Student:	Email:
Amar Korac	akorac@neiu.edu

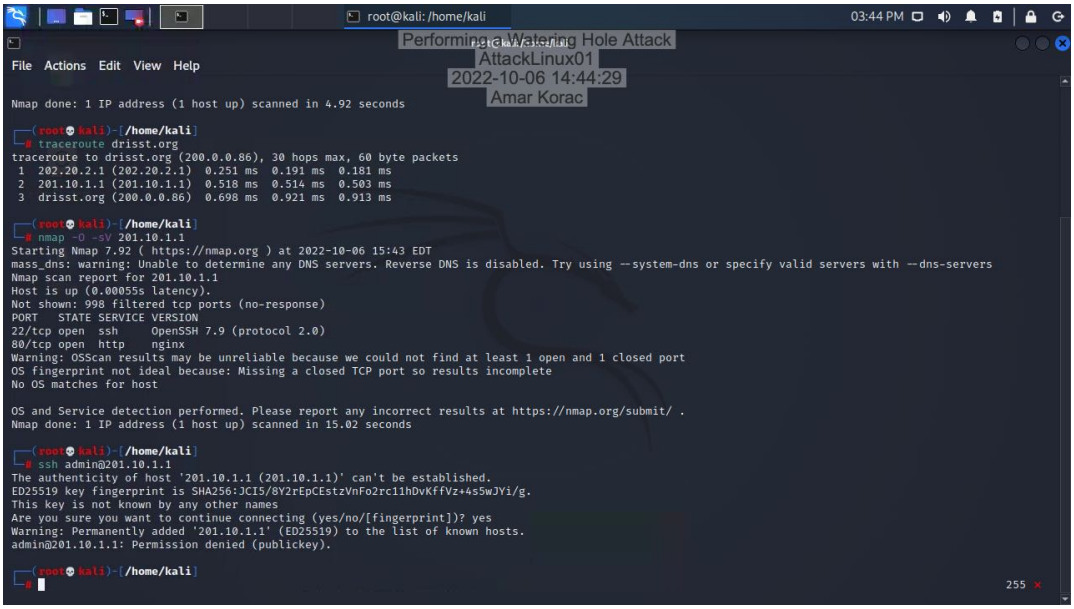
Time on Task:	Progress:
4 hours, 35 minutes	100%

