Security Assessment & Monitoring

Girindro Pringgo Digdo

Whoami

- Seven years in Information Security
- Lecturer
- Author

Agenda

- Why do you need security monitoring?
- Sources of Security Holes
- System Security Tester
- Probing Services
- Network Monitoring

Why do you need a security monitoring?

- Found a new security hole
    - Hardware and software usually have a complicated things. Thus, a security hole raised by mistaken implementation.
- Configuration Error
    - Configuration is not right so that give rise to security hole.
    - Administrator forgot or lack of knowledge
    - Permission mode of password file (/etc/passwd/) inadvertently changed so that it could be changed or modified by unauthorized persons.

Why do you need a security monitoring?

- Adding new components (hardware or software)
  - It lead to decrease the security level or changed the method to operate the system.
  - Operator or Administrator had to learn again.
  - In the learning period, many problems that occur.
  - Server or software is still using default configuration from vendor

A sources of security holes

- Design flaw
  - Security holes caused by wrong design is generally rare.
  - But if it happens to be very difficult to repair.
  - Due to incorrect design, so even though it is implemented properly, the weaknesses of the system will remain.
  - ROT13 encryption algorithm or a Caesar Cipher, where the character is shifted 13 letters or three letters. Although implemented with meticulous programming, anyone who knows the encryption algorithm can solve.

A sources of security holes

- Incorrect of implementation
  - Many programs are implemented in a hurry so that less careful in coding. As a result, checks or testing should be done but being not done.
  - Filtering malicious character for input form.
  - HTML script so that the apps can access files or confidential information.
- Incorrect of configuration
  - Files that should not be changed by the user inadvertently become a "writeable"

A sources of security holes

- Incorrect of use
    - Mistake of using a program that is run by using the root account (super user/administrator) can be fatal.
    - The new administrator careless in running the command "rm-rf" in the system UNIX (which delete files or directories and sub-directories in it).

System security tester

- Because of the many things that have to be monitored, the administrator of the information system requires automated tools.
- The auto attendant, which can help to test or evaluate the safety of the system being managed.

System security tester

- For UNIX-based systems there are several tools that can be used:
    - Tripwire
    - SAINT
    - COPS
    - ?

Probing Services

- Internet service is generally done using TCP or UDP protocol. Every service is executed by using a different port, for example:
    - HTTP; TCP port 80
    - FTP; TCP port 21
    - ?

Probing Services

- Selection of what services depend on the need and the level of security desired.

