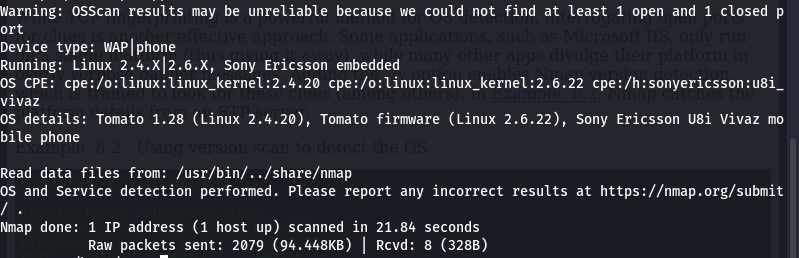
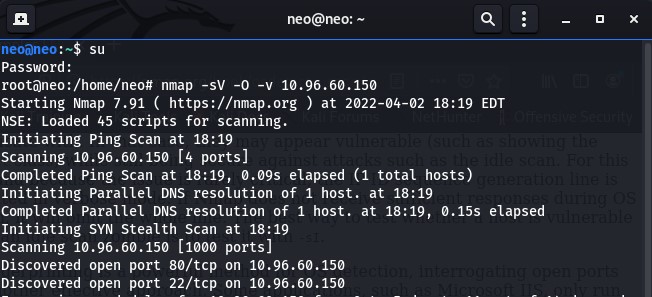
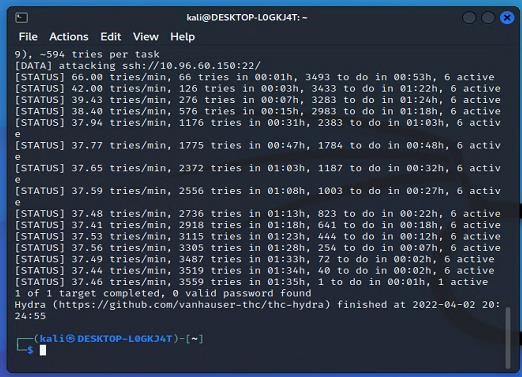
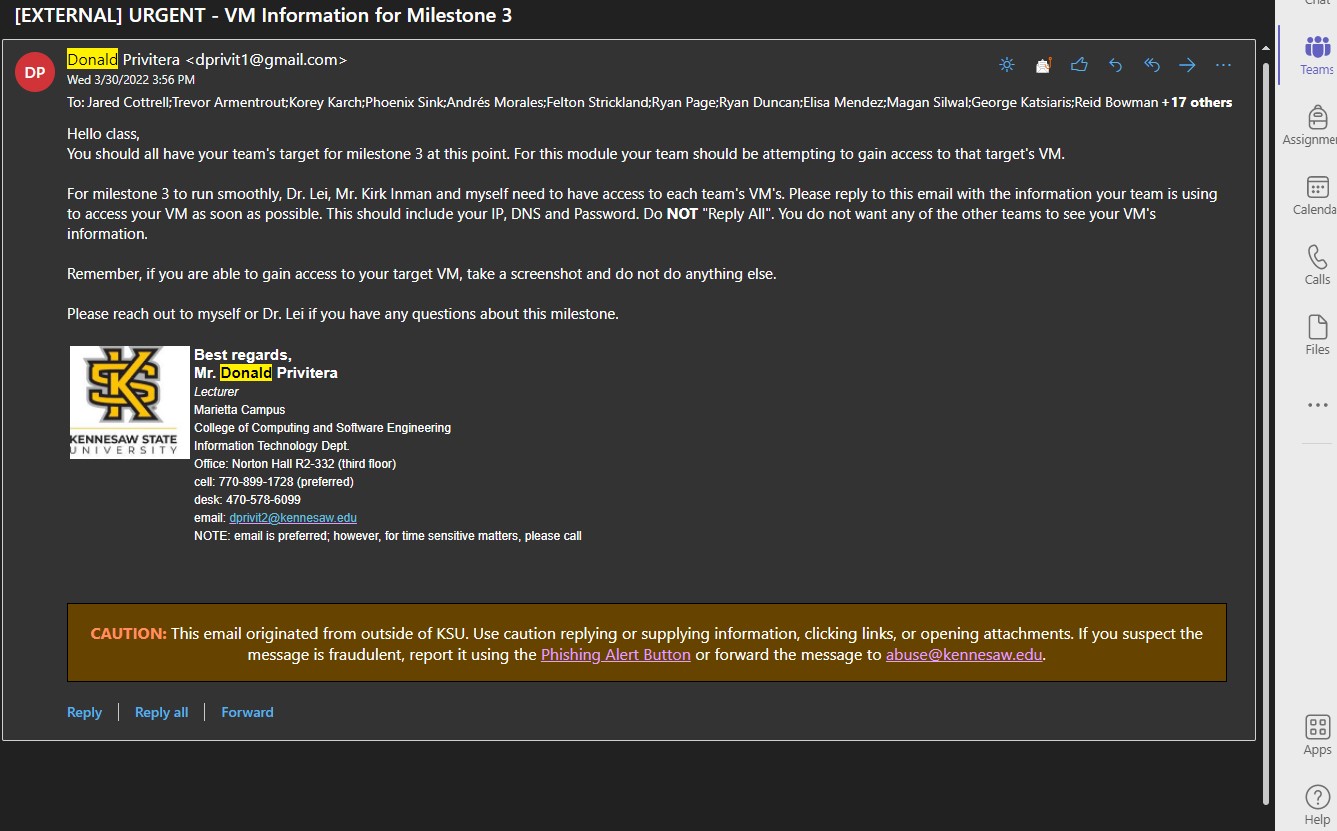
1. **The images below show host information such as server’s OS, open ports, and firmware from Nmap. OS details may not be accurate.**



