Performing Social Engineering Attacks (4e)

Ethical Hacking, Fourth Edition - Lab 08

Student: Brayden Mitchell
Email: brayden.m.mitchell@gmail.com
Time on Task: 0 hours, 55 minutes
Progress: 100%
Report Generated: Tuesday, October 20, 2026 at 3:19 PM

Hands-On Demonstration

Part 1: Perform Reconnaissance

5. **Document** the **names** and **email addresses** of the people on the About Us page.

Kristen Ibarra kibarra@drisst.org
Kiran Radcliffe kradcliffe@drisst.org
Matt Ramone mattr@drisst.org
Kane Szekeres kszekeres@drisst.org

14. **Make a screen capture** showing the captured test credentials in the log.

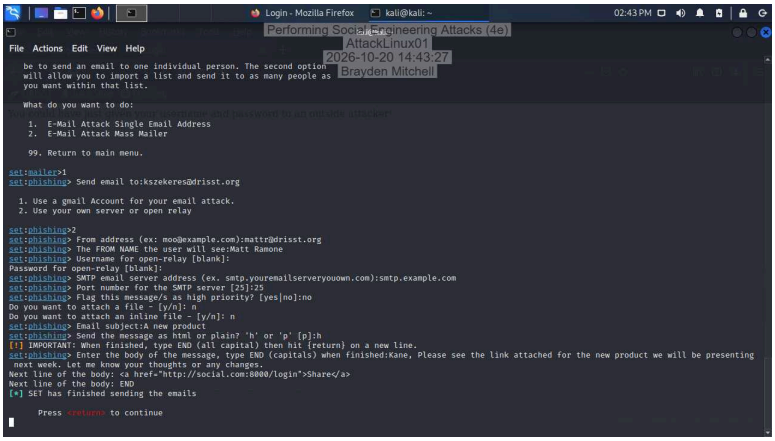


Part 2: Send a phishing email

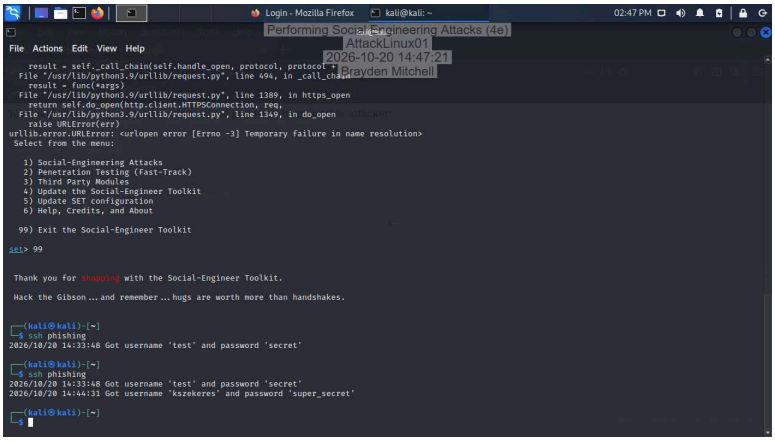
19. **Document** the message you created for the spear phishing email.

Kane, Please see the link attached for the new product we will be presenting next week. Let me know your thoughts or any changes.

24. **Make a screen capture** showing the message was sent.



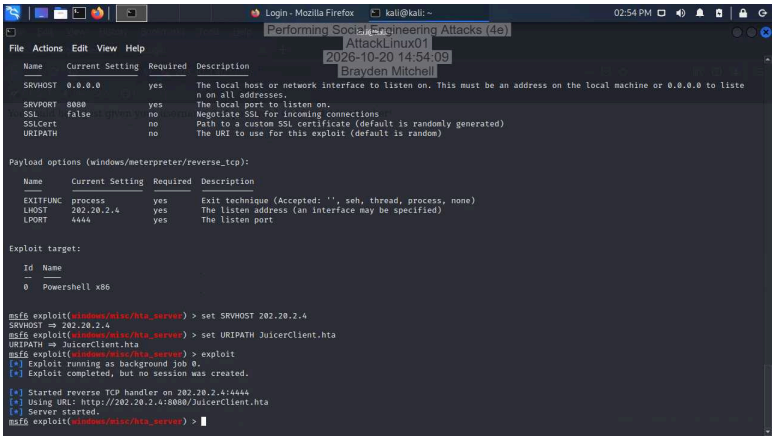
28. **Make a screen capture** showing the username and password collected from Kane.