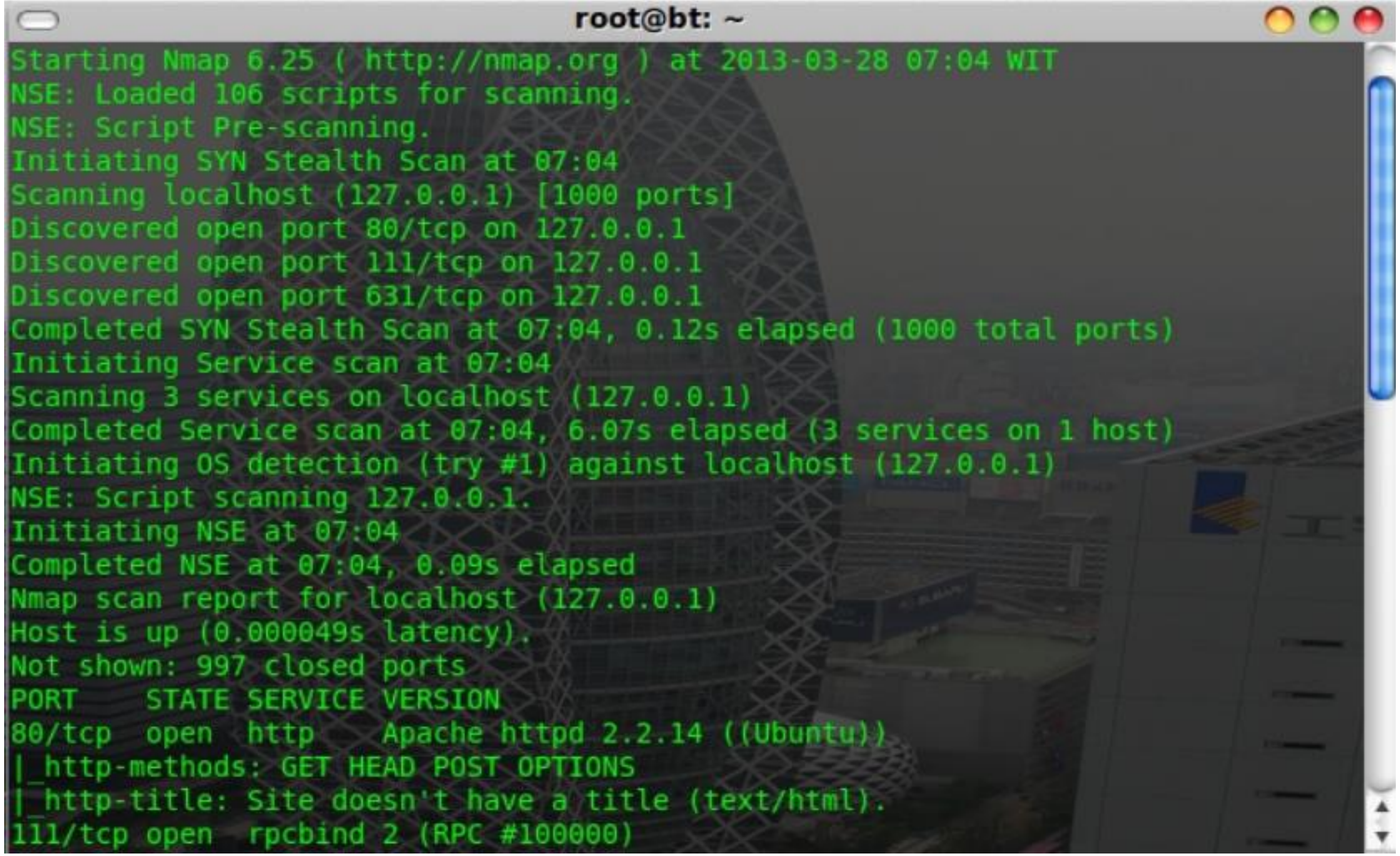
- Often purchased or assembled systems running several major services as "default". Sometimes some of the services to be switched off because there is likely to be exploited by attackers.

Probing Services

- There are several tools that can be used to perform a "probe" (feeling) what services are available.

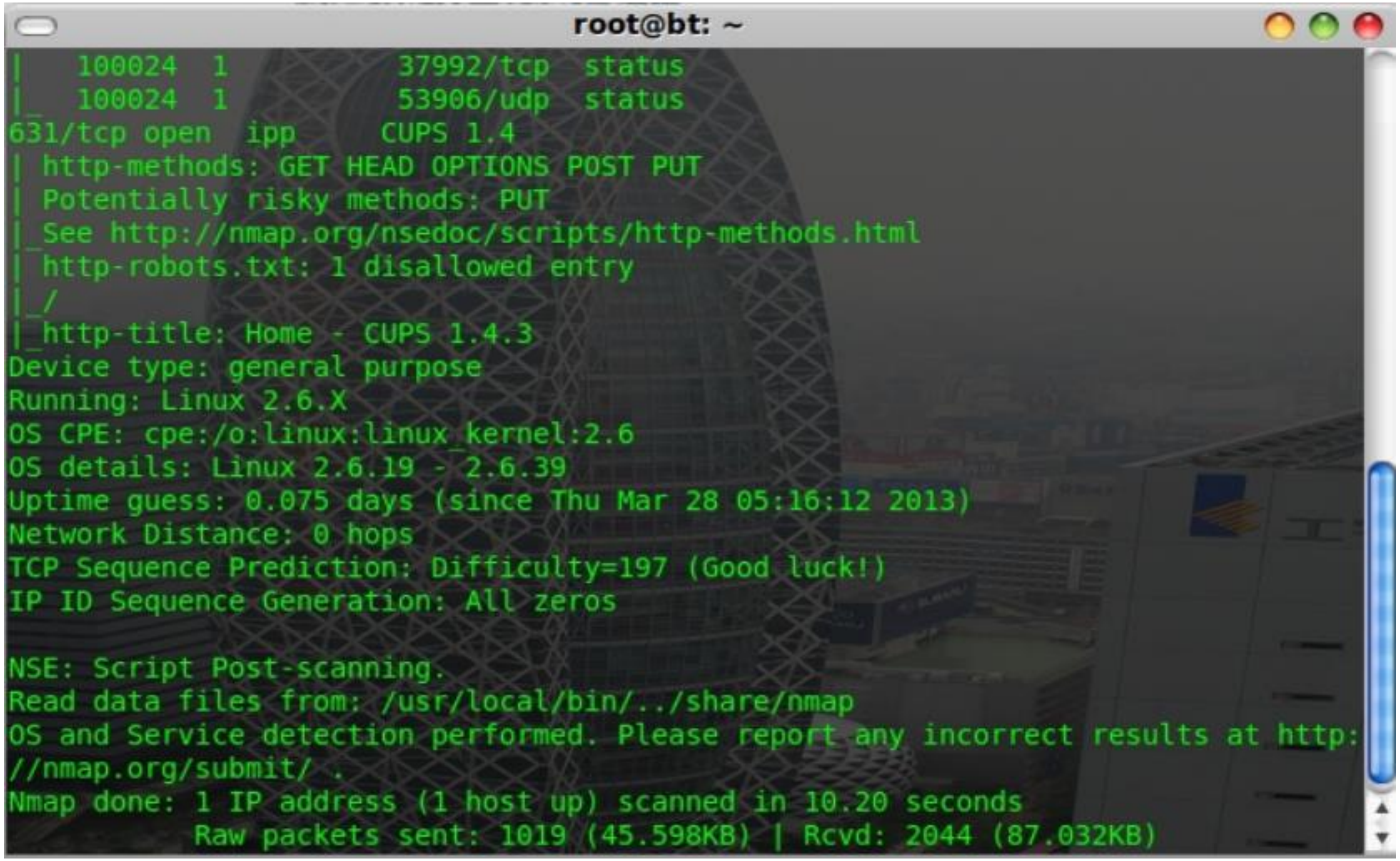
- The program can also be used by criminals to see what services are available in the system to be attacked and based on the data obtained can launch an attack.