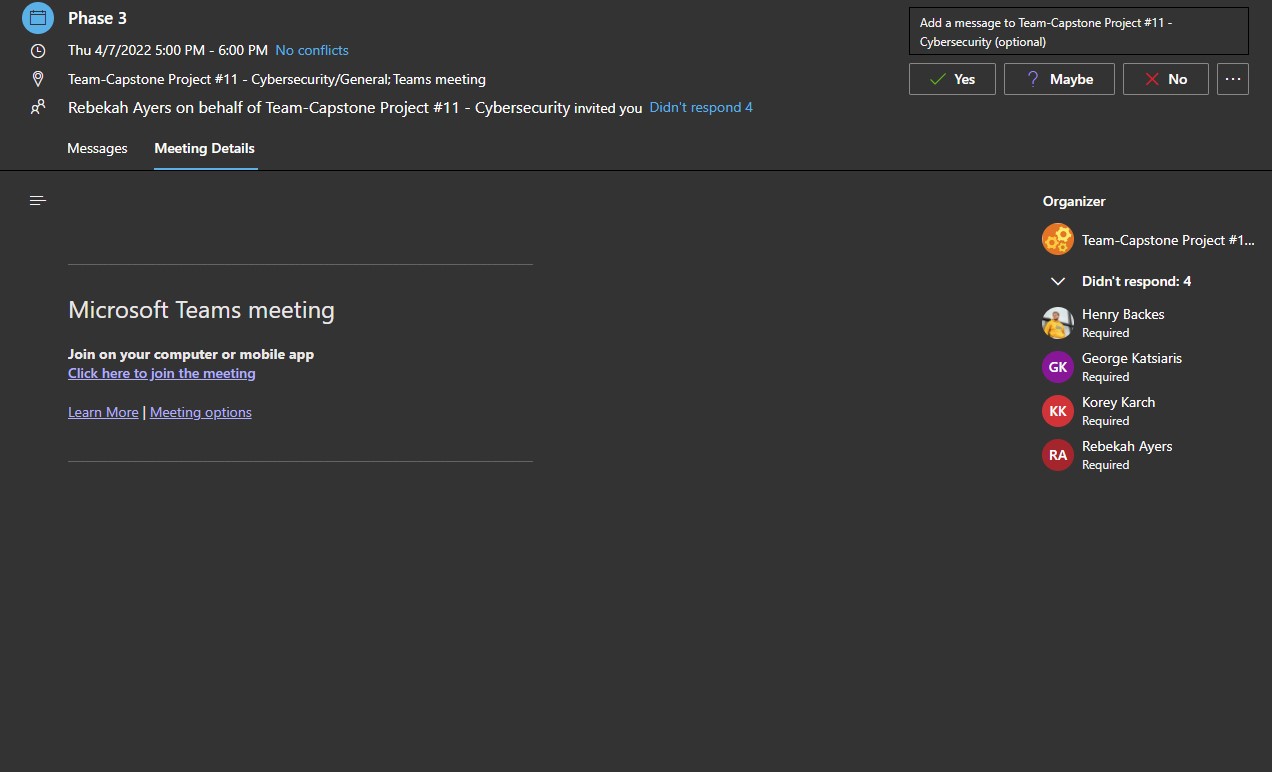
1. Attempted to do a brute force password attack with HYDRA.



