Randolph Domigpe

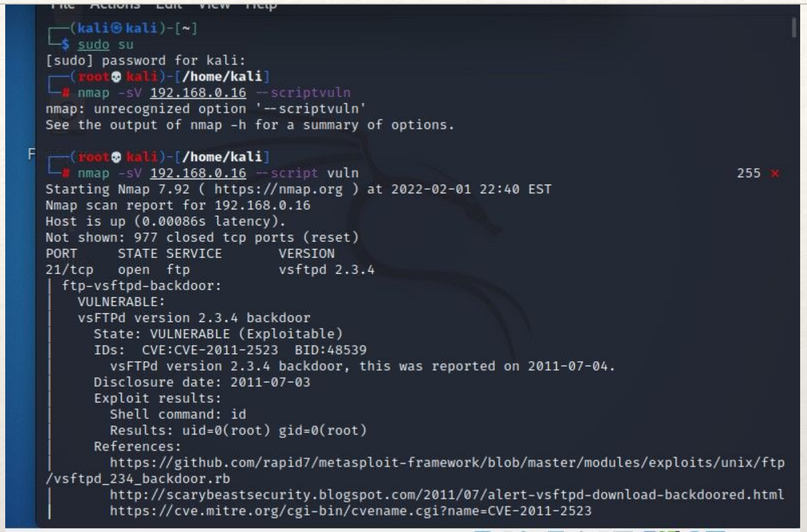
Project C - Ethical Hacking

Executive Summary

Demonstrate my ability to scan a computer for vulnerabilities, analyze those vulnerabilities for exploitability, execute exploits against a target computer, and create persistence.

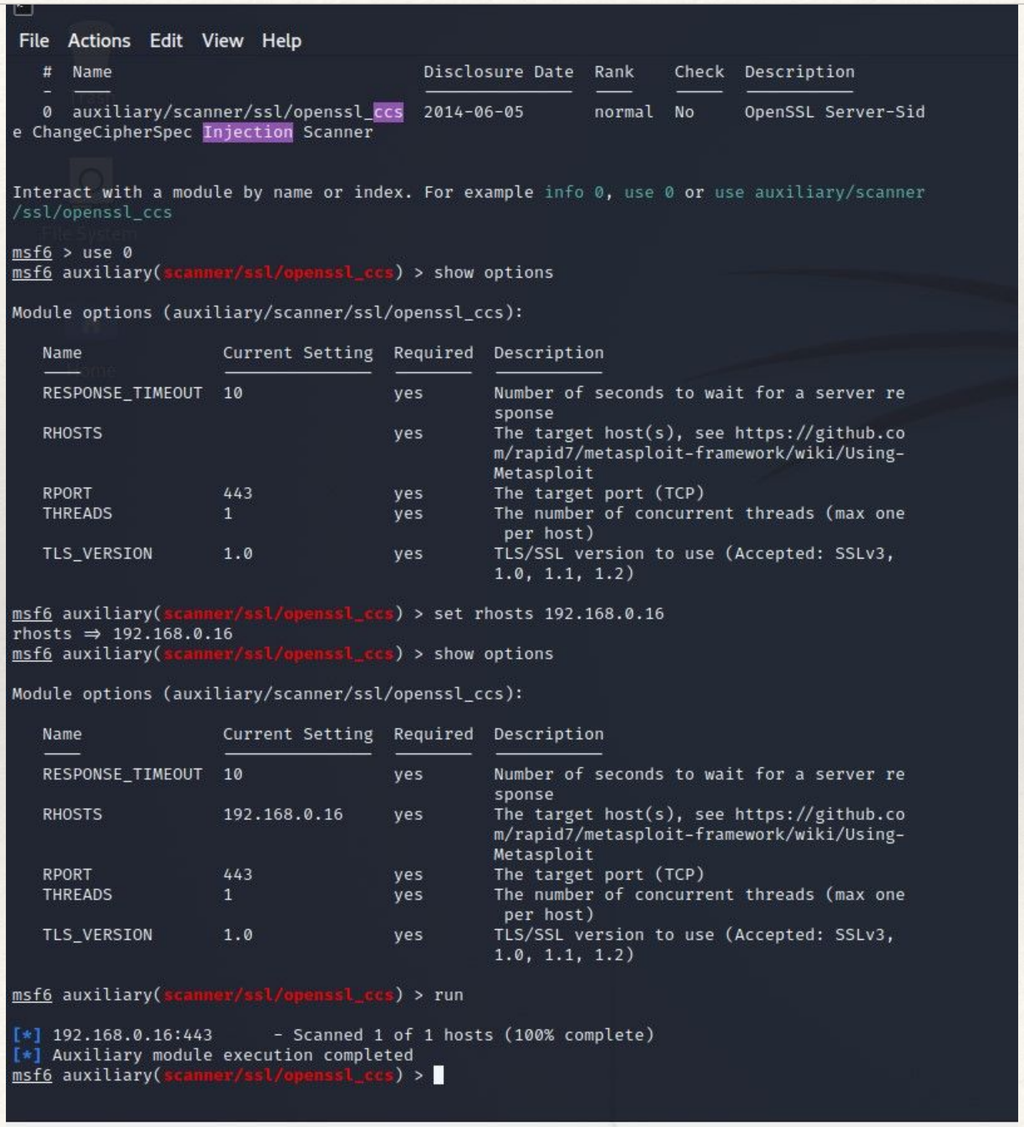
Possible vulnerabilities on production server

