Student:	Email:
Belizaire Bassette II	bebasset@syr.edu

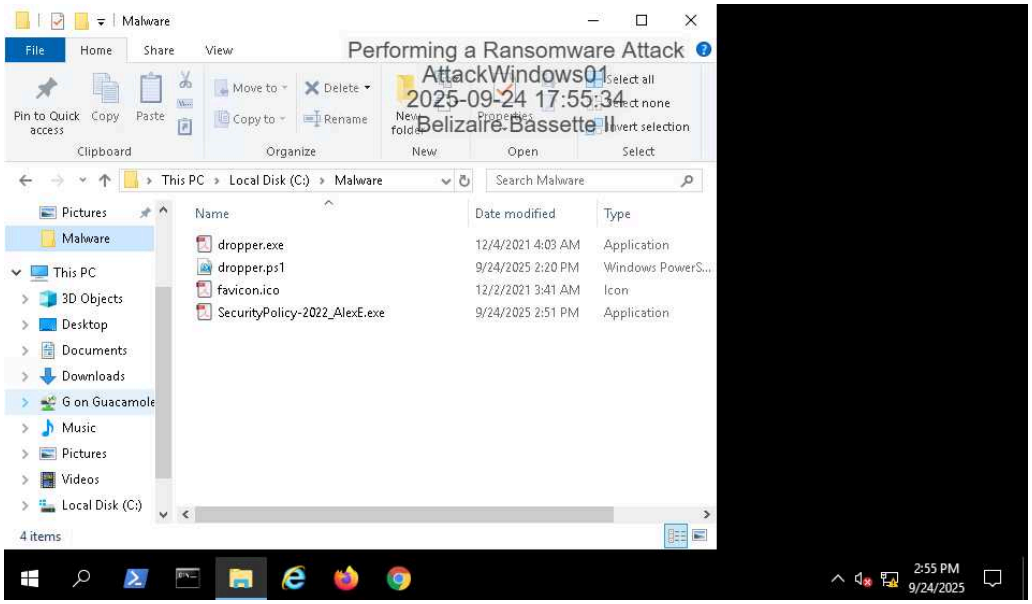
Time on Task:	Progress:
10 hours, 34 minutes	100%

Report Generated: Thursday, September 25, 2025 at 11:25 AM

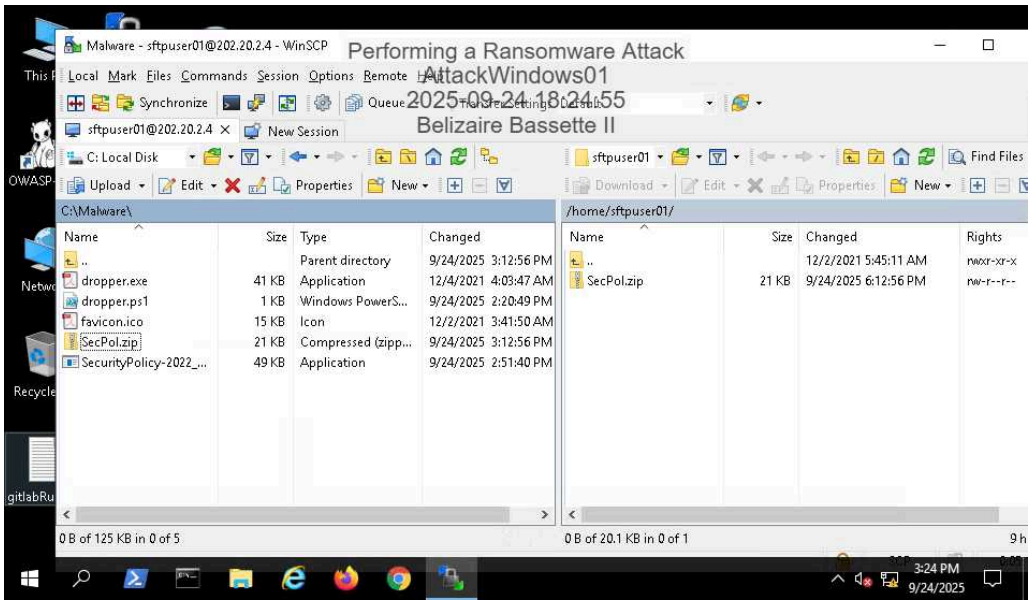
Hands-On Demonstration

Part 1: Prepare a Ransomware Dropper

13. **Make a screen capture** showing the **SecurityPolicy-2022_AlexE.exe file**.