Probing Services



```
Starting Nmap 6.25 ( http://nmap.org ) at 2013-03-28 07:04 WIT
NSE: Loaded 106 scripts for scanning.
NSE: Script Pre-scanning.
Initiating SYN Stealth Scan at 07:04
Scanning localhost (127.0.0.1) [1000 ports]
Discovered open port 80/tcp on 127.0.0.1
Discovered open port 111/tcp on 127.0.0.1
Discovered open port 631/tcp on 127.0.0.1
Completed SYN Stealth Scan at 07:04, 0.12s elapsed (1000 total ports)
Initiating Service scan at 07:04
Scanning 3 services on localhost (127.0.0.1)
Completed Service scan at 07:04, 6.07s elapsed (3 services on 1 host)
Initiating OS detection (try #1) against localhost (127.0.0.1)
NSE: Script scanning 127.0.0.1.
Initiating NSE at 07:04
Completed NSE at 07:04, 0.09s elapsed
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000049s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE VERSION
80/tcp  open  http    Apache httpd 2.2.14 ((Ubuntu))
|_http-methods: GET HEAD POST OPTIONS
|_http-title: Site doesn't have a title (text/html).
111/tcp open  rpcbind 2 (RPC #100000)
```

Probing Services



```
|   100024  1          37992/tcp  status
|_  100024  1          53906/udp  status
631/tcp open  ipp     CUPS 1.4
| http-methods: GET HEAD OPTIONS POST PUT
| Potentially risky methods: PUT
|_See http://nmap.org/nsedoc/scripts/http-methods.html
| http-robots.txt: 1 disallowed entry
|_/
|_http-title: Home - CUPS 1.4.3
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.19 - 2.6.39
Uptime guess: 0.075 days (since Thu Mar 28 05:16:12 2013)
Network Distance: 0 hops
TCP Sequence Prediction: Difficulty=197 (Good luck!)
IP ID Sequence Generation: All zeros

NSE: Script Post-scanning.
Read data files from: /usr/local/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at http:
//nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.20 seconds
           Raw packets sent: 1019 (45.598KB) | Rcvd: 2044 (87.032KB)
```

Probing Services

- Nmap
- Strobe
- Tcpprobe

Using of program

- One of way to identify the weaknesses of your information system is to attack yourself.

- Do not use these programs to attack other systems (systems that you do not manage).

Two types of program

- Active

  Programs that are aggressive of attack and paralyze the target system.

