Government Incident Drill 2014

Kitisak Jirawannakool

Electronics Government Agency
(public organisation)

Agenda

- What is Incident Drill?
- Why we need?
- Objectives
- Overview scenarios
- Tools
- Tasks

Incident Drill

- Incident Response Process
- Exercises
- Methodologies
- Communication channels
- CSIRT

Incident Response Process

User

1. Someone report or you found by yourself

2. Solve the problems

Incident

3. Inform to ECC to keep recording or ask for help from EGA

EGA Contact Center

4. ECC will forward your requests to G-CERT

G-CERT

Incident Response Process

EGA CC

1. G-CERT inform to ECC

5. ECC inform to G-CERT

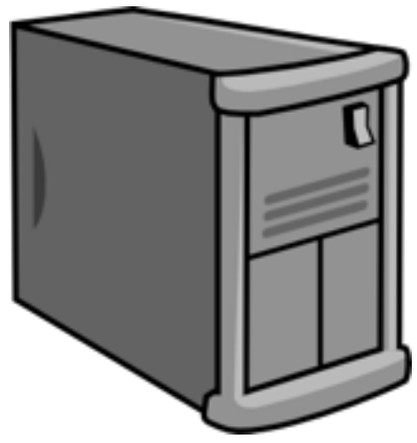
2. ECC notify User via E-mail and Phone

4. User reply to ECC
- receive already
- fix already
- accept the risk
- require EGA's help

User

3. Check the system deeply

G-CERT



Servers and Network

Why we need?

- To test and improve the incident response process
- To check the readiness of our staffs and stakeholders
- To find the most suitable communication channel
- To build the community to exchange knowledge among members

Objectives (for this drill)

- Know more each others
- Focus on the communication methodologies
- Little technical
- Test communication among all stakeholders
- Learn some simple techniques to investigate cases
- Discuss about responding process and others

How to investigate?

- We will focus on ....
  - Mail header => for every cases which are related to email
  - IP address => One of our target which we want to find
- Need to understand about IT (a.k.a. Computer, Network, OS, etc.)
- Depends on our imagine and creative idea
- Maybe need to guess attacker's behavior

Mail header

Hide

From:	**STA Travel <newsletter@statravel.co.za>**
Subject:	[MARKETING] Get 20% off selected tours. See Cambodia from only R5050!
Date:	April 24, 2555 BE 9:38:58 PM GMT+07:00
To:	kitisak@nectec.or.th
Reply-To:	newsletter@statravel.co.za
Return-Path:	<v-fapofm_bncflpgeo_lnaagke_lnaagke_a@bounce.mkt293.com>
Delivered-To:	kitisak@nectec.or.th
Received:	(qmail 19890 invoked from network); 24 Apr 2012 14:39:03 -0000
Received:	from unknown (HELO mailgateway2.nectec.or.th) ([10.226.48.170]) (envelope-sender <v-fapofm_bncflpgeo_lnaagke_lnaagke_a@bounce.mkt293.com>) by nectec.or.th (NectecNet Mail) with SMTP for <kitisak@nectec.or.th>; 24 Apr 2012 14:39:03 -0000
Received:	(qmail 22183 invoked by uid 98); 24 Apr 2012 14:39:03 -0000
Received:	from 203.185.132.74 by mailgateway2.nectec.or.th with Mailgateway-Engine-1.0 24 Apr 2012 14:39:03 -0000
Received:	from unknown (HELO imail.nectec.or.th) (203.185.132.74) by mailgateway2.nectec.or.th with SMTP; 24 Apr 2012 14:39:03 -0000
Received:	from mail1240c.mkt293.com (HELO mail1240c.links.statravel.co.uk) ([74.112.64.14]) by imail.nectec.or.th with ESMTP; 24 Apr 2012 21:39:00 +0700
Received:	by mail1240c.links.statravel.co.uk (PowerMTA(TM) v3.5r16) id hiqtga0iiksm for <kitisak@nectec.or.th>; Tue, 24 Apr 2012 14:38:58 +0000 (envelope-from <v-fapofm_bncflpgeo_lnaagke_lnaagke_a@bounce.mkt293.com>)
X-Ironport-Anti-Spam-Filtered:	true
X-Ironport-Anti-Spam-Result:	AogCAGGtlk9KcEAOmWdsb2JhbABEgkYMgxMDmjylOQGFOYQCAQEBAQElCwsHFCeCEyAKEwMBAggDKQEFPRkCAjEbGQsdAQOHbgumZQFuK4MegU6OKAEGiniDNIlNgRiVfoERkhaBVgY
Dkim-Signature:	v=1; a=rsa-sha1; c=relaxed/relaxed; s=spop; d=statravel.co.za; h=Date:From:Reply-To:To:Message-ID:Subject:MIME-Version:Content-Type:List-Unsubscribe; i=newsletter@statravel.co.za; bh=tlhyqmW4MbasQj3d4lQJJuSKHg4=; b=fed5y6hsUi9YH2GyYBsiadS50lCmYonaDUmRnJJSLpbAl6l6SXK2GmviEThAObYle0DtucVKzMc8 uHAUNSaEfw==
Domainkey-Signature:	a=rsa-sha1; c=nofws; q=dns; s=spop; d=statravel.co.za; b=QAp9GYa234rH6dvbegCzxWewnffvrKGayKtkCE2EK5DjYJViPdjyTXwS5lLyZpZRHxKV1Bnp5NV0 Bb3UNyqR6A==;
Message-Id:	<122461090.210335951335278338097.JavaMail.app@rbg32.atlis1>
Mime-Version:	1.0
Content-Type:	multipart/alternative; boundary="----=_Part_75301_962745790.1335278317907"
X-Mid:	5307996
X-Job:	5307996
X-Orgid:	11147
List-Unsubscribe:	<mailto:v-fapofm_bncflpgeo_lnaagke_lnaagke_a@bounce.mkt293.com?subject=Unsubscribe>