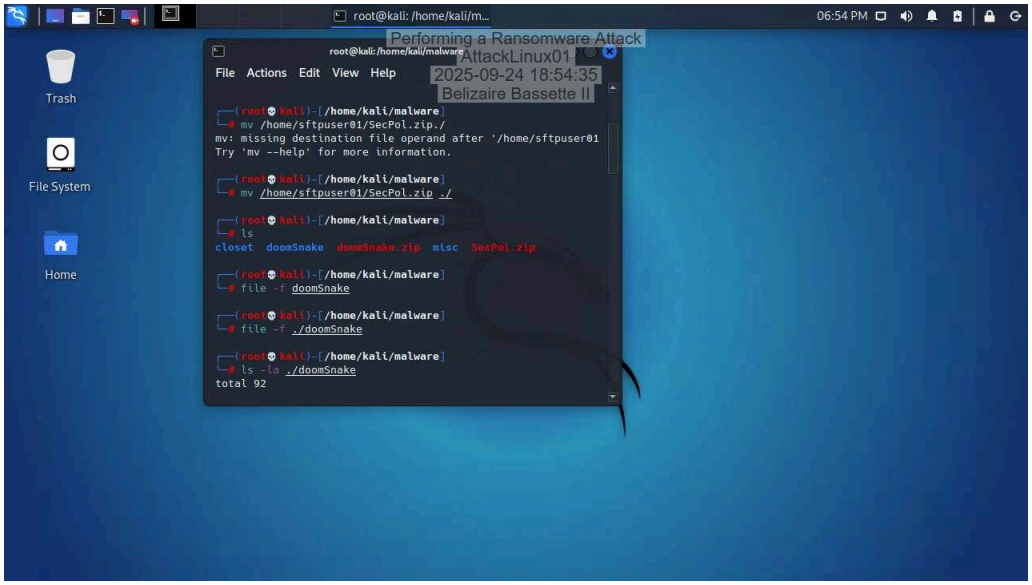


25. **Make a screen capture** showing the **SecPol.zip file in the Remote File Panel**.