- Used Nmap in Kali-linux(trusted network).
- nmap -sV 192.168.0.16 —script vuln
- Possible vulnerabilities include, Backdoor attacks, SSL attacks, and man in the middle attacks.



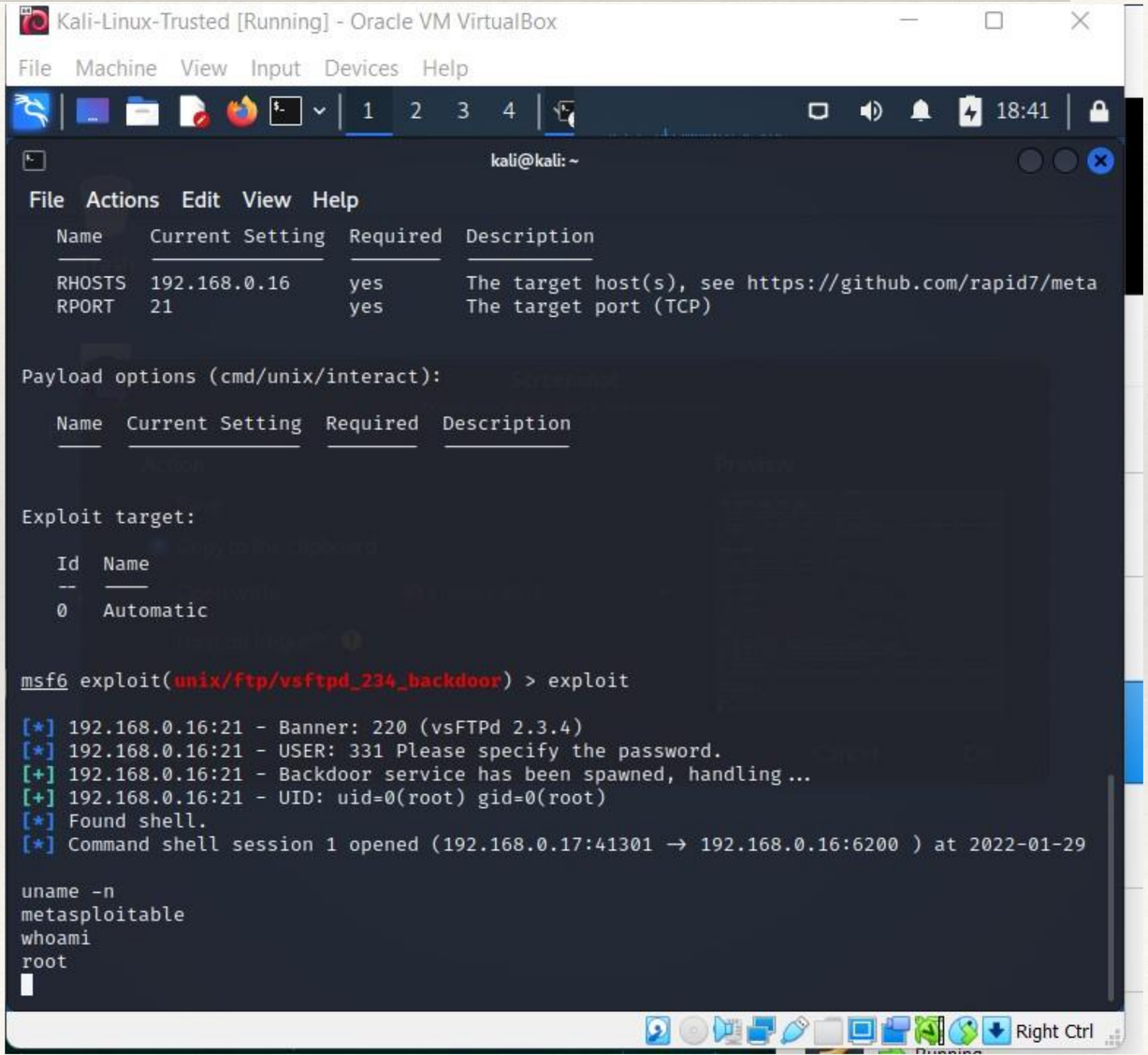
Exploiting vulnerabilities on the Production server