Find the "Received"

Hide

From: **STA Travel <newsletter@statravel.co.za>**
Subject: [MARKETING] Get 20% off selected tours. See Cambodia from only R5050!
Date: April 24, 2555 BE 9:38:58 PM GMT+07:00
To: kitisak@nectec.or.th
Reply-To: newsletter@statravel.co.za
Return-Path: <v-fapofm_bncflpgeo_lnaagke_lnaagke_a@bounce.mkt293.com>
Delivered-To: kitisak@nectec.or.th
Received: (qmail 19890 invoked from network); 24 Apr 2012 14:39:03 -0000
Received: from unknown (HELO mailgateway2.nectec.or.th) ([10.226.48.170]) (envelope-sender <v-fapofm_bncflpgeo_lnaagke_lnaagke_a@bounce.mkt293.com>) by nectec.or.th (NectecNet Mail) with SMTP for <kitisak@nectec.or.th>; 24 Apr 2012 14:39:03 -0000
Received: (qmail 22183 invoked by uid 98); 24 Apr 2012 14:39:03 -0000
Received: from 203.185.132.74 by mailgateway2.nectec.or.th with Mailgateway-Engine-1.0 24 Apr 2012 14:39:03 -0000
Received: from unknown (HELO imail.nectec.or.th) (203.185.132.74) by mailgateway2.nectec.or.th with SMTP; 24 Apr 2012 14:39:03 -0000
Received: from mail1240c.mkt293.com (HELO mail1240c.links.statravel.co.uk) ([74.112.64.14]) by imail.nectec.or.th with ESMTP; 24 Apr 2012 21:39:00 +0700
Received: by mail1240c.links.statravel.co.uk (PowerMTA(TM) v3.5r16) id hiqtga0iiksm for <kitisak@nectec.or.th>; Tue, 24 Apr 2012 14:38:58 +0000 (envelope-from <v-fapofm_bncflpgeo_lnaagke_lnaagke_a@bounce.mkt293.com>)
-Spam-Filtered: true

We can see the mail route!!!!

EGA
e-Government Agency

G-CERT by EGA

IP Address

- Dotted Decimal
  - 192.168.20.59
- Binary
  - 11000000.10101000.00010100.00111011
- Decimal
  - 3232240699
- Hexadecimal
  - 0xC0.0xA8.0x14.0x3B

What can we know more about IP?