1. Copy of other team failed phishing attack.

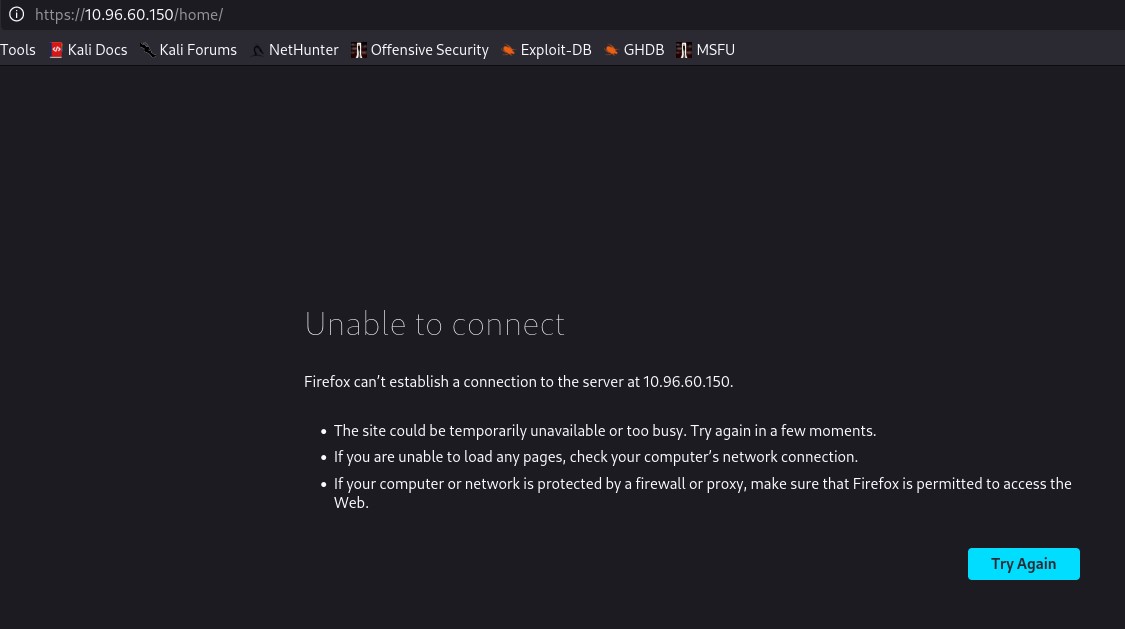


