Student:	Email:
Truc Huynh	huyntl02@pfw.edu

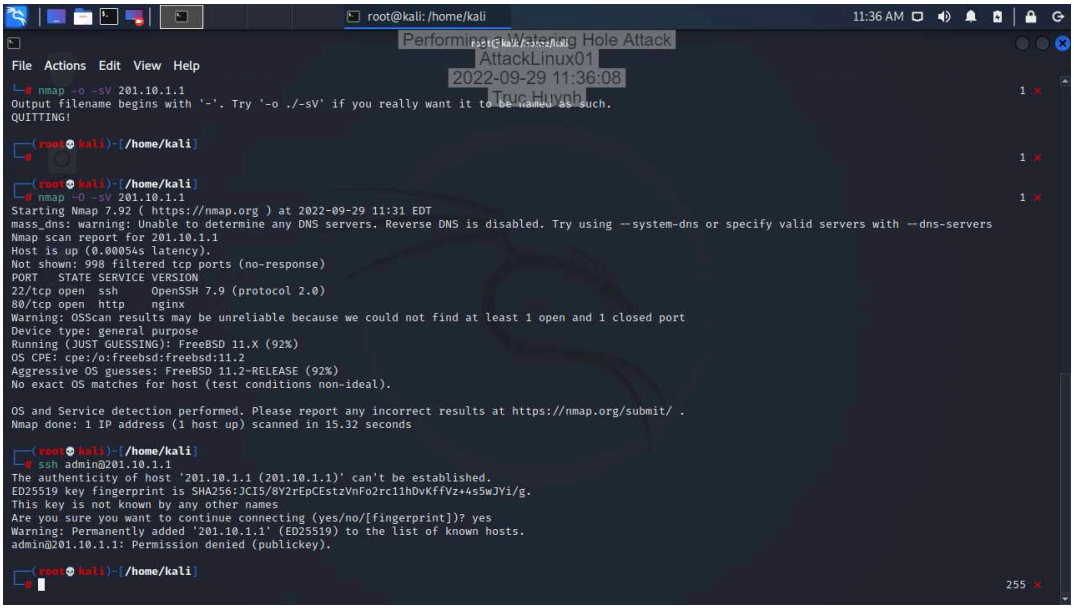
Time on Task:	Progress:
2 hours, 31 minutes	100%