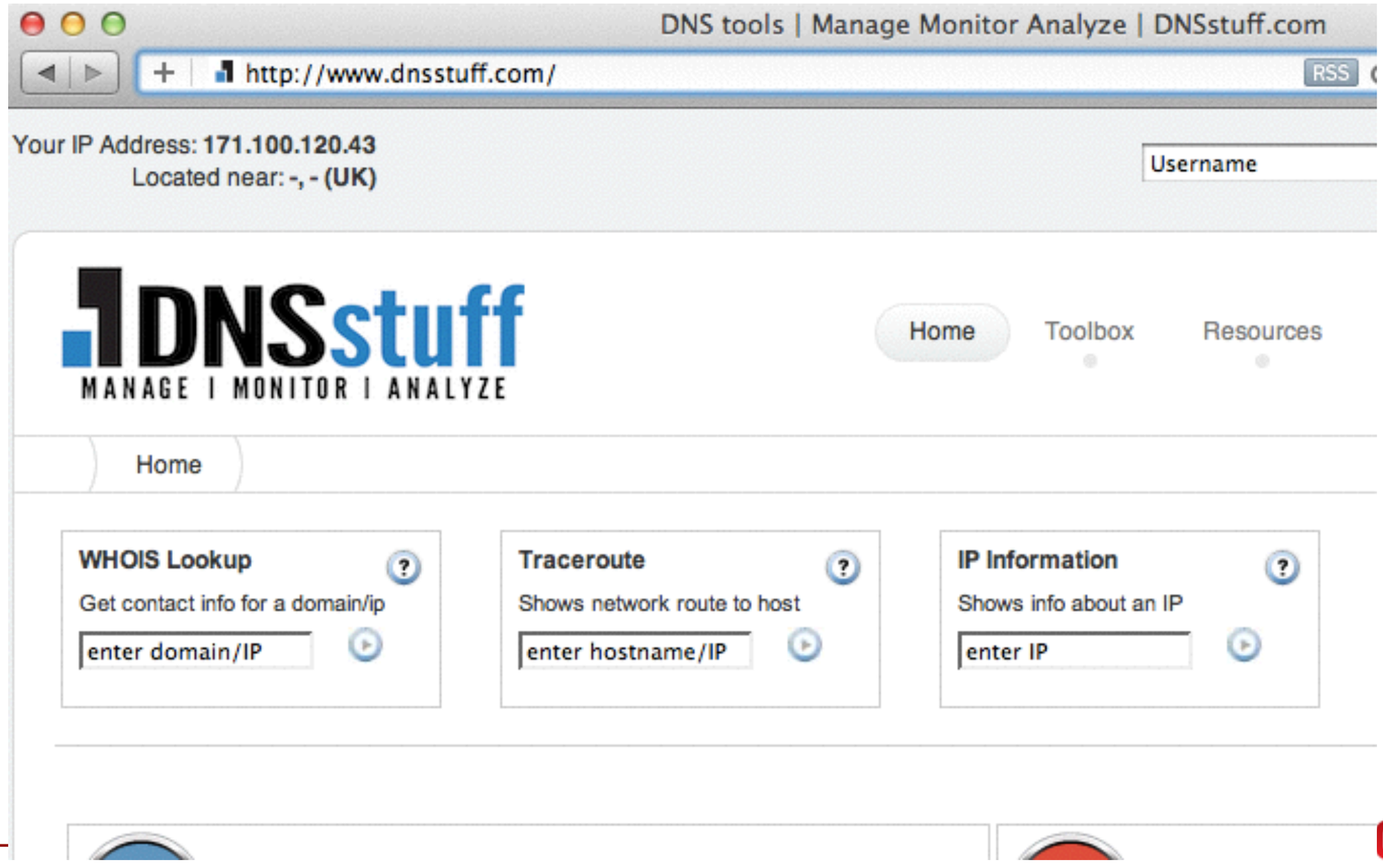
- IP Owner's name or Provider
- Contact point
  - Email address
  - Telephone number
- Route
- Active or not?
- Opened ports
- Vulnerabilities

Recommended tools

- Whois – IP address information
- Tracert/Traceroute – Determine the path to another host
- Ping – Detect if another host is reachable
- nslookup – Resolve DNS
- Dig – Utility for checking DNS resolution
- Wireshark – Network sniffer (use with cares)
- Nmap – Port scanner (use with cares)
- Nessus – Vulnerability scanner (use with cares)

Whois

- IP registration database
- http://www.dnstuff.com



Whois result

Using 0 day old cached answer (or, you can get fresh results).
Hiding E-mail address (you can get results with the E-mail address).

% [whois.apnic.net node-1]
% Whois data copyright terms http://www.apnic.net/db/dbcopyright.html

inetnum: 171.100.0.0 - 171.100.127.255
netname: TRUENET-BB
descr: TRUE BROADBAND
country: TH
admin-c: TIA6-AP
tech-c: TIA6-AP
status: ASSIGNED NON-PORTABLE
remarks: Abusing network please contact : *******@trueinternet.co.th
mnt-by: MAINT-AP-TRUEINTERNET
mnt-lower: MAINT-AP-TRUEINTERNET
mnt-routes: MAINT-AP-TRUEINTERNET
mnt-irt: IRT-TRUEINTERNET-TH
changed: *******@trueinternet.co.th 20120111
source: APNIC