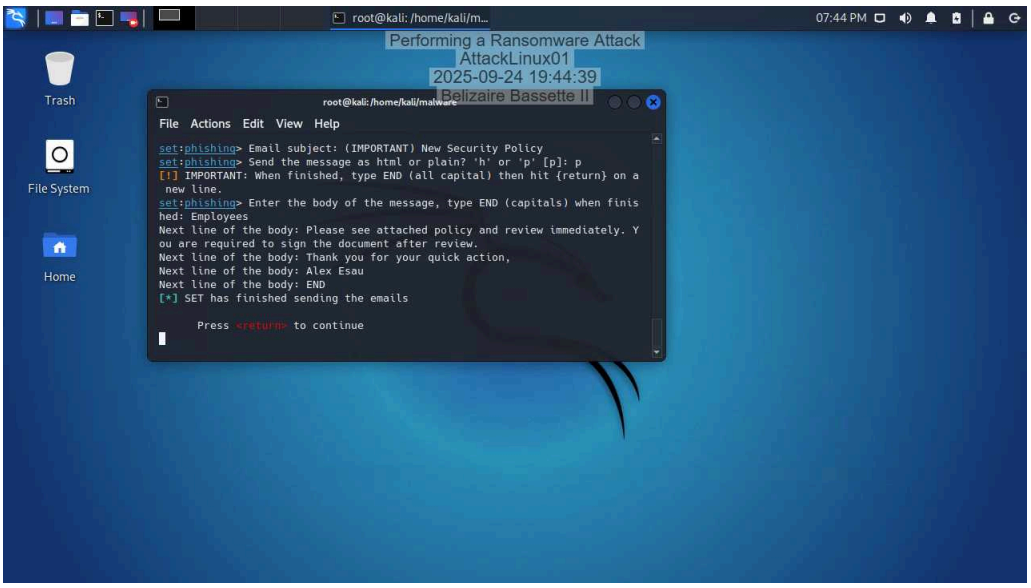


Part 2: Construct a Spear Phishing Email

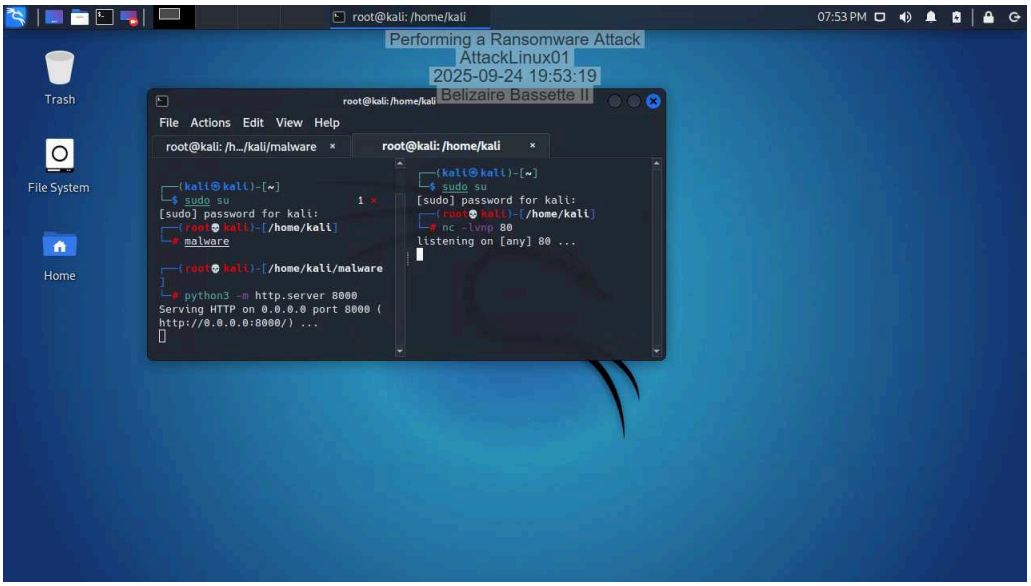
7. **Make a screen capture** showing the **dropper and malware files in the kali user's malware directory**.



27. **Make a screen capture** showing the **confirmation message stating that SET has finished sending the email to your victim**.