Report Generated: Thursday, September 29, 2022 at 12:32 PM

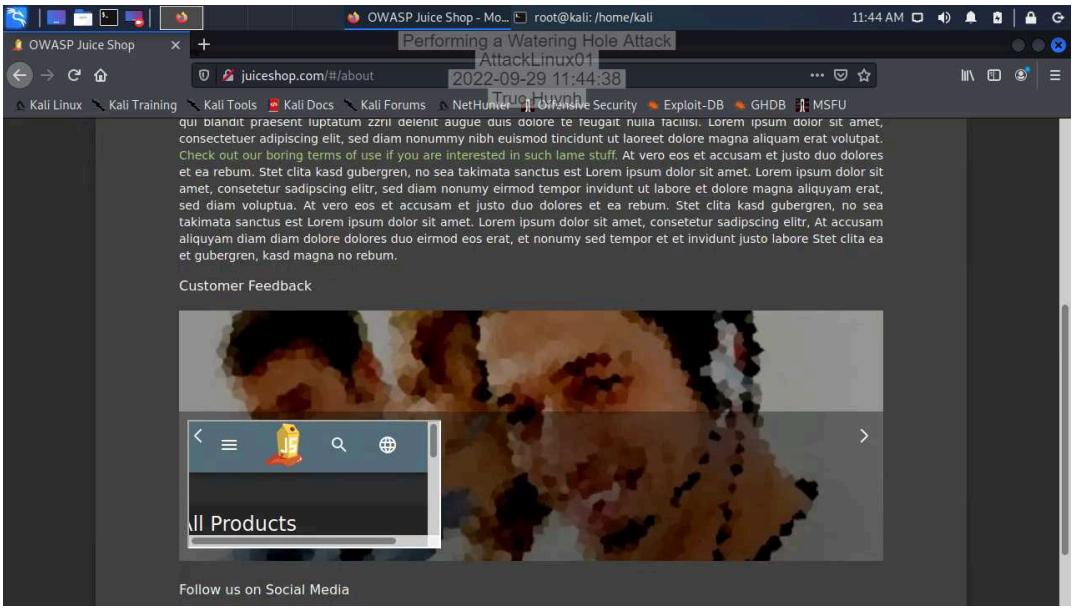
Hands-On Demonstration

Part 1: Perform Reconnaissance on the Target

8. **Make a screen capture** showing the **server's rejection of the SSH login**.

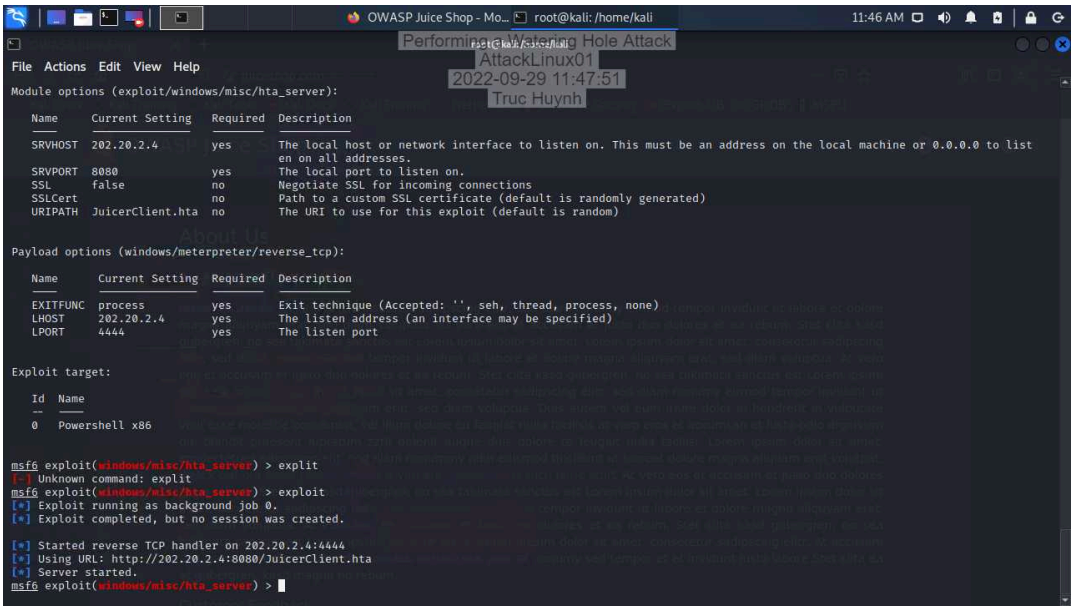


18. **Make a screen capture** showing the **XSS proof-of-concept on the watering hole**.