Tracert / Traceroute

kitisak — bash — 95×34

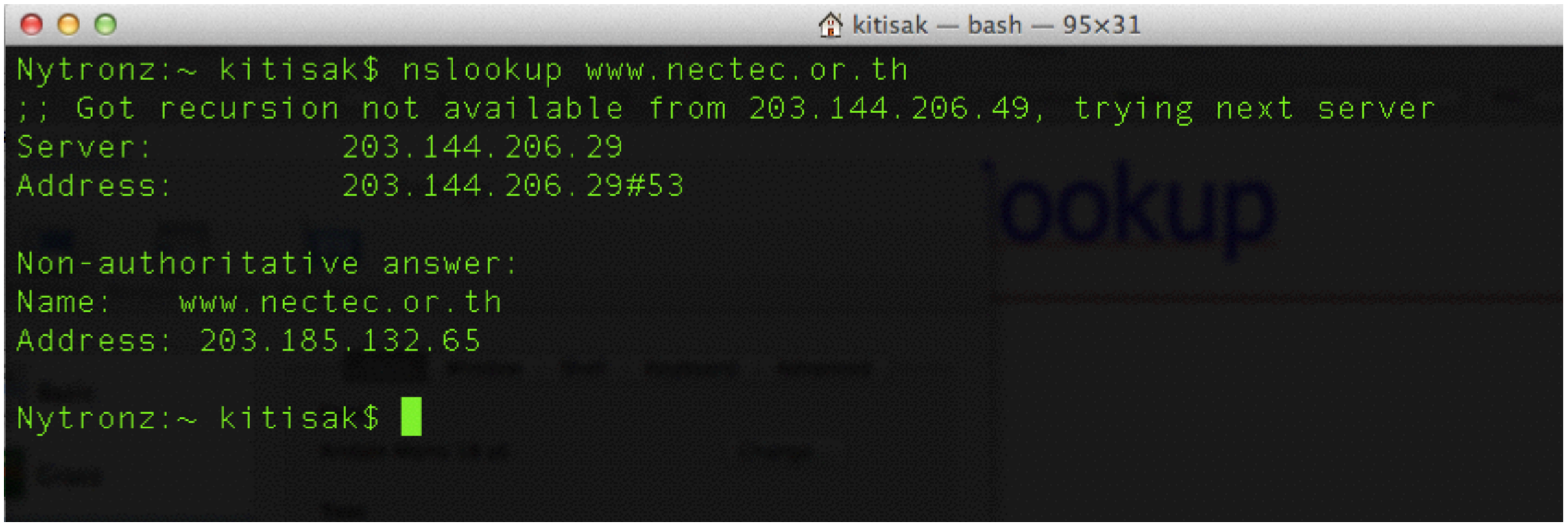
```
Nytronz:~ kitisak$ traceroute www.google.com
traceroute: Warning: www.google.com has multiple addresses; using 209.85.175.147
traceroute to www.l.google.com (209.85.175.147), 64 hops max, 52 byte packets
 1  10.23.224.1 (10.23.224.1)  9.650 ms  8.920 ms  8.236 ms
 2  10.92.229.177 (10.92.229.177)  8.528 ms  8.469 ms  11.302 ms
 3  203-144-128-26.static.asianet.co.th (203.144.128.26)  11.363 ms
    58-97-4-46.static.asianet.co.th (58.97.4.46)  12.628 ms
    203-144-128-30.static.asianet.co.th (203.144.128.30)  9.655 ms
 4  58-97-4-45.static.asianet.co.th (58.97.4.45)  10.564 ms  9.913 ms  10.182 ms
 5  203-144-193-75.static.asianet.co.th (203.144.193.75)  9.814 ms  10.288 ms  9.400 ms
 6  58-97-38-42.static.asianet.co.th (58.97.38.42)  10.555 ms  9.498 ms  8.953 ms
 7  58-97-38-41.static.asianet.co.th (58.97.38.41)  10.695 ms  9.471 ms  10.174 ms
 8  61-91-210-5.static.asianet.co.th (61.91.210.5)  10.952 ms  11.785 ms  9.631 ms
 9  tig-net28-157.trueintergateway.com (122.144.28.157)  14.734 ms  15.071 ms  11.747 ms
10  th-icr-tt1-26-129.trueintergateway.com (122.144.26.129)  14.903 ms  11.450 ms  12.408 ms
11  72.14.215.181 (72.14.215.181)  36.610 ms  37.179 ms  36.253 ms
12  209.85.242.244 (209.85.242.244)  37.336 ms
    209.85.242.236 (209.85.242.236)  39.682 ms
    209.85.242.244 (209.85.242.244)  80.278 ms
13  209.85.250.237 (209.85.250.237)  39.135 ms
    209.85.250.255 (209.85.250.255)  35.729 ms  36.069 ms
14  66.249.94.186 (66.249.94.186)  37.170 ms
    66.249.94.166 (66.249.94.166)  33.974 ms
    66.249.94.186 (66.249.94.186)  49.599 ms
15  nx-in-f147.1e100.net (209.85.175.147)  39.634 ms  36.794 ms  38.312 ms
Nytronz:~ kitisak$
```