- Exploiting a “Man in the middle attack”(SSL poodle)
- Search “Poodle”
- Use (index #)
- Show options
- Set rhost (target subnet)
- To check= “Show options”
- RUN



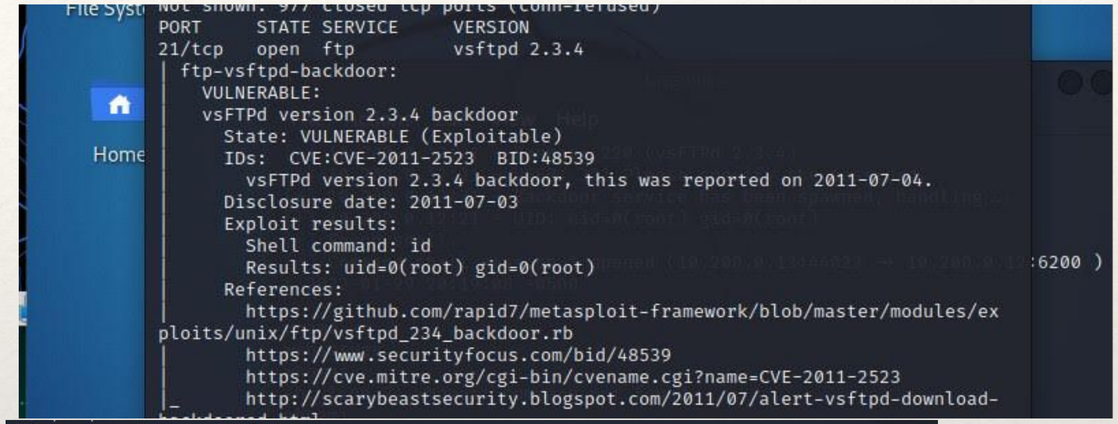
Exploiting the Production server cont.

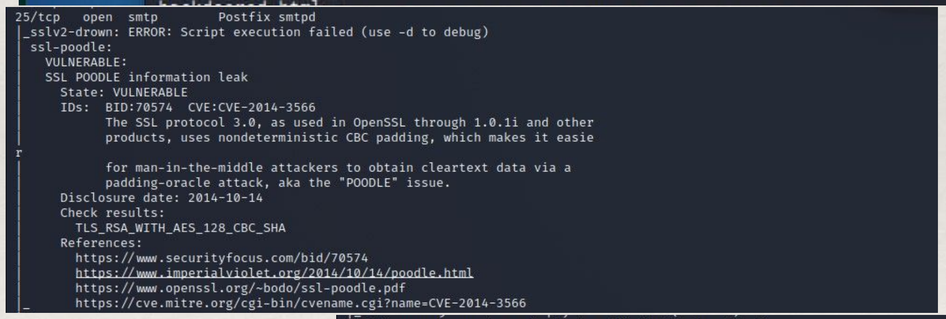
- Exploiting the Production server using a back door attack (vsftpd)
- Search “vsftpd”
- Use (index #)
- “Show options”
- Set hosts (target subnet)
- To check = “Show options”
- EXPLOIT
- To check if you have root access = “whoami”