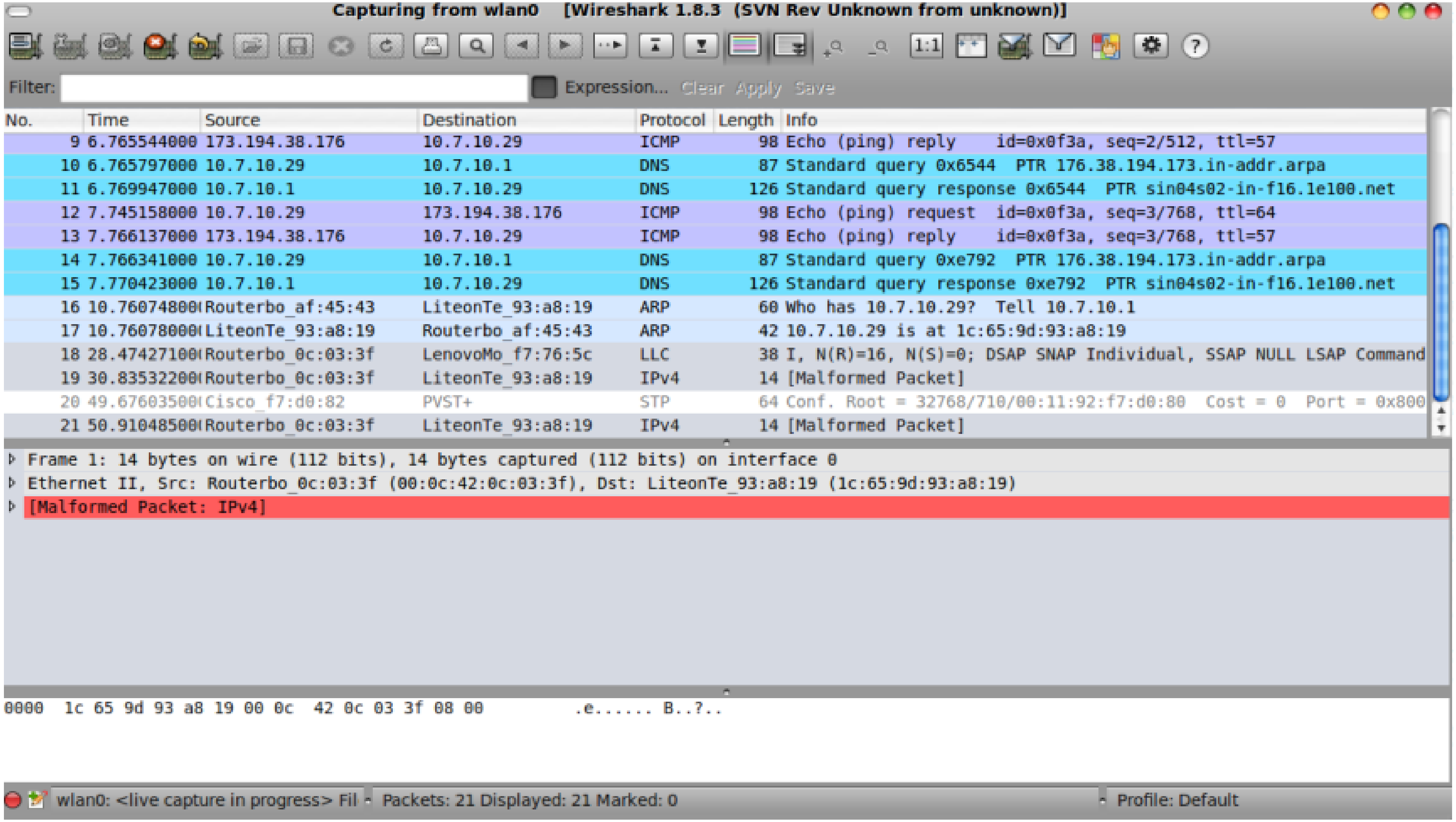
- Passive

  Programs that are nature of theft or interception of data.