Ping

kitisak — bash — 95×28

```
Nytronz:~ kitisak$ ping www.google.com
PING www.l.google.com (209.85.175.105): 56 data bytes
64 bytes from 209.85.175.105: icmp_seq=0 ttl=52 time=37.520 ms
64 bytes from 209.85.175.105: icmp_seq=1 ttl=52 time=40.838 ms
64 bytes from 209.85.175.105: icmp_seq=2 ttl=52 time=38.211 ms
64 bytes from 209.85.175.105: icmp_seq=3 ttl=52 time=37.954 ms
64 bytes from 209.85.175.105: icmp_seq=4 ttl=52 time=35.862 ms
^C
--- www.l.google.com ping statistics ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 35.862/38.077/40.838/1.605 ms
Nytronz:~ kitisak$
```

nslookup


kitisak — bash — 95×31
Nytronz:~ kitisak$ nslookup www.nectec.or.th
;; Got recursion not available from 203.144.206.49, trying next server
Server: 203.144.206.29
Address: 203.144.206.29#53
Non-authoritative answer:
Name: www.nectec.or.th
Address: 203.185.132.65
Nytronz:~ kitisak$

Dig

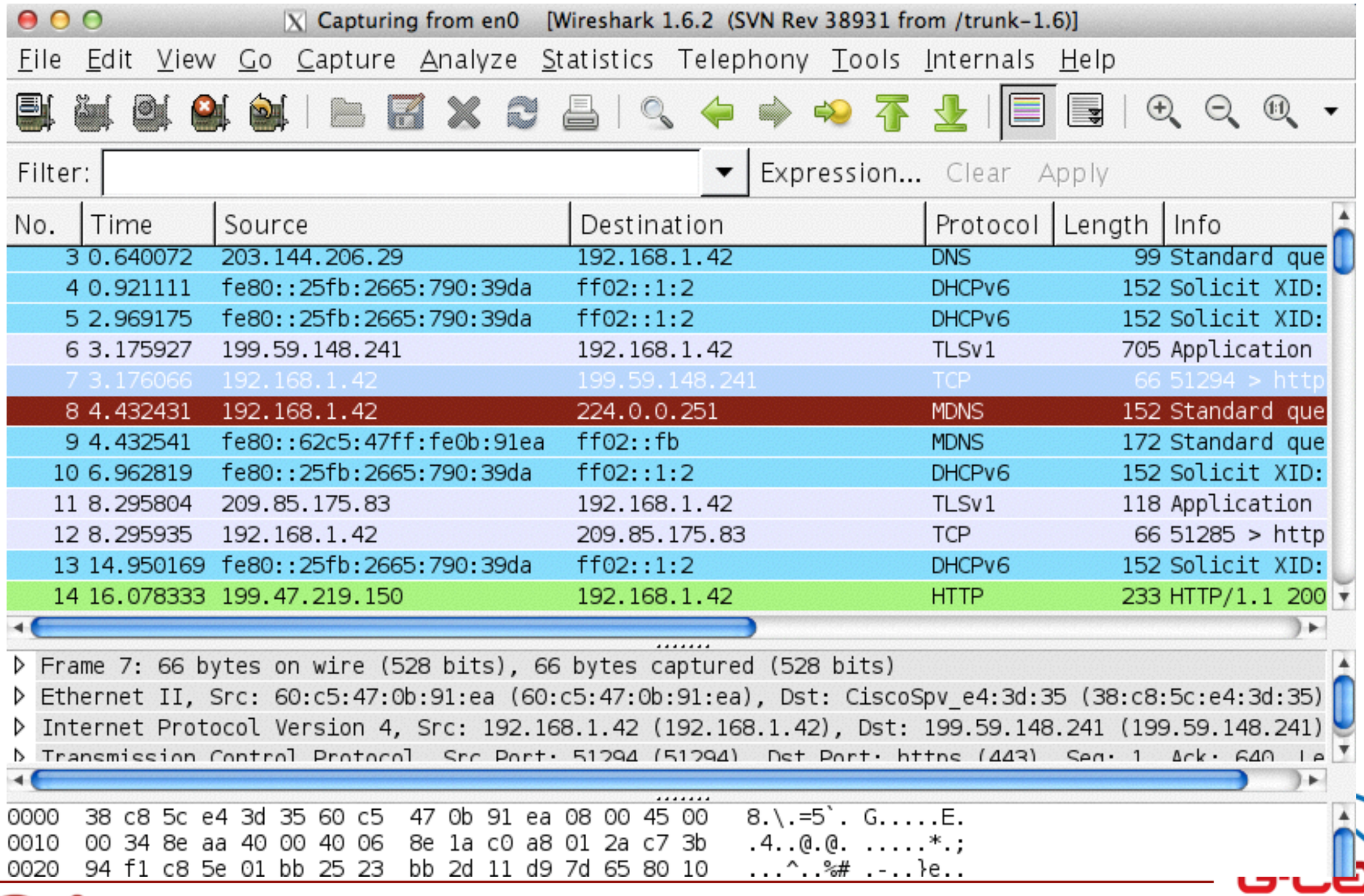
kitisak — bash — 95×28

```
Nytronz:~ kitisak$ dig www.nectec.or.th

; <<>> DiG 9.7.3-P3 <<>> www.nectec.or.th
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 31344
;; flags: qr rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;www.nectec.or.th.              IN      A

;; ANSWER SECTION:
www.nectec.or.th.       2967    IN      A       203.185.132.65

;; Query time: 10 msec
;; SERVER: 203.144.206.49#53(203.144.206.49)
;; WHEN: Wed Apr 25 05:29:39 2012
;; MSG SIZE  rcvd: 50

Nytronz:~ kitisak$
```