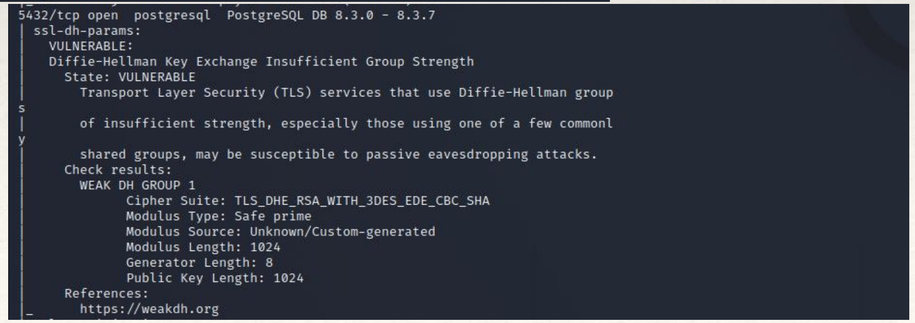


Possible vulnerabilities on the Web server

- Nmap -sV 10.200.0.12
- Possible vulnerabilities on the Web server include, Backdoor attacks, Man in the middle attacks, SSL attacks, and DOS attacks.

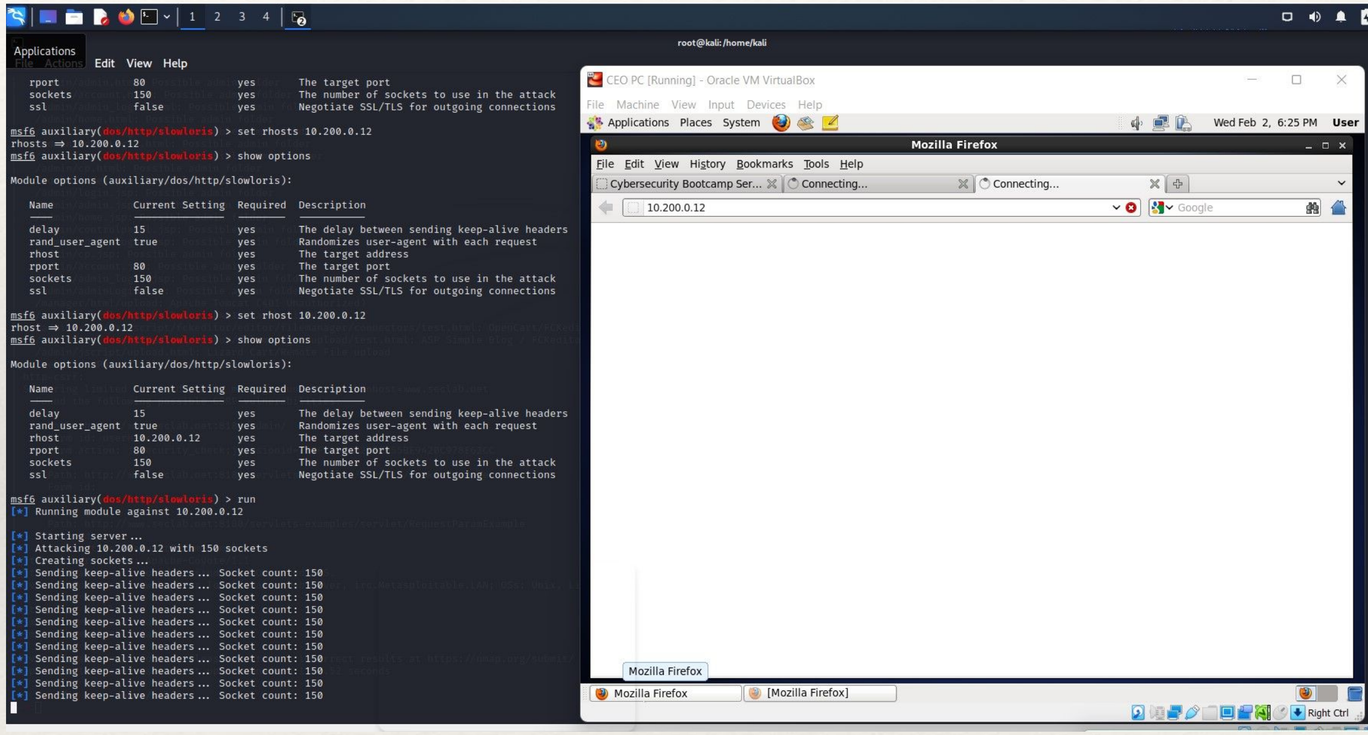






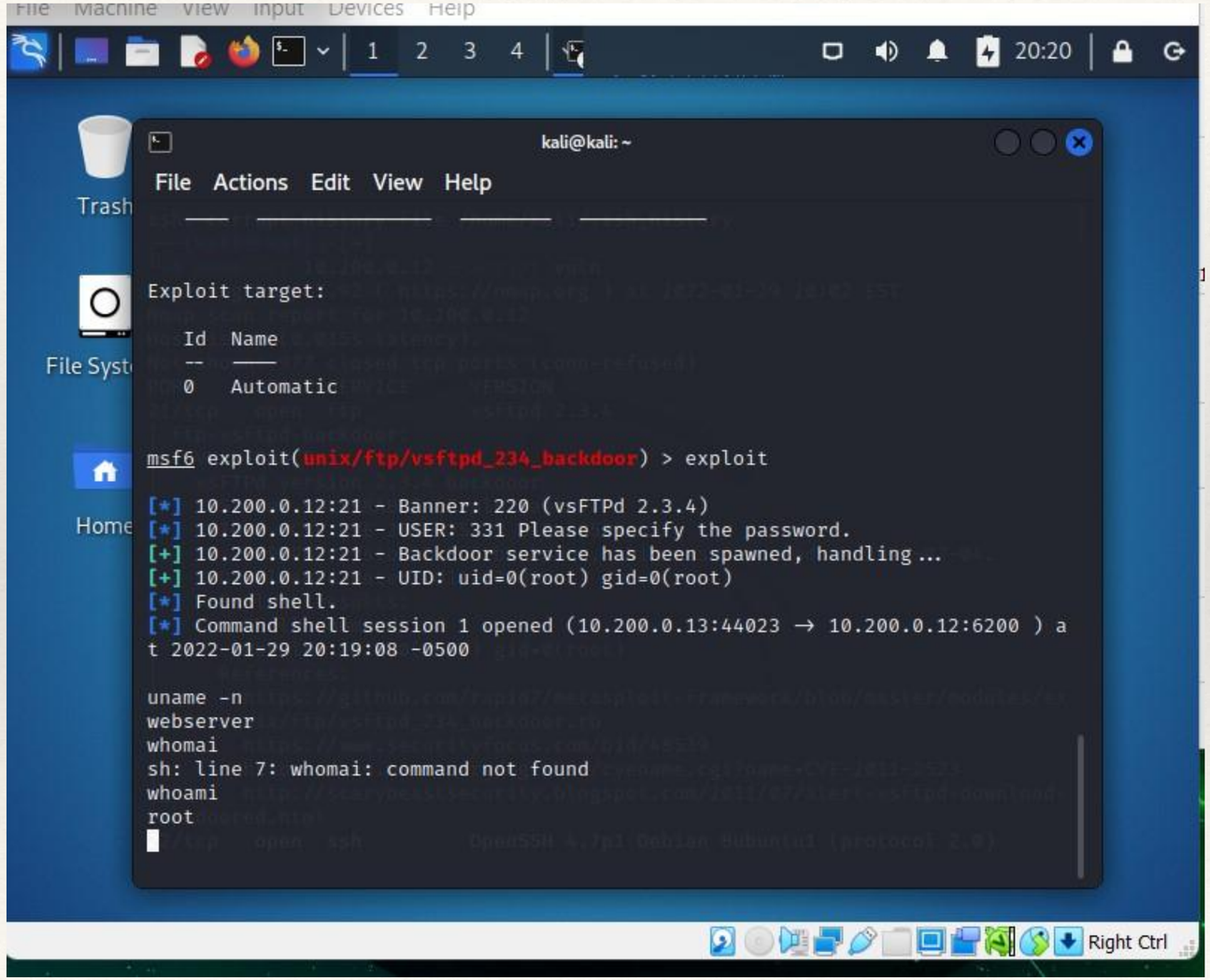
Exploiting vulnerabilities to the Web server