Report Generated: Tuesday, October 11, 2022 at 9:28 PM

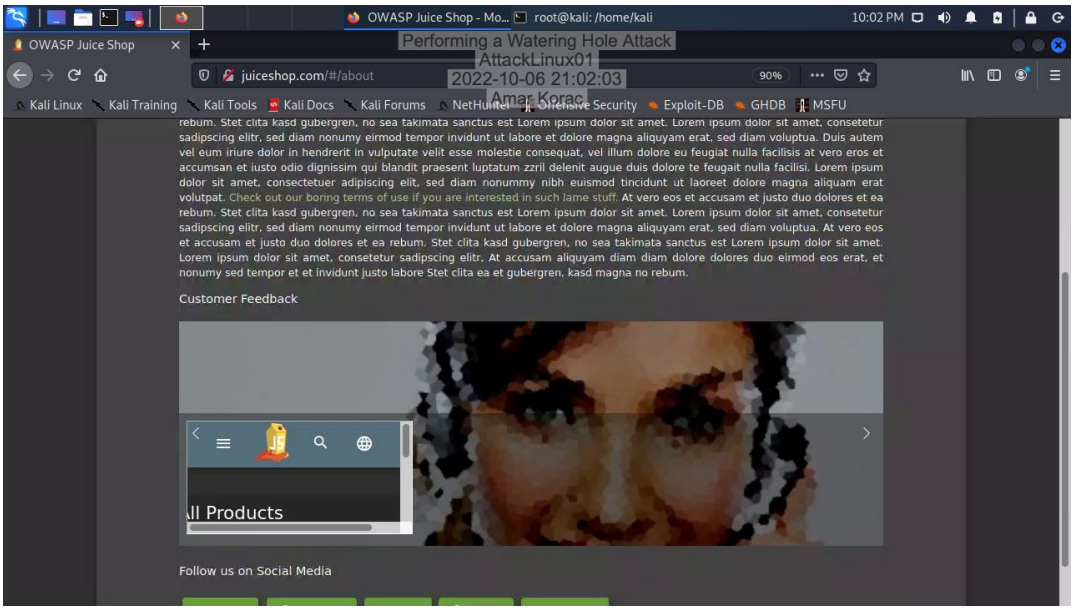
Hands-On Demonstration

Part 1: Perform Reconnaissance on the Target

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

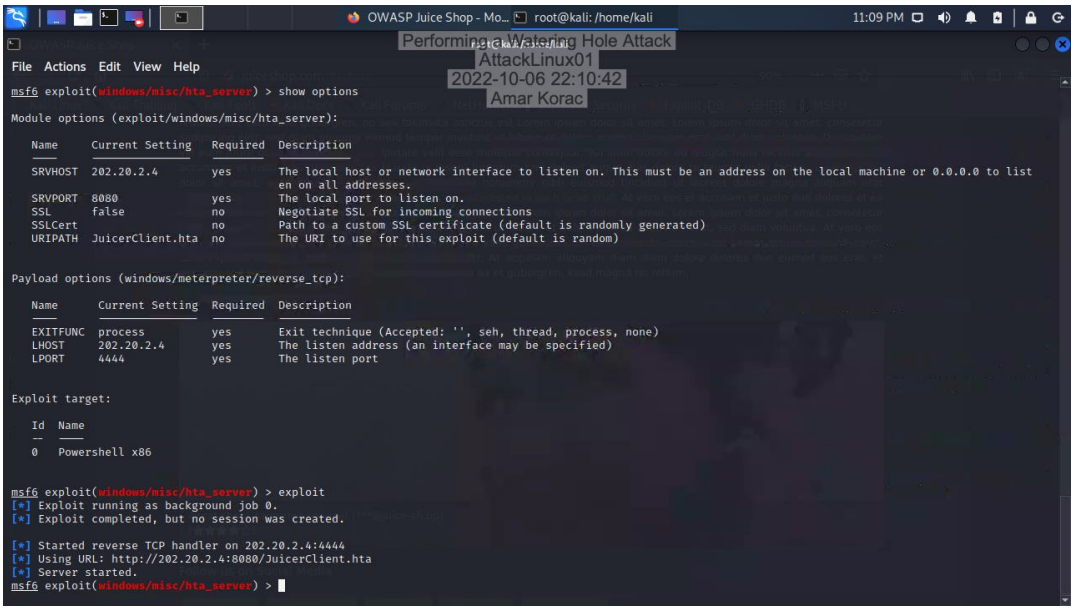


18. **Make a screen capture** showing the **XSS proof-of-concept on the watering hole**.