Wireshark

- Formerly known as “Ethereal”
- Free
- Official website :http://www.wireshark.org/
- Requirement
  - Need to install winpcap
  - (On Windows Vista) Need Administrator privilege to capture
- GUI

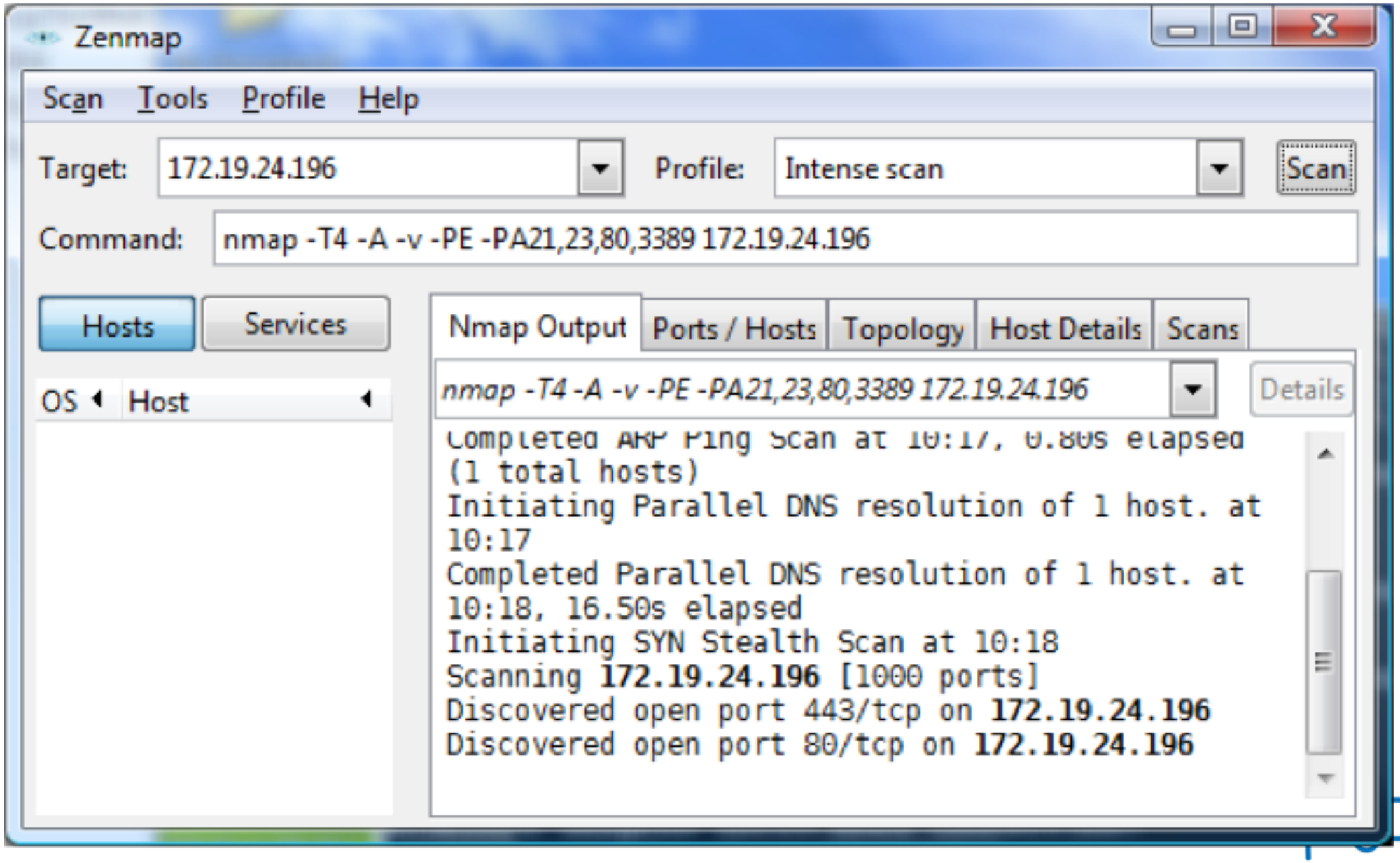
Wireshark


Capturing from en0 [Wireshark 1.6.2 (SVN Rev 38931 from /trunk-1.6)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Length Info
3 0.640072 203.144.206.29 192.168.1.42 DNS 99 Standard que
4 0.921111 fe80::25fb:2665:790:39da ff02::1:2 DHCPv6 152 Solicit XID:
5 2.969175 fe80::25fb:2665:790:39da ff02::1:2 DHCPv6 152 Solicit XID:
6 3.175927 199.59.148.241 192.168.1.42 TLSv1 705 Application
7 3.176066 192.168.1.42 199.59.148.241 TCP 66 51294 > http
8 4.432431 192.168.1.42 224.0.0.251 MDNS 152 Standard que
9 4.432541 fe80::62c5:47ff:fe0b:91ea ff02::fb MDNS 172 Standard que
10 6.962819 fe80::25fb:2665:790:39da ff02::1:2 DHCPv6 152 Solicit XID:
11 8.295804 209.85.175.83 192.168.1.42 TLSv1 118 Application
12 8.295935 192.168.1.42 209.85.175.83 TCP 66 51285 > http
13 14.950169 fe80::25fb:2665:790:39da ff02::1:2 DHCPv6 152 Solicit XID:
14 16.078333 199.47.219.150 192.168.1.42 HTTP 233 HTTP/1.1 200
Frame 7: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
Ethernet II, Src: 60:c5:47:0b:91:ea (60:c5:47:0b:91:ea), Dst: CiscoSpv_e4:3d:35 (38:c8:5c:e4:3d:35)
Internet Protocol Version 4, Src: 192.168.1.42 (192.168.1.42), Dst: 199.59.148.241 (199.59.148.241)
0000 38 c8 5c e4 3d 35 60 c5 47 0b 91 ea 08 00 45 00 8.\.=5`. G.....E.
0010 00 34 8e aa 40 00 40 06 8e 1a c0 a8 01 2a c7 3b .4..@.@. .....*.;
0020 94 f1 c8 5e 01 bb 25 23 bb 2d 11 d9 7d 65 80 10 ...^..%# .-..}e..

Nmap

- Port scanning tools
- Both GUI and Command line
- Free download at http://www.nmap.org
- Compatible with Windows, Linux and MacOS
- Last version is 5.6x