- Exploiting the web server using a DOS attack (Sloworis)
- Search “slowloris”
- Use (index #)
- “Show options”
- Set rhost (Target subnet) * to check= show options again*
- RUN
- ***to stop attack, CTRL +C



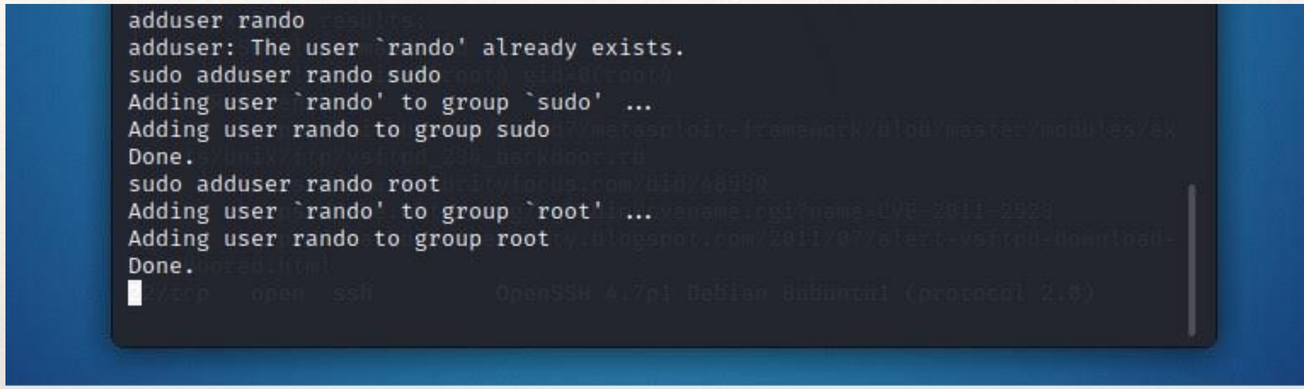
Exploiting vulnerabilities on Web server cont.

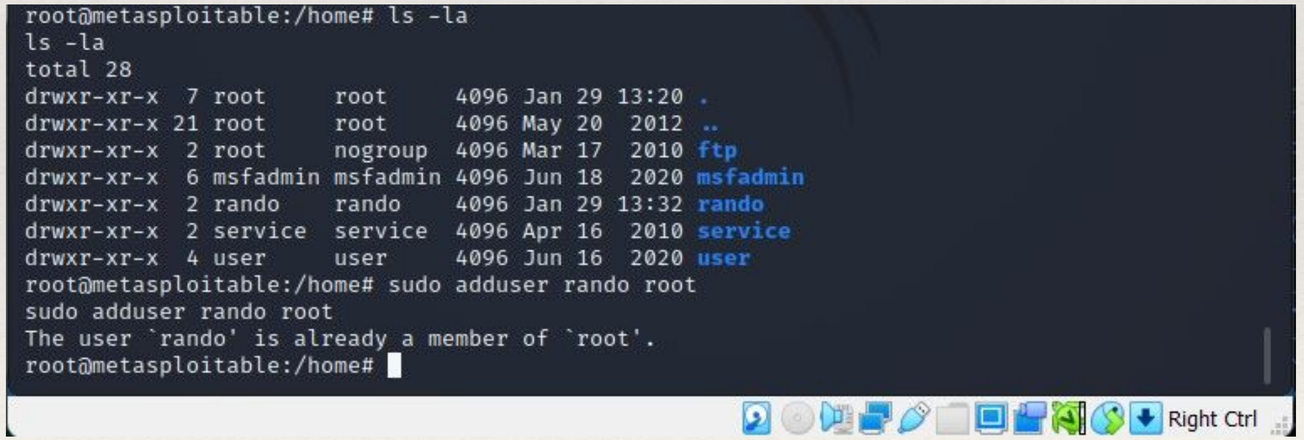
- Exploiting the Web server using a back door attack (vsftpd)
- Search “vsftpd”
- Use (index #)
- “Show options”
- Set rhost (target subnet) *to check= “Show options”
- “exploit”
- To show I have root access, “whoami”