1. Possible Phish from Rebekah Ayers(Team Lead) of different group.

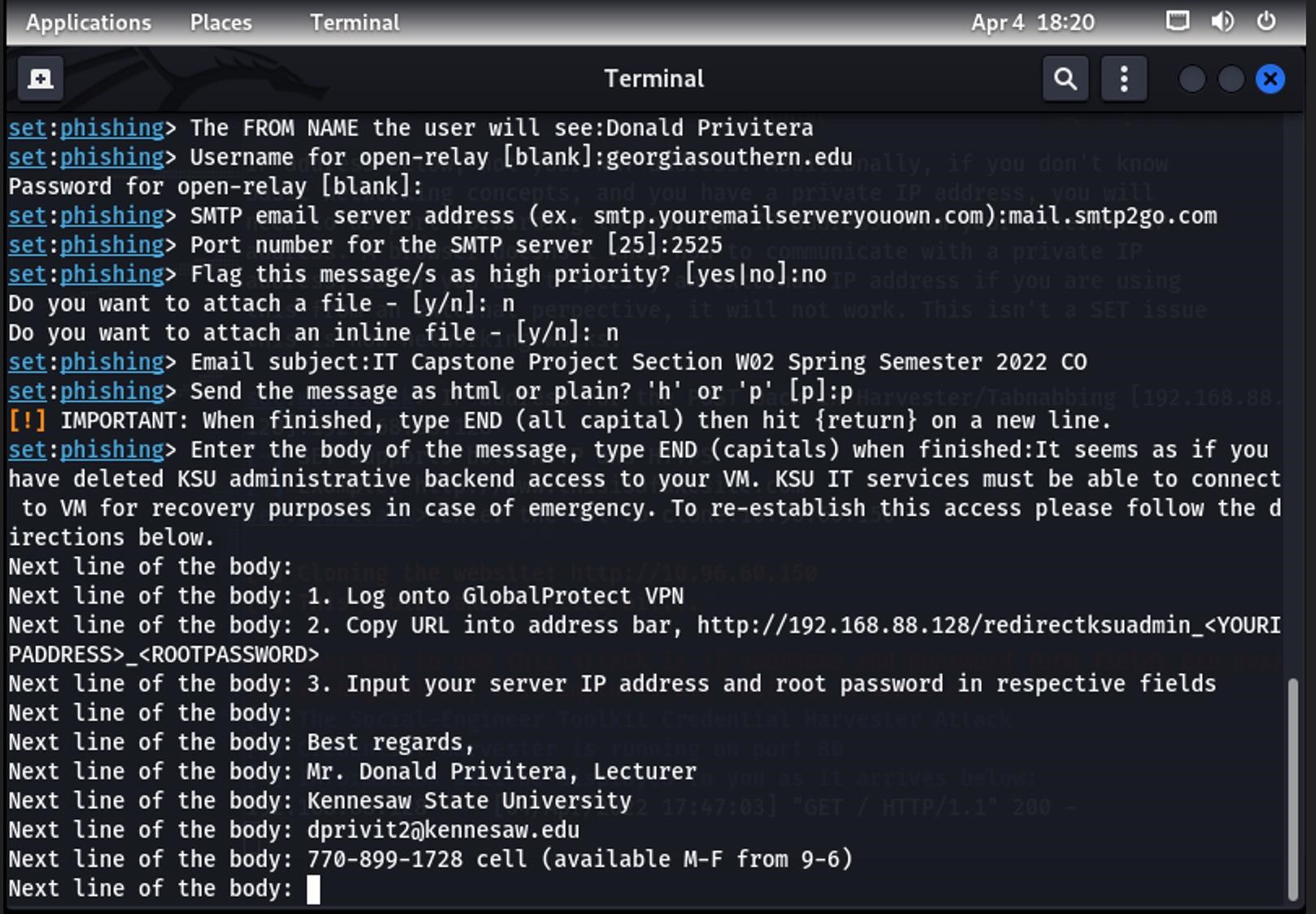


5.