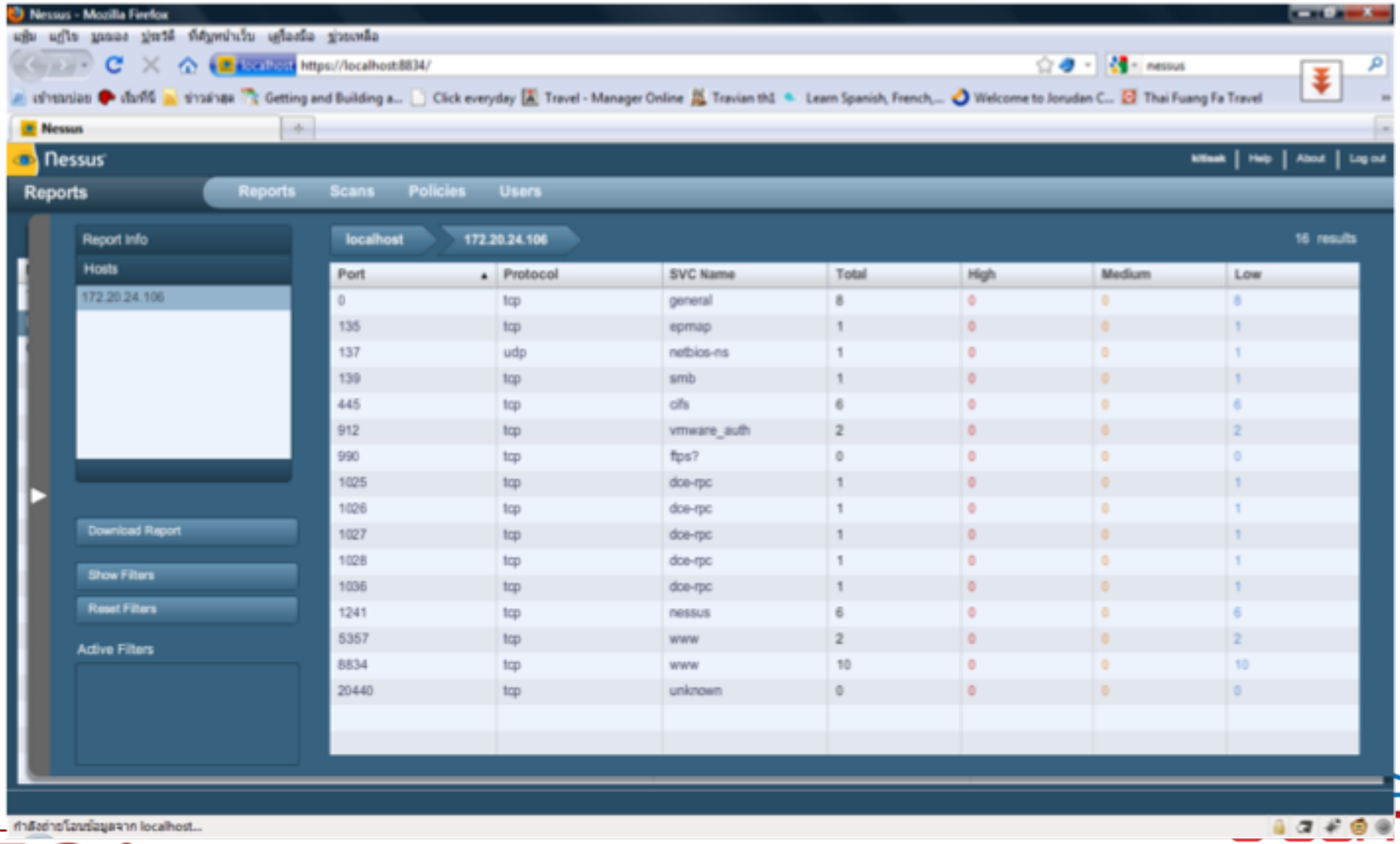
Nmap (Windows)



Nessus

- Free download at http://www.nessus.org
- Vulnerabilities Scanner
- Last version is 5
- Compatible with both Linux and Windows
- 2 Softwares
  - Nessus Server
  - Nessus Client

Nessus


Nessus - Mozilla Firefox
https://localhost:8834/
Nessus
Reports
Reports
Scans
Policies
Users
Report Info
Hosts
172.20.24.106
Download Report
Show Filters
Reset Filters
Active Filters
localhost
172.20.24.106
16 results
Port
Protocol
SVC Name
Total
High
Medium
Low
0 tcp general 8 0 0 8
135 tcp epmap 1 0 0 1
137 udp netbios-ns 1 0 0 1
139 tcp smb 1 0 0 1
445 tcp cifs 6 0 0 6
912 tcp vmware_auth 2 0 0 2
990 tcp ftps? 0 0 0 0
1025 tcp dce-rpc 1 0 0 1
1026 tcp dce-rpc 1 0 0 1
1027 tcp dce-rpc 1 0 0 1
1028 tcp dce-rpc 1 0 0 1
1036 tcp dce-rpc 1 0 0 1
1241 tcp nessus 6 0 0 6
5357 tcp www 2 0 0 2
8834 tcp www 10 0 0 10
20440 tcp unknown 0 0 0 0

Overview Scenarios

- 3 Tasks (2 incident cases and 1 report)
- Cases
  - Spam mail
  - Hack

Tools

- Mail server
- Web server
- Wifi (intranet)

Task 1

Task 1

- Investigate mail header
- Find the sender
- Inform EGA Contact Center to contact the attacker

- contact@ega.or.th

- Remind: mail.server1.go.th is the mailer engine

Task 2

Task 2

- We will receive the case from EGA Contact Center
- Investigate our web server
- Find the Message ID in the server (to prove)
- Find the attacker ’s IP and how to hack
- Find the solutions
- Report back to EGA Contact Center (G-CERT)

Task 3

Task 3

- Make some presentations about cases
  - Who are your attackers? (both cases)
  - How do the attackers attack?
  - What will you do to fix and prevent?
  - Feedback about the scenarios
- Share your feedback about this event
- Present tomorrow