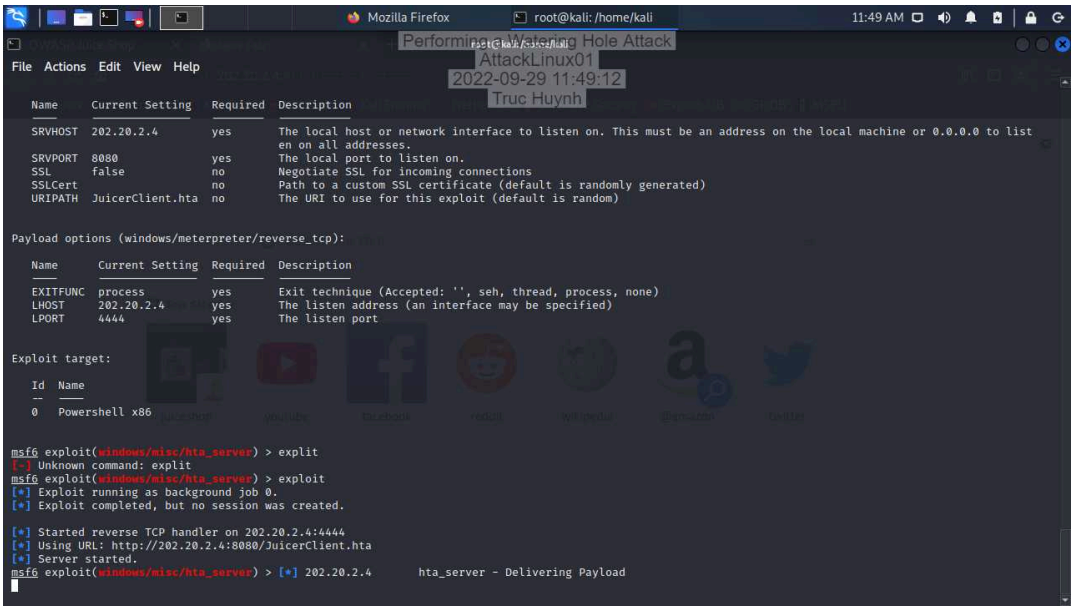


Part 2: Perform a Watering Hole Attack

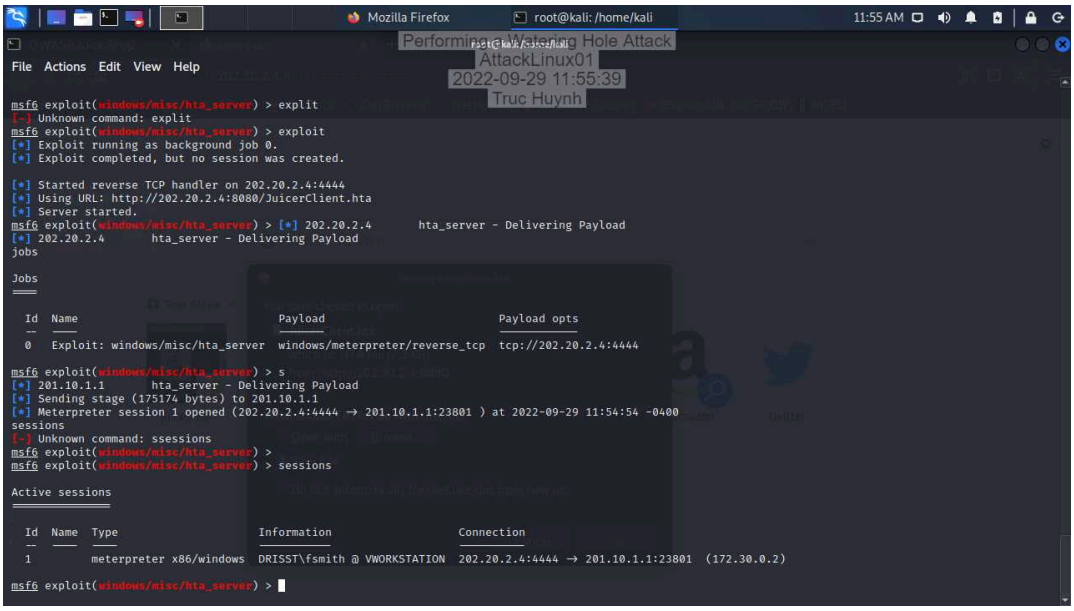
10. **Make a screen capture** showing the **successful server start-up in Metasploit**.



15. **Make a screen capture** showing the **delivering payload message**.