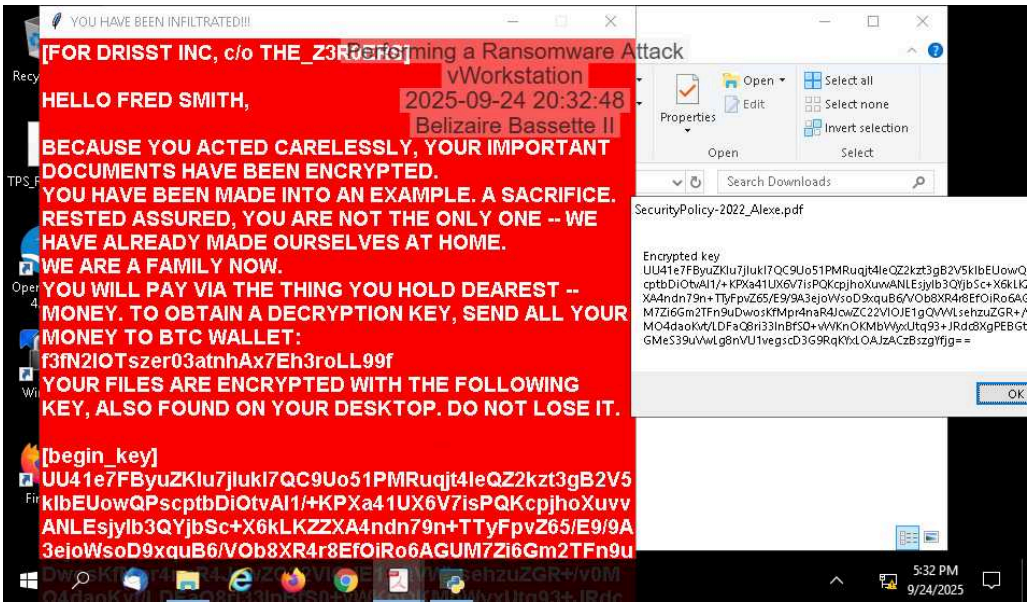


37. **Make a screen capture** showing the **HTTP listener on port 8000 and the Netcat listener running on port 80**.

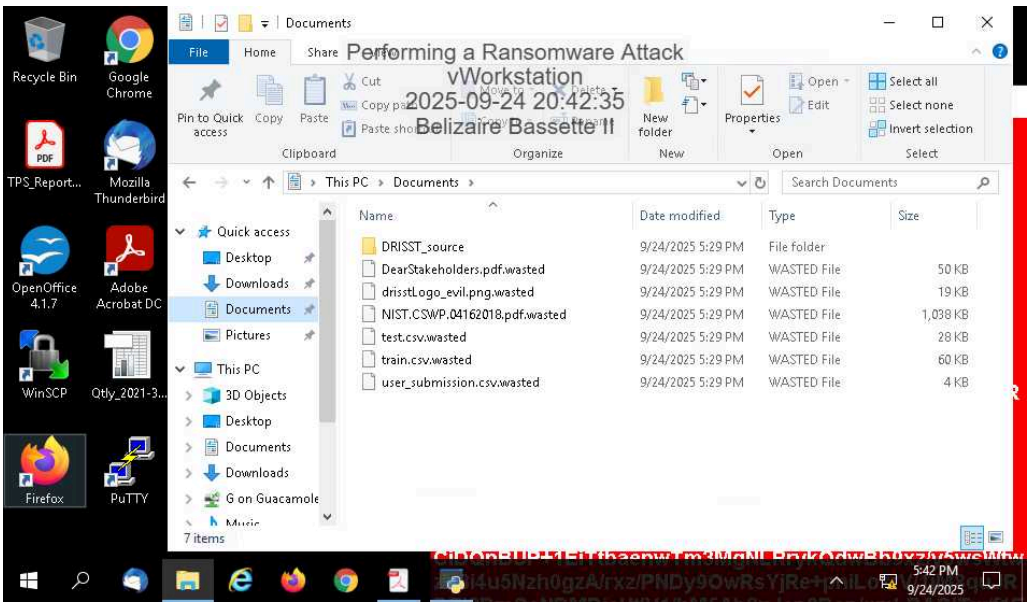


Part 3: Trigger the Ransomware Payload

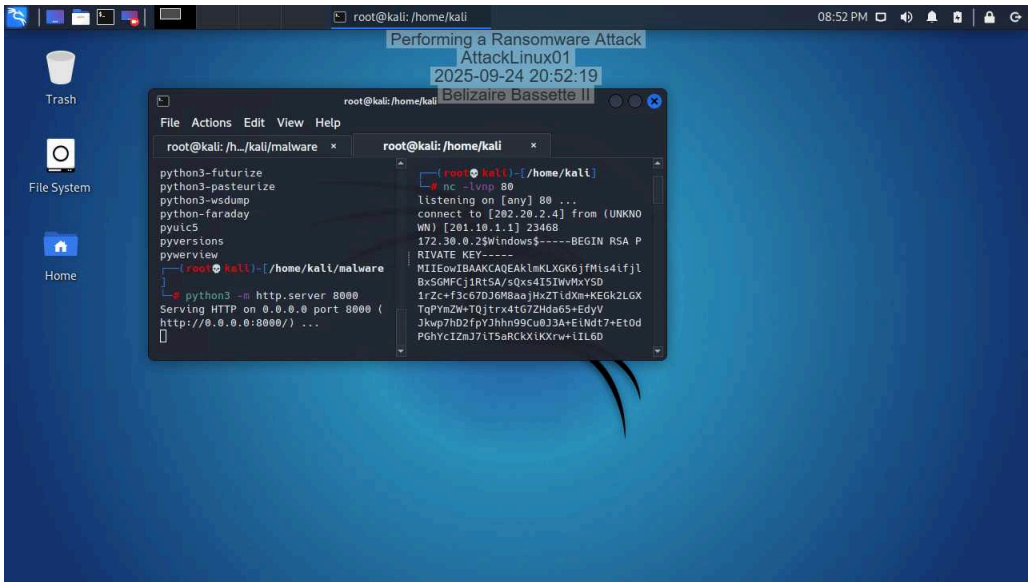
12. **Make a screen capture** showing the **ransomware pop-up**.