Creating an account on the Production sever

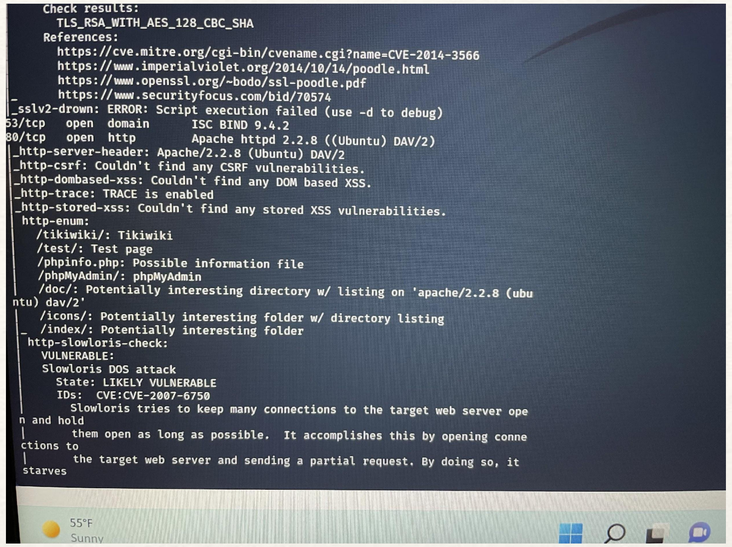
- Once gaining root access by using a backdoor attack (fsftpd)
- “Adduser” (username)
- “Sudo adduser” (username) root
- Ls -la =Directory