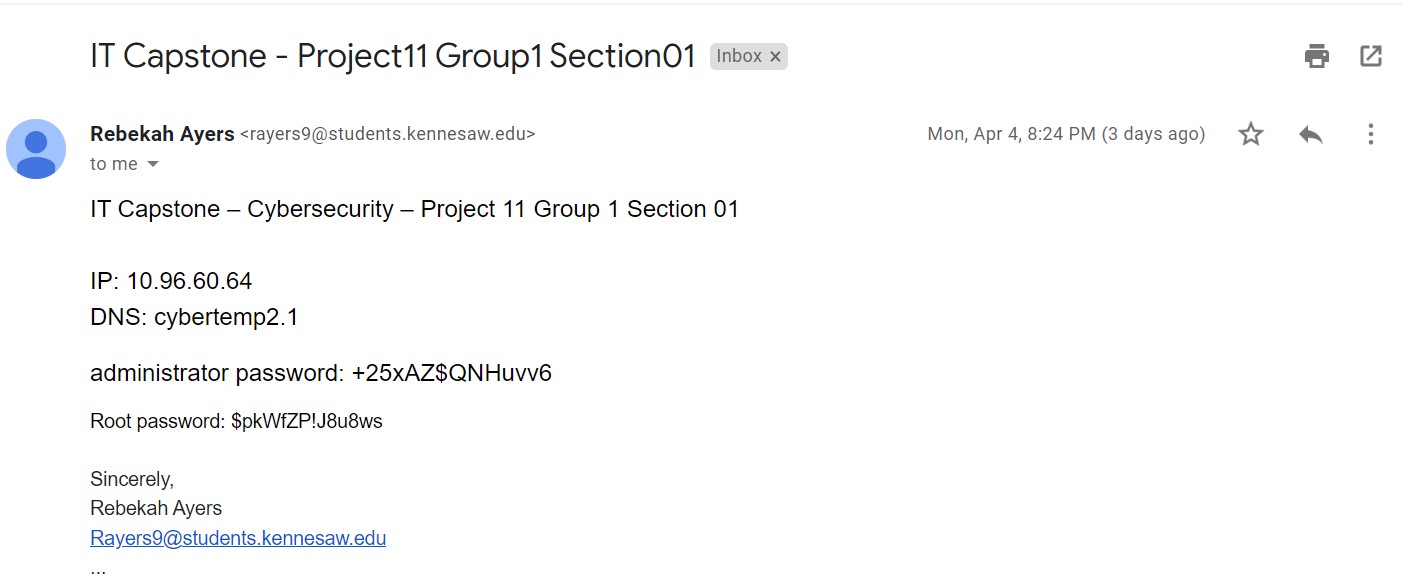
HTTPS is not enabled on site



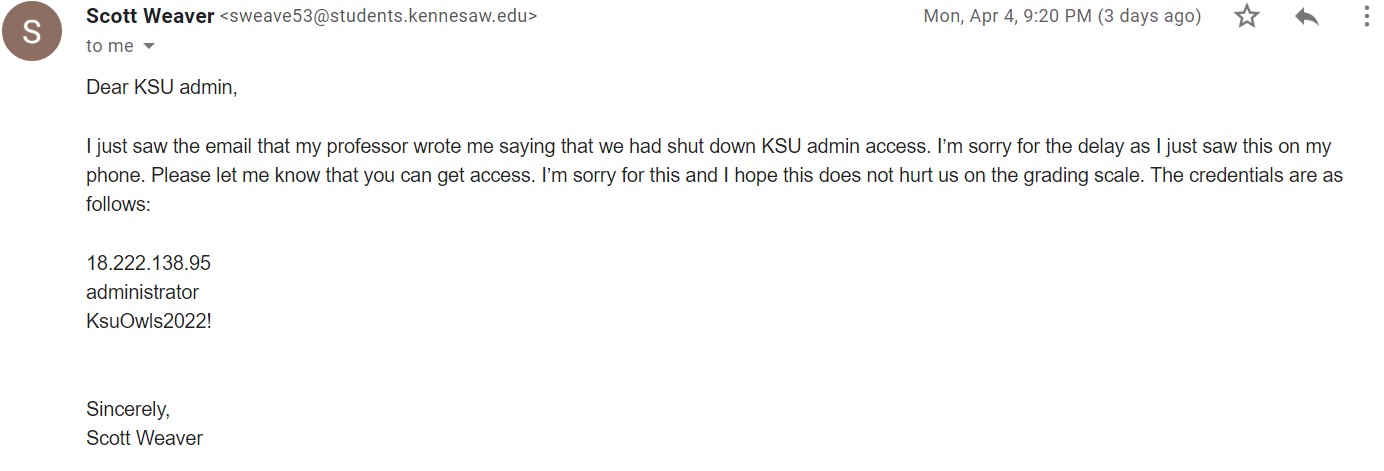
1. Social engineering phishing attack on all group leaders by spoofing email. Complexity of VPN preventing this attack from being effective.



1. I was able to successfully log into this team’s VM with provided credentials



1. Scott Weaver provided me with false information regarding his team’s VM. As you can see the IP address is not even on the same subnet as other VM’s.



1. Tested site to see if XSS vulnerability was present and exploitable. Vulnerability is not present, which may be a sign that a WAF may be installed even though the site is using HTTP only.