Example

- Pcapture
- Tcpdump
- Wireshark

Example



Capturing from wlan0   [Wireshark 1.8.3 (SVN Rev Unknown from unknown)]

```
No.   Time         Source              Destination        Protocol Length Info
    9 6.765544000 173.194.38.176      10.7.10.29         ICMP        98 Echo (ping) reply    id=0x0f3a, seq=2/512, ttl=57
   10 6.765797000 10.7.10.29          10.7.10.1          DNS         87 Standard query 0x6544  PTR 176.38.194.173.in-addr.arpa
   11 6.769947000 10.7.10.1           10.7.10.29         DNS        126 Standard query response 0x6544  PTR sin04s02-in-f16.1e100.net
   12 7.745158000 10.7.10.29          173.194.38.176     ICMP        98 Echo (ping) request  id=0x0f3a, seq=3/768, ttl=64
   13 7.766137000 173.194.38.176      10.7.10.29         ICMP        98 Echo (ping) reply    id=0x0f3a, seq=3/768, ttl=57
   14 7.766341000 10.7.10.29          10.7.10.1          DNS         87 Standard query 0xe792  PTR 176.38.194.173.in-addr.arpa
   15 7.770423000 10.7.10.1           10.7.10.29         DNS        126 Standard query response 0xe792  PTR sin04s02-in-f16.1e100.net
   16 10.76074800 Routerbo_af:45:43   LiteonTe_93:a8:19  ARP         60 Who has 10.7.10.29?  Tell 10.7.10.1
   17 10.76078000 LiteonTe_93:a8:19   Routerbo_af:45:43  ARP         42 10.7.10.29 is at 1c:65:9d:93:a8:19
   18 28.47427100 Routerbo_0c:03:3f   LenovoMo_f7:76:5c  LLC         38 I, N(R)=16, N(S)=0; DSAP SNAP Individual, SSAP NULL LSAP Command
   19 30.83532200 Routerbo_0c:03:3f   LiteonTe_93:a8:19  IPv4        14 [Malformed Packet]
   20 49.67603500 Cisco_f7:d0:82      PVST+              STP         64 Conf. Root = 32768/710/00:11:92:f7:d0:80  Cost = 0  Port = 0x800
   21 50.91048500 Routerbo_0c:03:3f   LiteonTe_93:a8:19  IPv4        14 [Malformed Packet]
```

```
▷ Frame 1: 14 bytes on wire (112 bits), 14 bytes captured (112 bits) on interface 0
▷ Ethernet II, Src: Routerbo_0c:03:3f (00:0c:42:0c:03:3f), Dst: LiteonTe_93:a8:19 (1c:65:9d:93:a8:19)
▷ [Malformed Packet: IPv4]
```

```
0000  1c 65 9d 93 a8 19 00 0c  42 0c 03 3f 08 00         .e...... B..?..
```

wlan0: <live capture in progress> Fil   Packets: 21 Displayed: 21 Marked: 0   Profile: Default

Network Monitoring

- Network monitoring system (network monitoring) can be used to detect security holes.

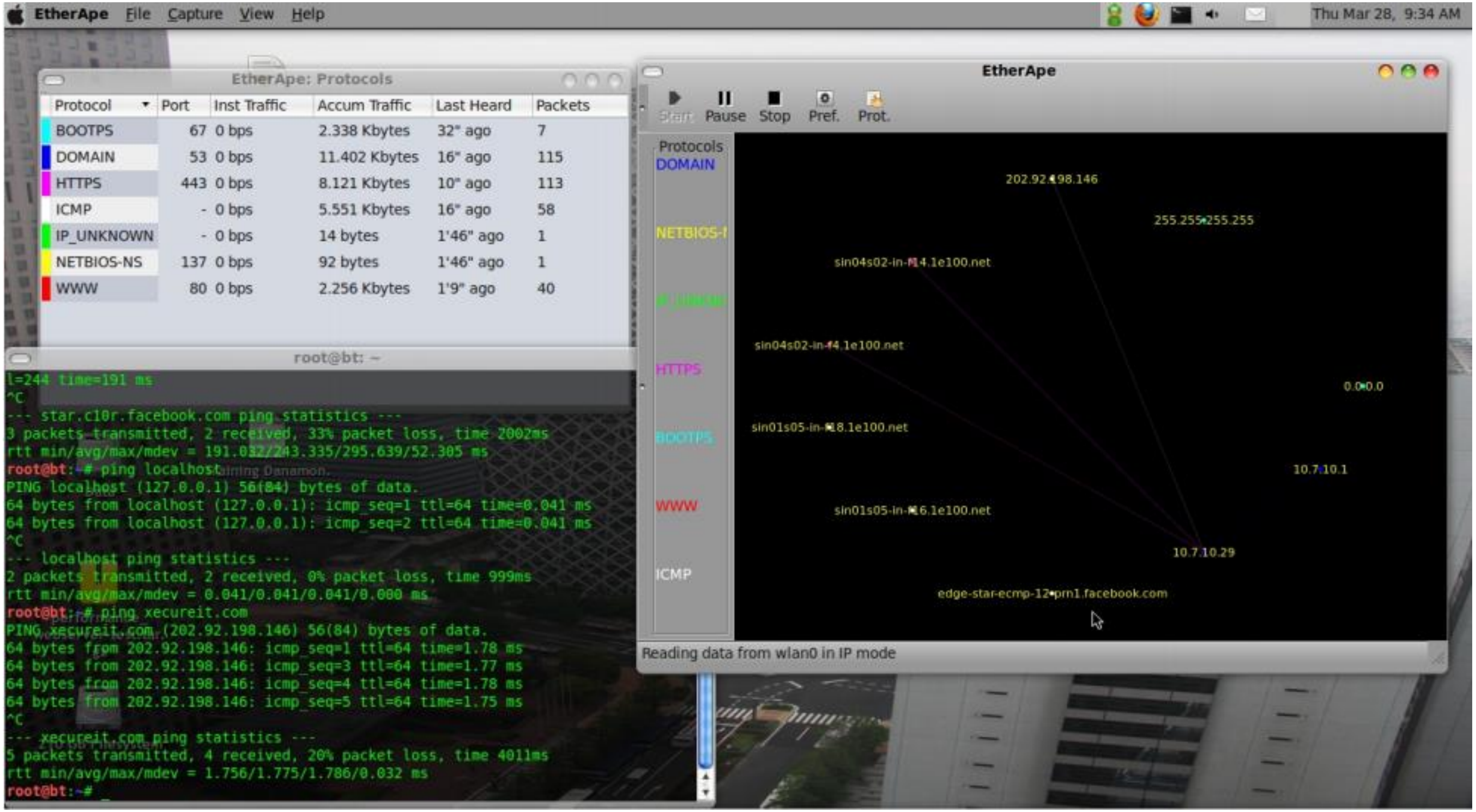
- By monitoring network can also be seen in efforts to cripple the system through denial of service attack (DoS) by sending packets excessive amount.

