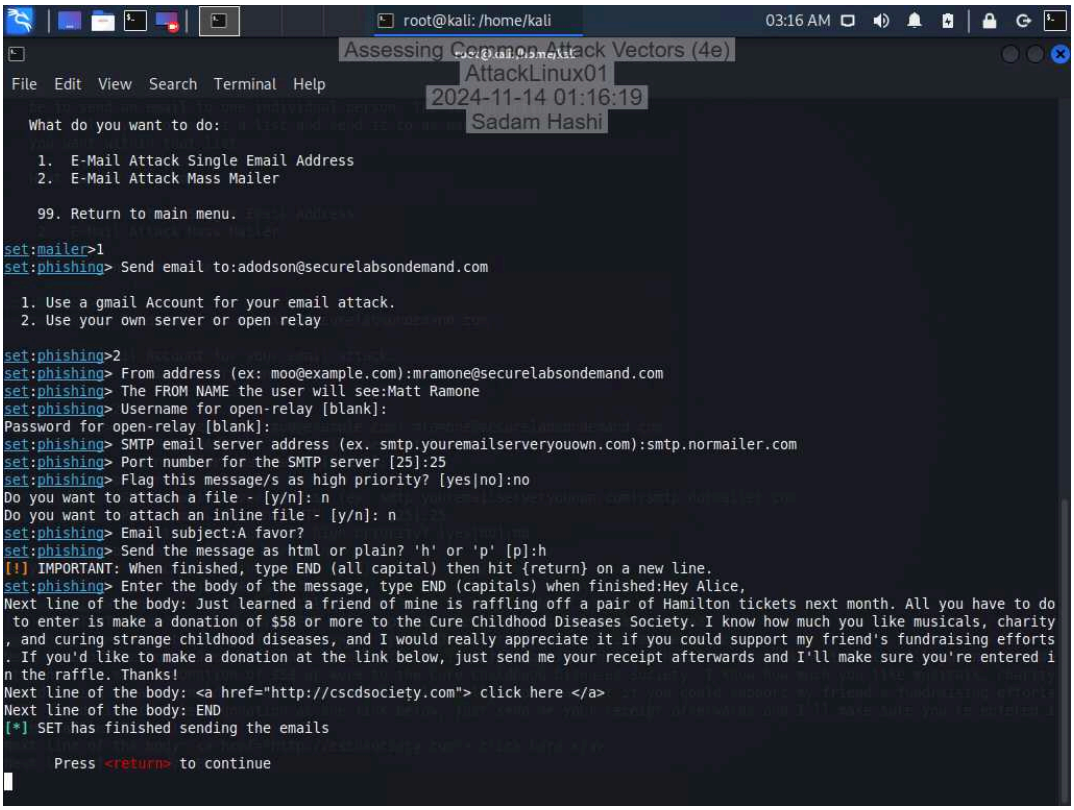


35. **Make a screen capture** showing the **"PF states limit reached" error message**.