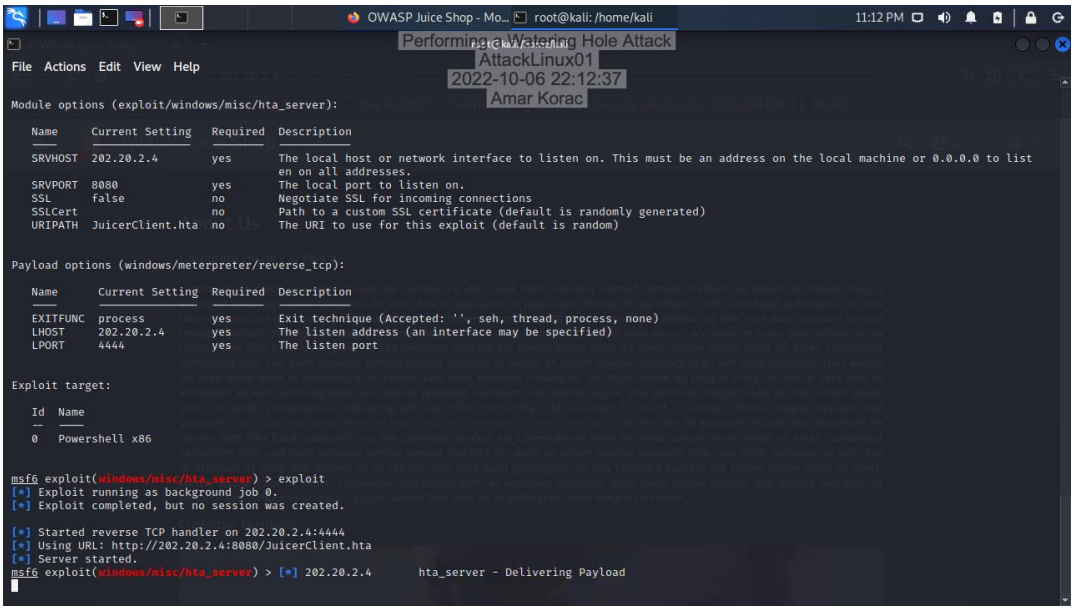


Part 2: Perform a Watering Hole Attack

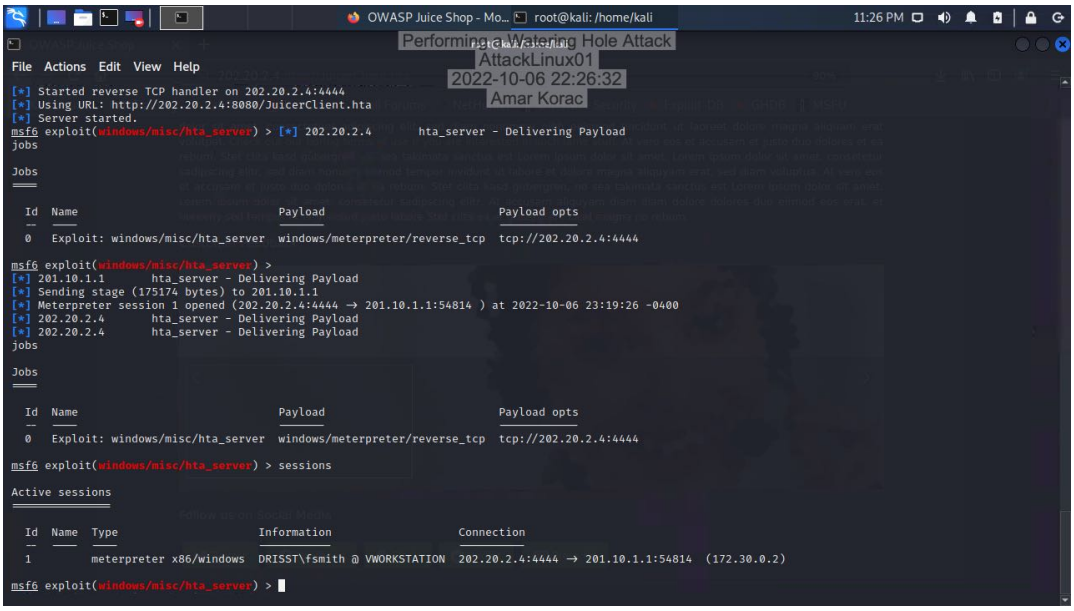
10. **Make a screen capture** showing the **successful server start-up in Metasploit**.



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

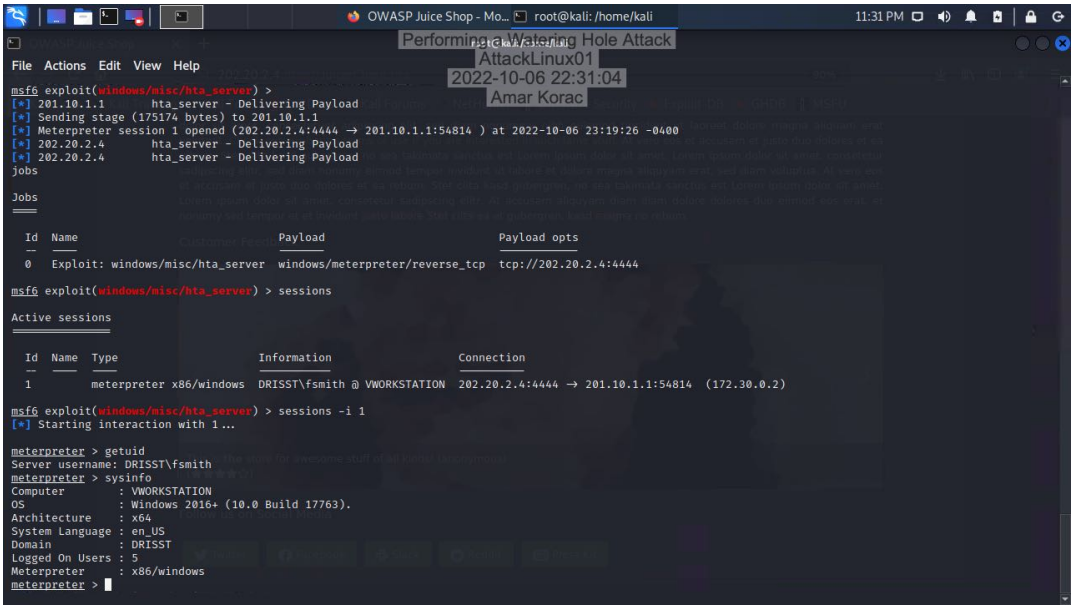


23. **Make a screen capture** showing the **session from the remote victim**.

