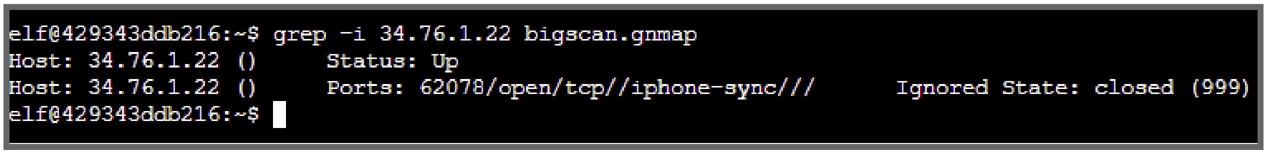
Grepping for Gold
SANS Holiday Hack 2021

Isaac Falero
IS 401/501
11/7/2023

1. **What port does 34.76.1.22 have open?**



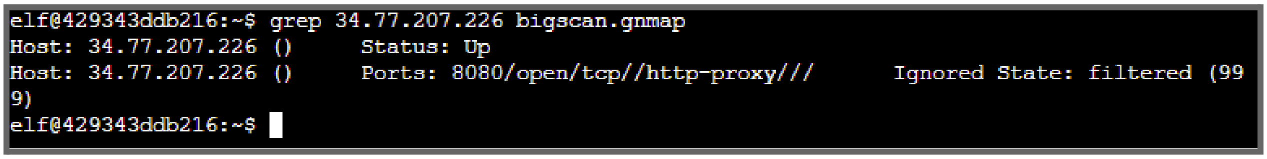
```
elf@429343ddb216:~$ grep -i 34.76.1.22 bigscan.gnmap
Host: 34.76.1.22 ()     Status: Up
Host: 34.76.1.22 ()     Ports: 62078/open/tcp//iphone-sync///      Ignored State: closed (999)
elf@429343ddb216:~$ 
```

Answer: 62078

Command: grep 34.76.1.22 bigscan.gnmap

Explanation: This command searches for and displays all the lines containing the specified IP address from the specified file.

2. **What port does 34.77.207.226 have open?**



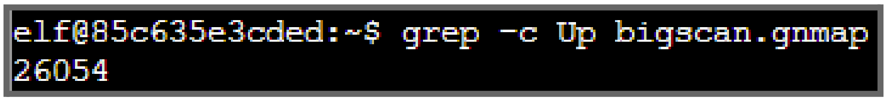
```
elf@429343ddb216:~$ grep 34.77.207.226 bigscan.gnmap
Host: 34.77.207.226 ()     Status: Up
Host: 34.77.207.226 ()     Ports: 8080/open/tcp//http-proxy///      Ignored State: filtered (99
9)
elf@429343ddb216:~$ 
```

Answer: 8080

Command: grep 34.77.207.226 bigscan.gnmap

Explanation: This command searches for and displays all the lines containing the specified IP address from the specified file.

3. **How many hosts appear "Up" in the scan?**



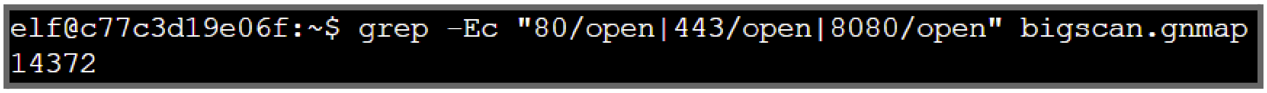
```
elf@85c635e3cded:~$ grep -c Up bigscan.gnmap
26054
```

Answer: 26054

Command: grep -c Up bigscan.gnmap

Explanation: This command searches for the specified string in the file. The “-c” flag instructs the grep command to output the number of lines in the file that contain the string.

4. **How many hosts have a web port open? (Let's just use TCP ports 80, 443, and 8080)**



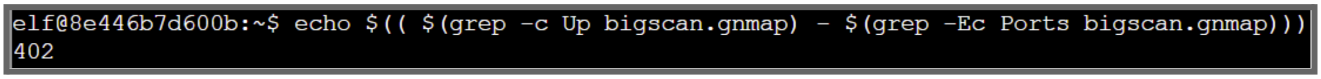
```
elf@c77c3d19e06f:~$ grep -Ec "80/open|443/open|8080/open" bigscan.gnmap
14372
```

Answer:14372

Command: grep -Ec "(80|443|8080)/open" bigscan.gnmap

Explanation: This command searches for the specified ports in the file. The “-E” flag instructs the grep command to accept extended regular expressions. The “-c” flag instructs the grep command to output the number of lines in the file that contain the string.

5. **How many hosts with status Up have no (detected) open TCP ports?**



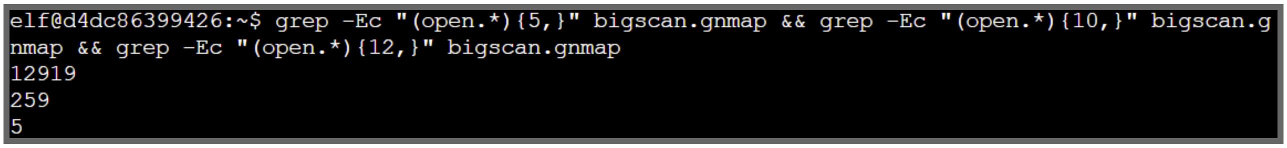
```
elf@8e446b7d600b:~$ echo $(( $(grep -c Up bigscan.gnmap) - $(grep -Ec Ports bigscan.gnmap)))
402
```

Answer: 402

Command: echo $(($(grep -c Up bigscan.gnmap) - $(grep -Ec Ports bigscan.gnmap)))

Explanation: The counted results of the two grep commands are enclosed in “$((...))”, which indicates that the shell should perform arithmetic operations on the enclosed expressions.

6. **What's the greatest number of TCP ports any one host has open?**



```
elf@d4dc86399426:~$ grep -Ec "(open.*){5,}" bigscan.gnmap && grep -Ec "(open.*){10,}" bigscan.g
nmap && grep -Ec "(open.*){12,}" bigscan.gnmap
12919
259
5
```

Answer: 12

Command: grep -Ec "(open.*){5,}" bigscan.gnmap && grep -Ec "(open.*){10,}" bigscan.gnmap && grep -Ec "(open.*){12,}" bigscan.gnmap

Explanation: This command begins with a search for lines in the file that contain the regular expression pattern "(open.*){5,}". The pattern “(open.*){5,}” matches lines that have the string "open" followed by any characters repeated at least 5 or more times. The && operator is used to combine multiple grep commands that use the same search pattern but for greater instances of repetition (10 and 12).