Applied Learning

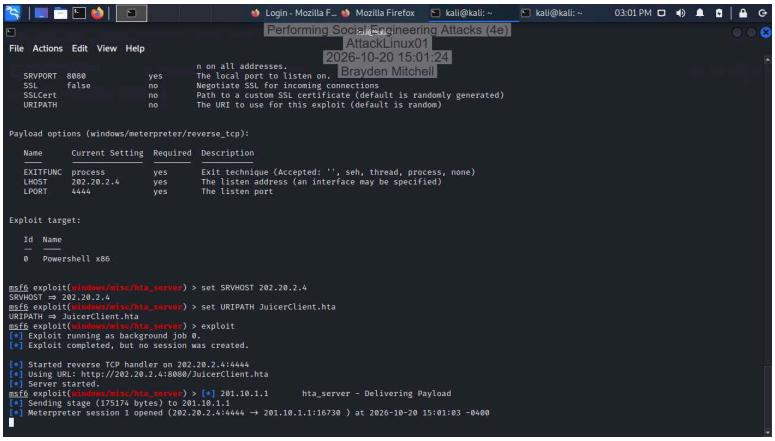
Part 1: Prepare the payload

9. **Make a screen capture** showing that the exploit is running.



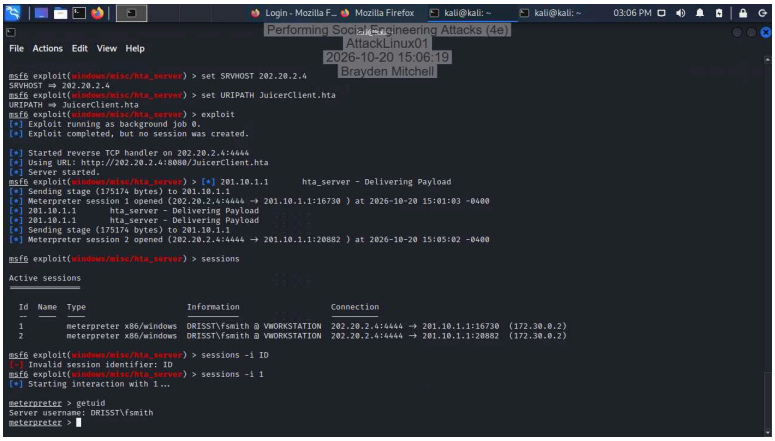
Part 2: Perform an XSS attack on the Juice Shop

11. **Make a screen capture** showing the valid Meterpreter session.

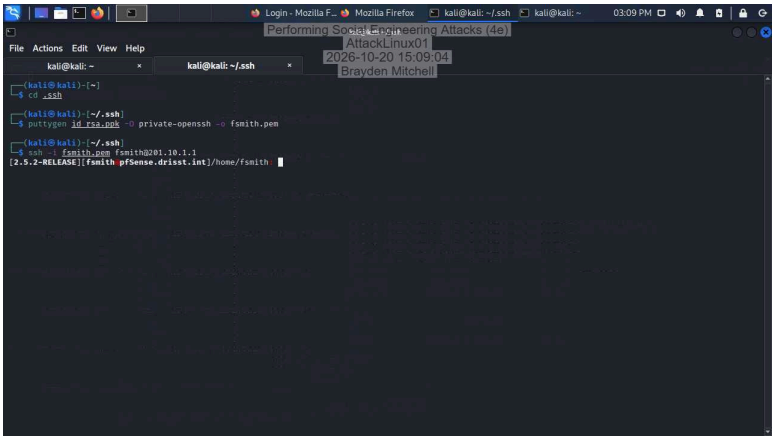


Part 3: Demonstrate Exploits

4. **Make a screen capture** showing the user id.



14. **Make a screen capture** showing the successful login.



Challenge and Analysis

Part 1: Recommend email server change

1. **Document** what SPF, DKIM, and DMARC stand for and the benefits of implementing each to drisst.org's mail system to counteract spoofed emails.

SPF: A DNS TXT record listing which servers are allowed to send mail for drisst.org (e.g., v=spf1 mx ip4:203.0.113.25 -all), so receivers can reject mail from any unlisted server. It only checks the envelope sender

and breaks on forwarding, so it isn’t enough alone.
DKIM: The sending server signs each message with a private key, and receivers verify it using a public key published in DNS (use 2048-bit RSA). A spoofer without the private key can’t forge a valid signature, and the signature also proves the message wasn’t altered.
DMARC: A DNS record at _dmarc.drisst.org that requires SPF or DKIM to pass and align with the visible From domain, and tells receivers to reject failures (p=reject). It also sends reports (rua) so you can see who is sending as your domain.
Recommended settings: Publish SPF with -all, sign mail with DKIM, and set DMARC to p=reject; sp=reject with rua reporting. Also enable SPF, DKIM, and DMARC checking on the receiving mail server, since the lab server accepted the forged mail.

Part 2: Recommend browser settings changes

1. **Provide** clear and comprehensive instructions detailing the necessary changes to be made in Firefox to ensure the consistent display of PUNY code in the address bar.

The setting is a preference in Firefox’s advanced configuration page, network.IDN_show_punycode.
1. Open a new tab and type about:config in the address bar, then press Enter.2. Click through the warning that appears (Accept the Risk and Continue).3. In the search box, type punycode to find the parameter network.IDN_show_punycode. winaero4. Set it to true by double-clicking it, or by clicking the toggle button.5. Reload the phishing link. The address bar should now show the raw xn-- form of the domain instead of the Unicode characters.