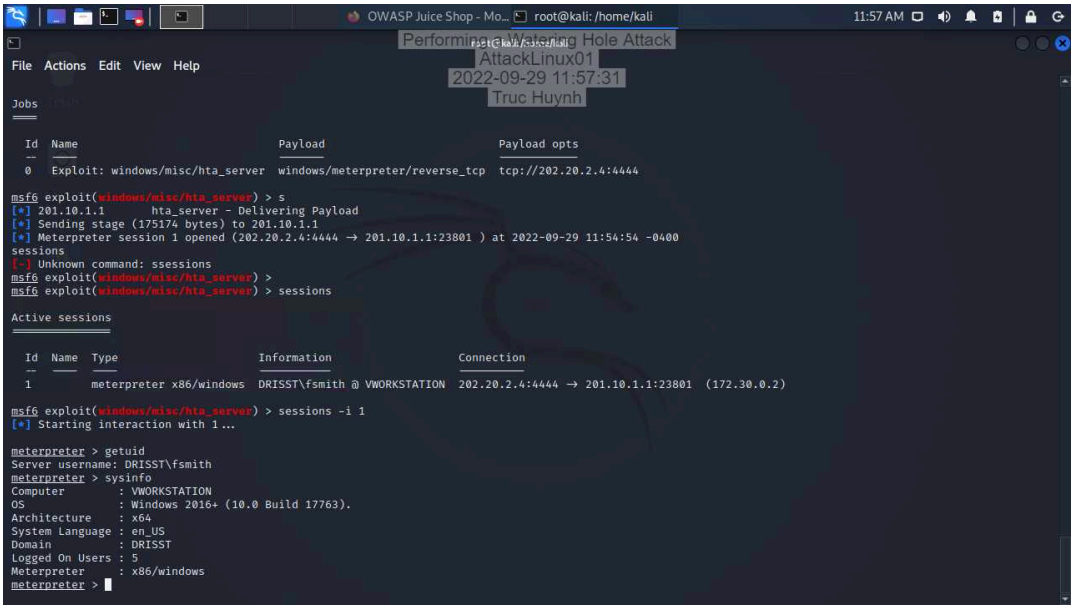


23. **Make a screen capture** showing the **session from the remote victim**.