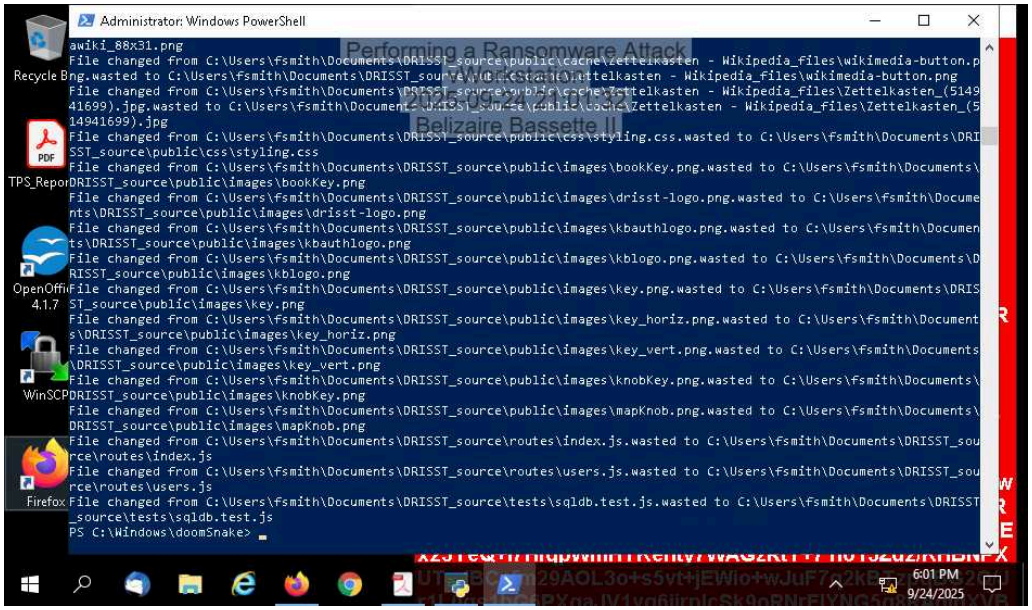
23. **Make a screen capture** showing the **.wasted files in the Documents folder**.



25. **Make a screen capture** showing the **key output returned by your ransomware attack**.



39. **Make a screen capture** showing the **successful decryption**.



Challenge and Analysis

Which type of ransomware was WannaCry?

WannaCry was classified as a crypto ransomware, specifically a ransomware crypto worm

How was the WannaCry attack executed and why?

WannaCry used the EternalBlue SMBv1 exploit (leaked from the NSA) to worm across Windows networks and install ransomware that encrypted files and demanded payment in Bitcoin. It spread automatically—no user click required—using the SMB vulnerability (and a dropped backdoor called DoublePulsar), which caused massive, indiscriminate disruption to hospitals, businesses, and governments. Authorities later linked the campaign to North Korea’s Lazarus Group, and the primary motive appears to have been financial extortion, though its scale caused widespread collateral damage.

How could WannaCry have been avoided?

WannaCry could have been avoided if organizations had promptly applied Microsoft’s MS17-010 security patch, which fixed the EternalBlue SMB vulnerability. Disabling or restricting SMBv1 file-sharing protocol on networks would also have limited its spread. Additionally, maintaining strong backup practices and up-to-date antivirus/IDS monitoring would have reduced both exposure and impact.