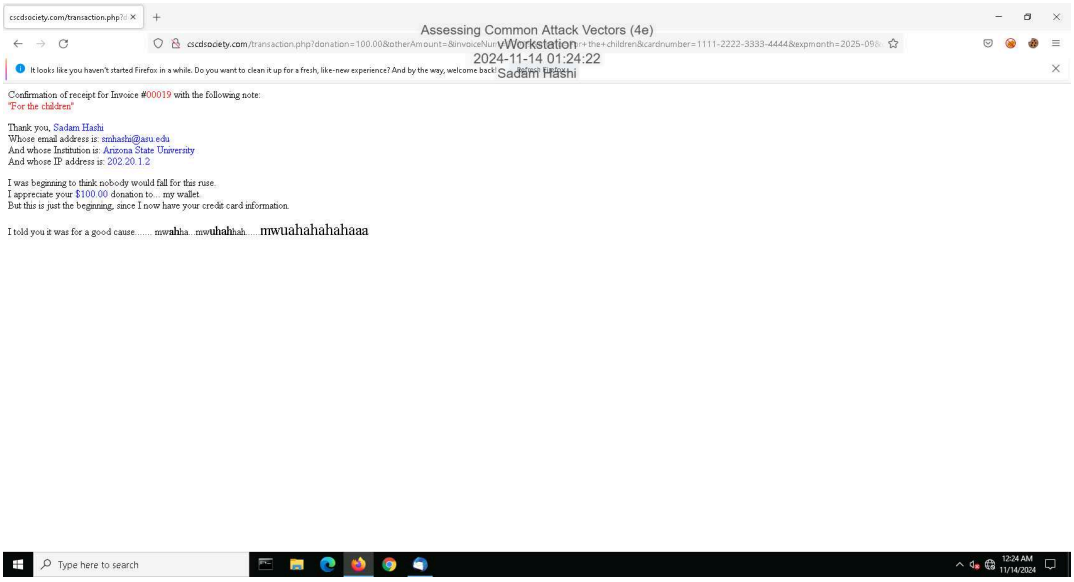


Part 2: Perform a Social Engineering Attack

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.

1. **Parametrized Queries** - One way to defend against injection attacks(sql injection), is to utilize an effective coding practice. In order to mitigate the risk of injection attacks, making sure to separate user inputs from the database(sql) query is key. Parameterization basically makes sure that the user input is treated as data and not executable code, which prevents it from modifying the database query.
2. **Web Application Firewall (WAF)** - WAF is another defensive measure against injection attacks. WAF filters and monitors HTTP requests to block any malicious inputs it encounters. WAF protects the malicious commands to fall to reach the server its tasked to protect.
Source:
Sundar, Venkatesh. “How to Prevent SQL Injection Attacks? | Indusface Blog.” Indusface, 28 Nov. 2016, www.indusface.com/blog/how-to-stop-sql-injection/.

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

1. **Maintaining Regular Software Updates** - An organization must update to the new released versions of whichever software or systems they are operating on. Regular updates can become a defensive measure by patching any vulnerabilities that can be exploited.
2. **Robust Anti-malware Software** - All the systems of an organization must have an up-to-date anti-malware software. These software need to be regularly updated and configured for regular scans in specific files important to the organization.
Source:
“10 Strategies to Protect against Malware Attacks.” Www.drivelock.com, 11 Sept. 2023, www.drivelock.com/en/blog/malware-attacks.

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

1. **Rate Limiting** - An organization can implement rate limits on server requests so the server is not overwhelmed if a DoS attack was to incite. Rate Limiting is a first line defense measure organization use.
2. **Load Balancing** - By distributing traffic to multiple servers, a DoS attack can prevented again by overwhelming one server. This defensive measure is versatile and can be implemented in software or hardware as a solution for DoS attacks.
Source:
Byos. “Denial-of-Service (DoS) Attack Prevention: The Definitive Guide.” Www.byos.io, 2023, 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.

1. **User Awareness & Education** - Users or an organization's employees play vital role in protecting an organization any cyber attacks. Training employees to recognize any suspicious activity is important. Users must learn to identify phishing spams, pretexting, baiting, etc. The employees themselves can become an organization's weakest link, but with proper training and education, the employees/users can become a defensive measure against social engineering attacks.
2. **Multi-Factor Authentication** - An organization can implement multiple forms of verification to verify users of the system. This means an attacker who social engineered a victim will still need more then a password and username to access sensitive data (i.e. sending a code to the phone number for verification). This can also be used as a defensive measure against social engineering.
source:
Kaspersky. “Ways to Avoid Social Engineering Attacks.” Www.kaspersky.com, 10 Sept. 2020, www.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.

Misconfiguration attacks - A misconfiguration attacks occur when a system is poorly configured in terms of hardware or software. The system faces threats and attackers can gain access or cause damage.
1. **Implementing Strong Access Points** - Following the principles of least privilege in order to limit a user the minimum resources needed to a perform a task. This can be used a defensive measure from an attacker using a comprised account to cause damage and prevent lateral movement attack.
2. **Regular Audits** - Conducting regular audits can help prevent misconfiguration attacks taking place. Doing a security assessment to locate vulnerabilities by penetration testing can also be used as a defensive measure.
Source:
Balbix. “Security Misconfiguration.” Balbix, 18 Nov. 2022, www.balbix.com/insights/security-misconfiguration-impact-examples-and-prevention/.