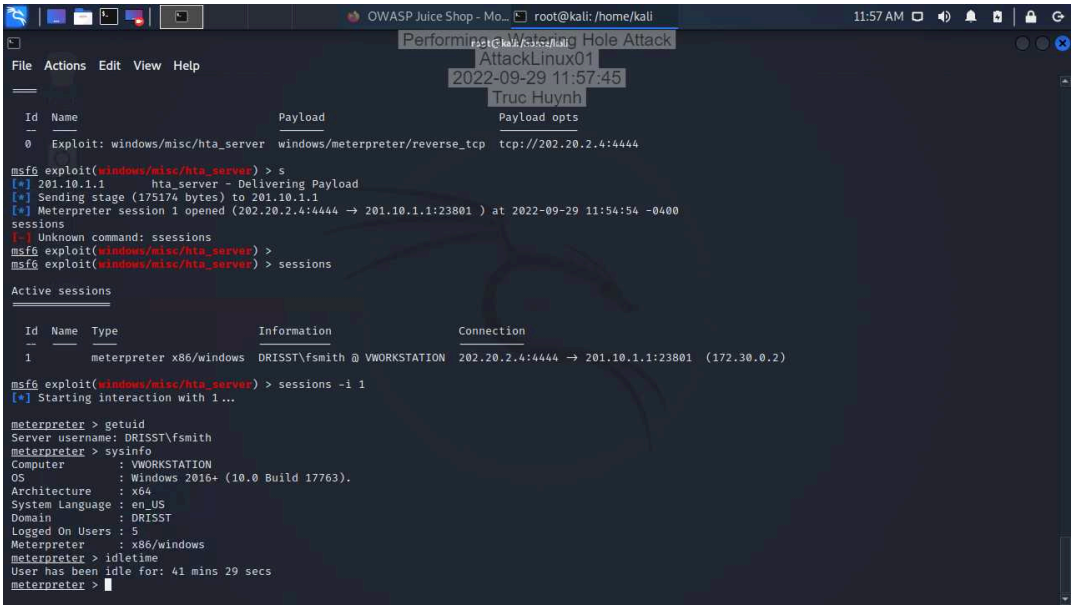


Part 3: Perform Post-Exploitation Maneuvers

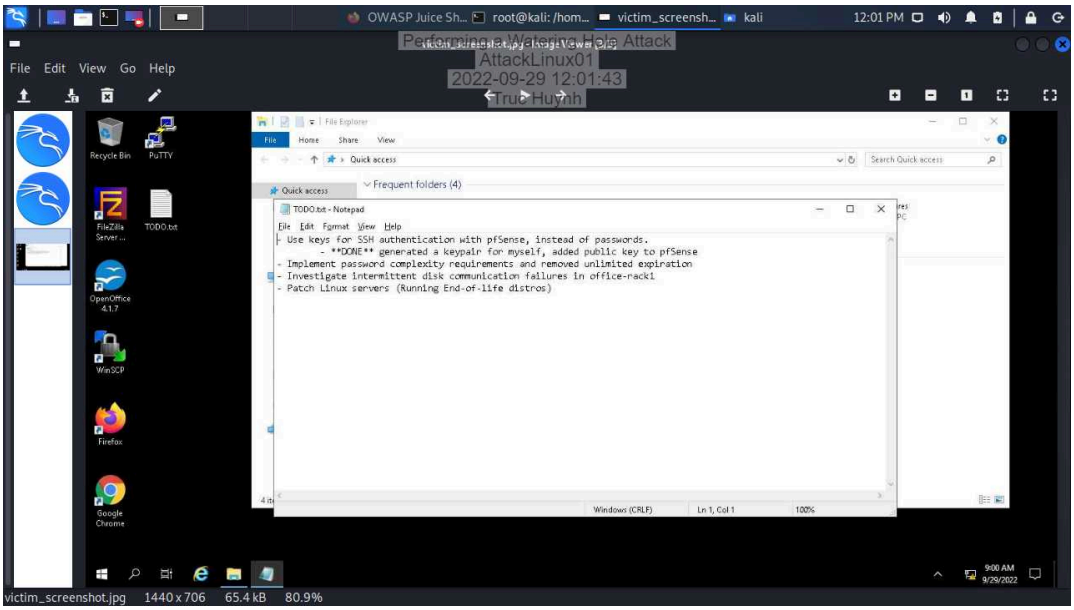
4. **Make a screen capture** showing the **operating system, workstation name, and domain name**.



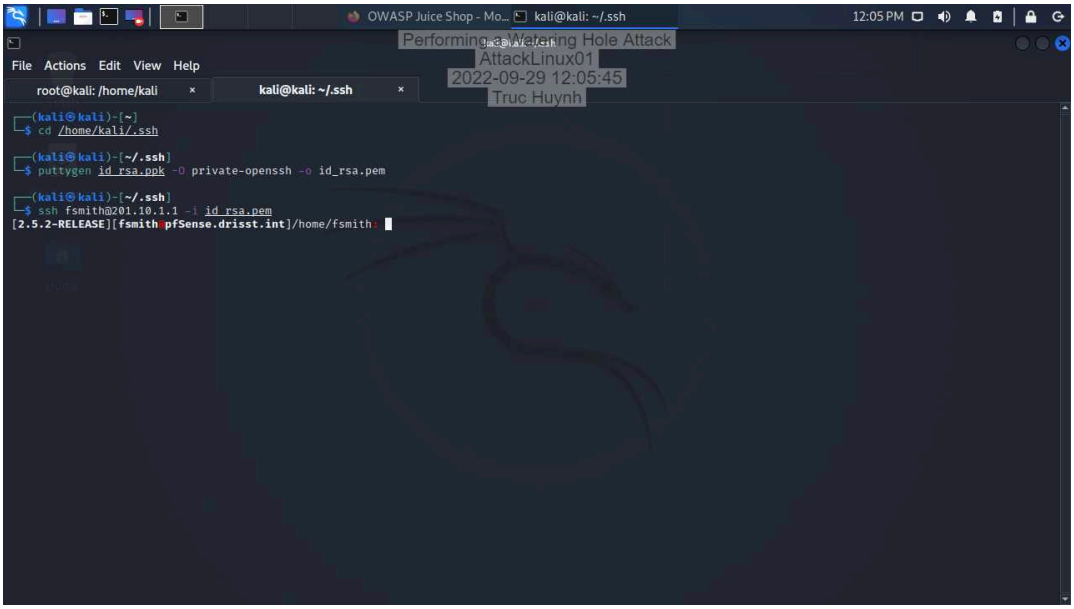
6. **Make a screen capture** showing the **system, user, and idletime information in your output**.