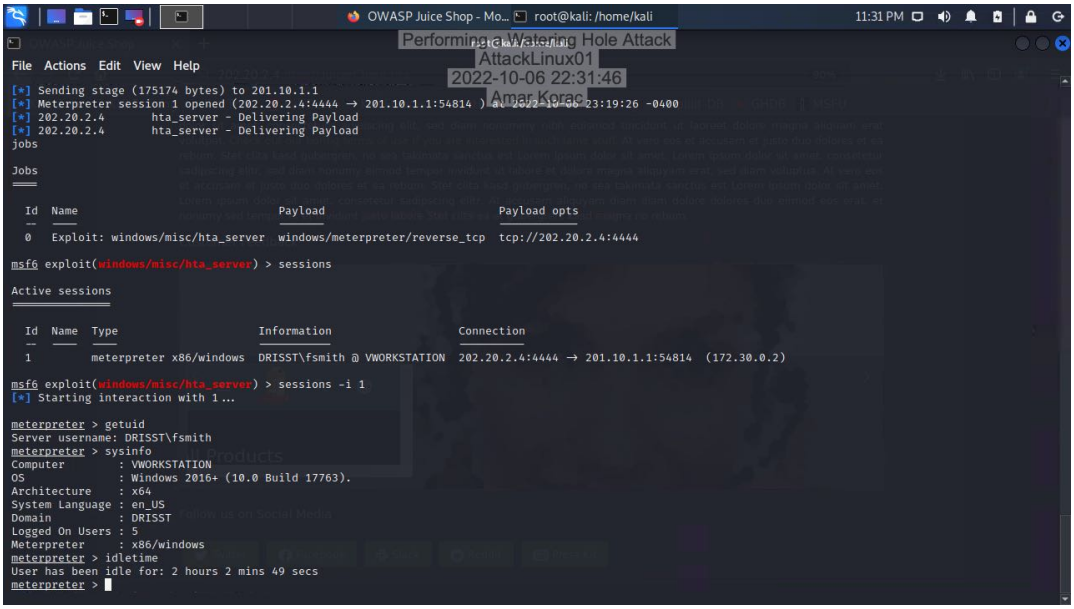


Part 3: Perform Post-Exploitation Maneuvers

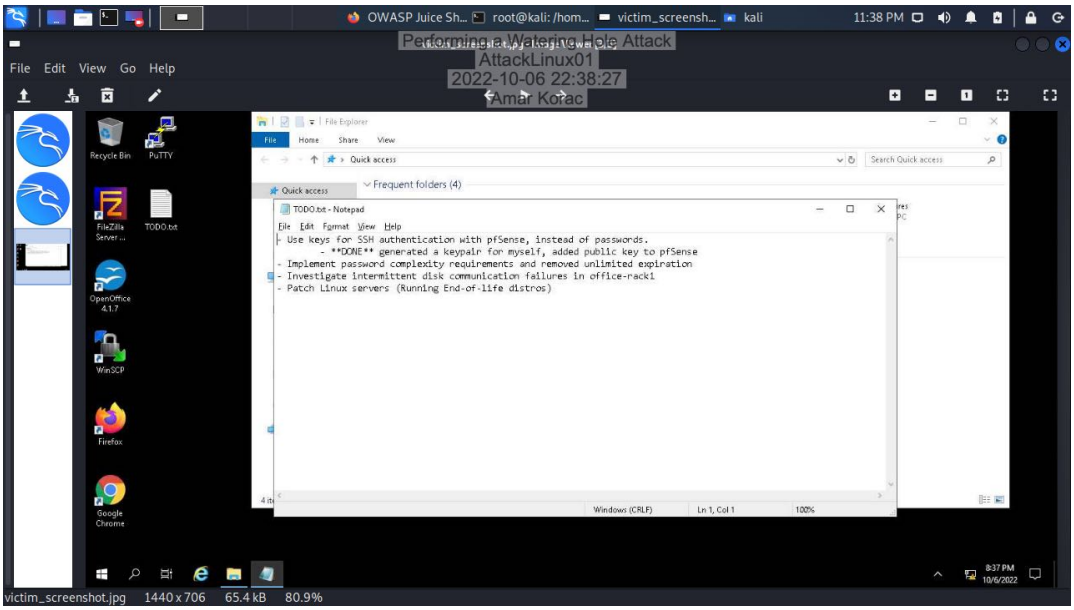
4. **Make a screen capture** showing the **operating system, workstation name, and domain name**.