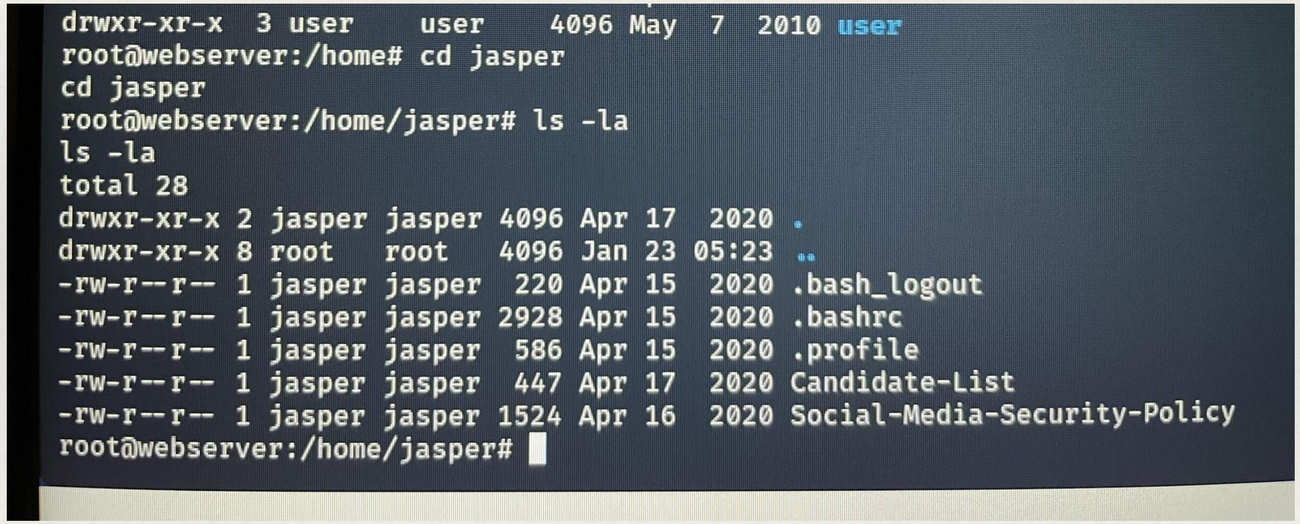




Interesting files on Production and Web server

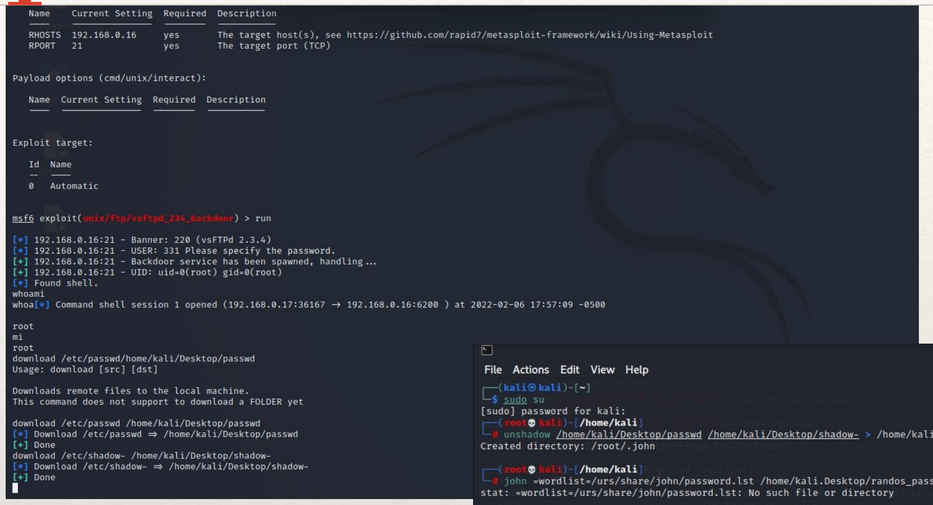
- When using Nmap to to find vulnerabilities I found “Potentially interesting folder w/ directory listing”
- Using Metasploit and gaining root access with a backdoor attack(fsftpd), I was able to view the contents of the jasper folder.
- The jasper folder had a file called, “Candidate-List”.

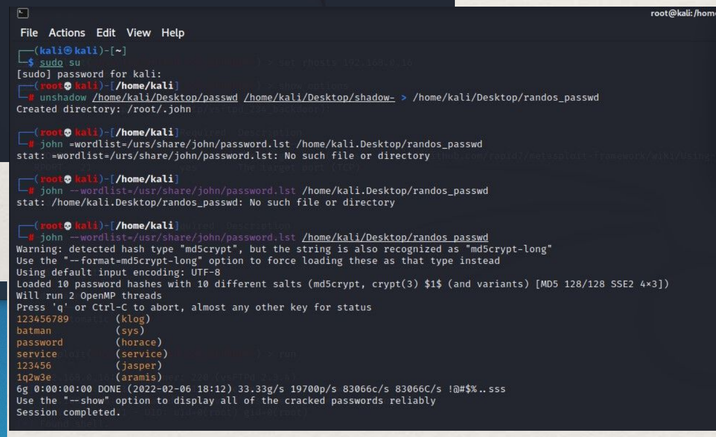


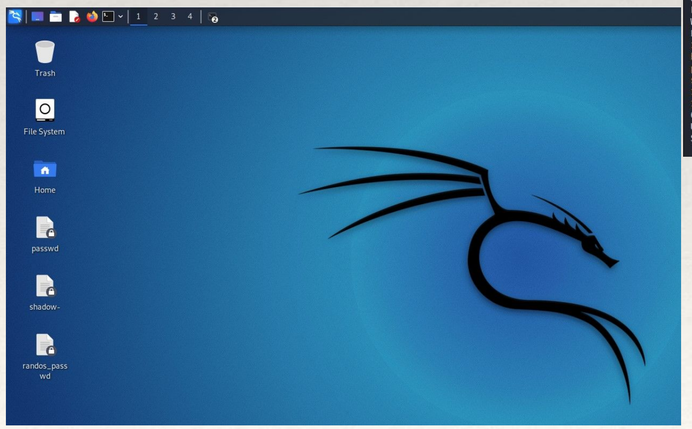


Cracking passwords on the Production server

- Cracked passwords on the production server using, “John the ripper”
- UserName: klog /Password:123456789
- Username: sys /Password:batman
- Username: horace /Password:password
- Username: service /Password:service
- Username: jasper /Password:123456
- Username: aramis /Password:1q2w3e







Recommendations and closing remarks

- Patch and update systems
- Always change default passwords
- Be careful what you click
- Never leave devices unattended
- Install antivirus software
- Backup your computer