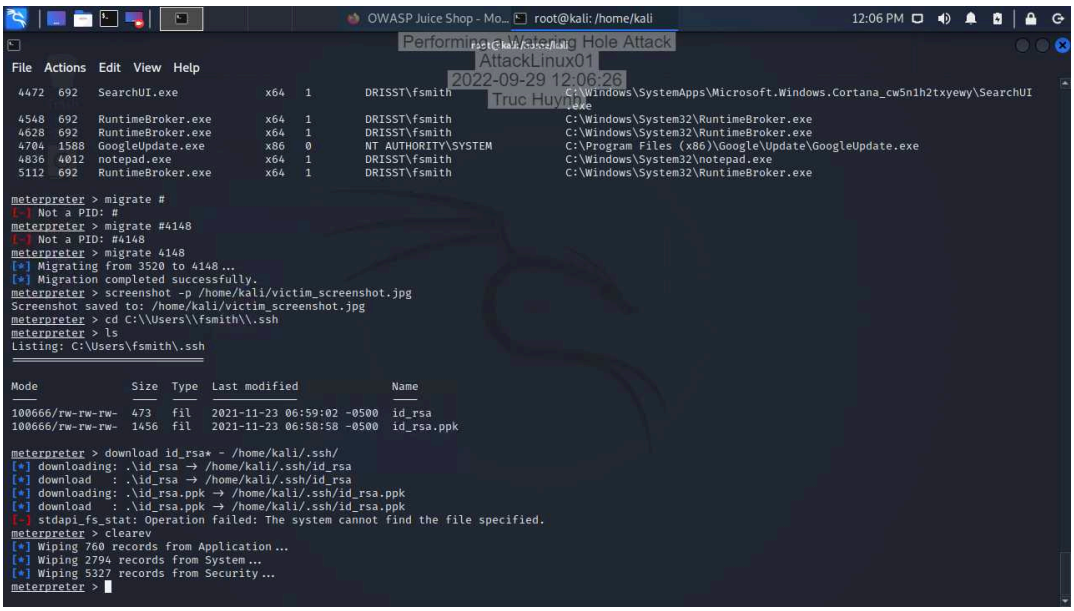
12. **Make a screen capture** showing the **screenshot of the user's desktop and TODO.txt file**.



23. **Make a screen capture** showing the **successful connection to pfSense firewall with user fsmith**.



27. **Make a screen capture** showing the **Application, System, and Security logs were successfully wiped from remote victim fsmith's workstation**.



Challenge and Analysis

Part 1: Research Watering Hole Attacks

Research a real-world watering hole attack. Who conducted it? Who/what was the target? What was used as the watering hole? What were the attack vectors? How long did the attack go unnoticed?

NotPetya attack on Ukran Who conducted it: Believed Russia (state actor) Who/what was the target: Ukraine (most hit), Europe, US What was used as the watering hole: government website for the Ukrainian (city of Bakhmut) was compromised and used in a watering hole attack to spread the malware via a drive-by download. What were the attack vectors: The malware erases the contents of victims' hard drives, and sabotaged thousands of PC How long did the attack go unnoticed: Estimate a month or less Reference: https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/notpetya-timeline-of-a-ransomworm/ https://threatpost.com/researchers-find-blackenergy-apt-links-in-expetr-code/126662/

Part 2: Configure an Additional XSS Payload

Make a screen capture showing the **successful alert box generation**.