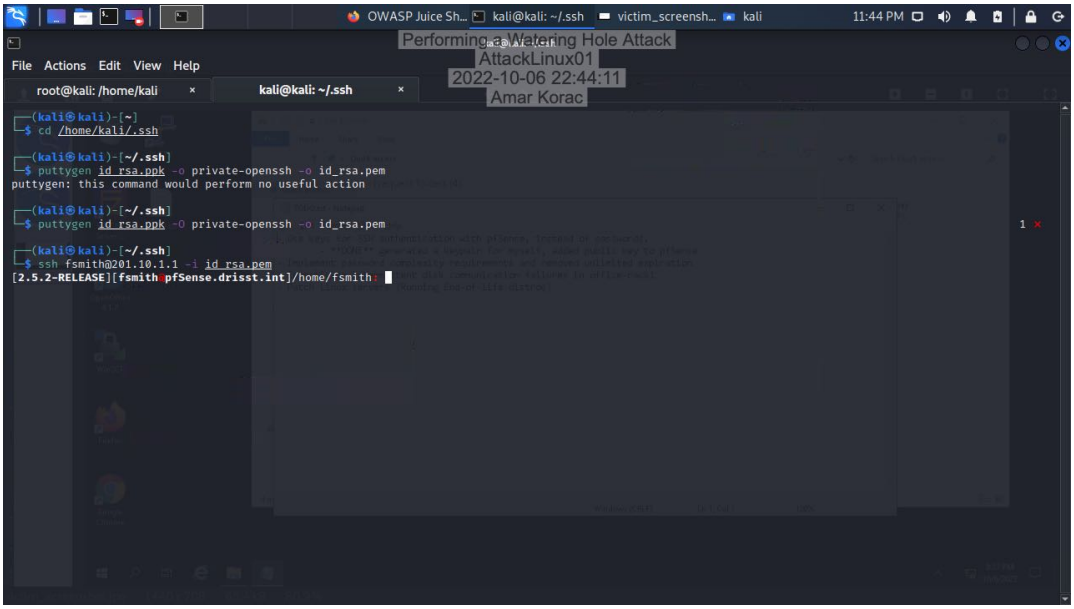
6. **Make a screen capture** showing the **system, user, and idletime information in your output**.



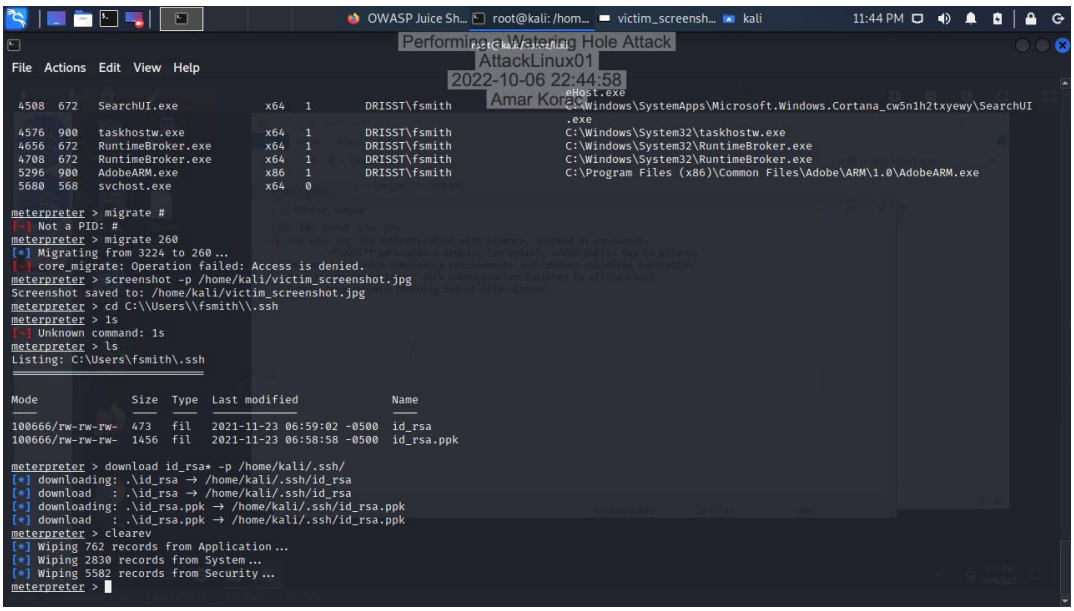
12. **Make a screen capture** showing the **screenshot of the user's desktop and TODO.txt file**.



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?

The recent Watering Hole Attack was performed by the Russian military in Ukraine. The primary target of this attack was accounting software used by the Ukraine government. The attack used infected systems to gain credentials and then spread itself further throughout network systems, coding each hard drive as it traveled. It took three months before the attack was noticed.

Part 2: Configure an Additional XSS Payload

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