- Network monitoring is usually done using protocol SNMP (Simple Network Management Protocol).

Network Monitoring

- Etherboy (Windows), Etherape (Unix)
- HP Openview (Windows)
- Packetboy (Windows), Packetman (Unix)
- SNMP Collector (Windows)
- Webboy (Windows)

Network Monitoring



Protocol	Port	Inst Traffic	Accum Traffic	Last Heard	Packets
🟦 BOOTPS	67	0 bps	2.338 Kbytes	32" ago	7
🟦 DOMAIN	53	0 bps	11.402 Kbytes	16" ago	115
🟪 HTTPS	443	0 bps	8.121 Kbytes	10" ago	113
⬜ ICMP	-	0 bps	5.551 Kbytes	16" ago	58
🟩 IP_UNKNOWN	-	0 bps	14 bytes	1'46" ago	1
🟨 NETBIOS-NS	137	0 bps	92 bytes	1'46" ago	1
🟥 WWW	80	0 bps	2.256 Kbytes	1'9" ago	40

```
l=244 time=191 ms
^C
--- star.c10r.facebook.com ping statistics ---
3 packets transmitted, 2 received, 33% packet loss, time 2002ms
rtt min/avg/max/mdev = 191.032/243.335/295.639/52.305 ms
root@bt:~# ping localhost
PING localhost (127.0.0.1) 56(84) bytes of data.
64 bytes from localhost (127.0.0.1): icmp_seq=1 ttl=64 time=0.041 ms
64 bytes from localhost (127.0.0.1): icmp_seq=2 ttl=64 time=0.041 ms
^C
--- localhost ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.041/0.041/0.041/0.000 ms
root@bt:~# ping xecureit.com
PING xecureit.com (202.92.198.146) 56(84) bytes of data.
64 bytes from 202.92.198.146: icmp_seq=1 ttl=64 time=1.78 ms
64 bytes from 202.92.198.146: icmp_seq=3 ttl=64 time=1.77 ms
64 bytes from 202.92.198.146: icmp_seq=4 ttl=64 time=1.78 ms
64 bytes from 202.92.198.146: icmp_seq=5 ttl=64 time=1.75 ms
^C
--- xecureit.com ping statistics ---
5 packets transmitted, 4 received, 20% packet loss, time 4011ms
rtt min/avg/max/mdev = 1.756/1.775/1.786/0.032 ms
root@bt:~#
```

Reading data from wlan0 in IP mode