TUGAS KEAMANAN JARINGAN KOMPUTER

NAMA: SYAMSUDIN
NIM: 09011281320012

UNIVERSITAS SRIWIJAYA
FAKULTAS ILMU KOMPUTER
JURUSAN SISTEM KOMPUTER

Target

- PT. PUSRI
- URL: http://pusri.co.id
- IP Address: 222.124.4.120

Tools

- Nmap
- Xprobe
- Netcat
- Nessus
- Wireshark
- Snort

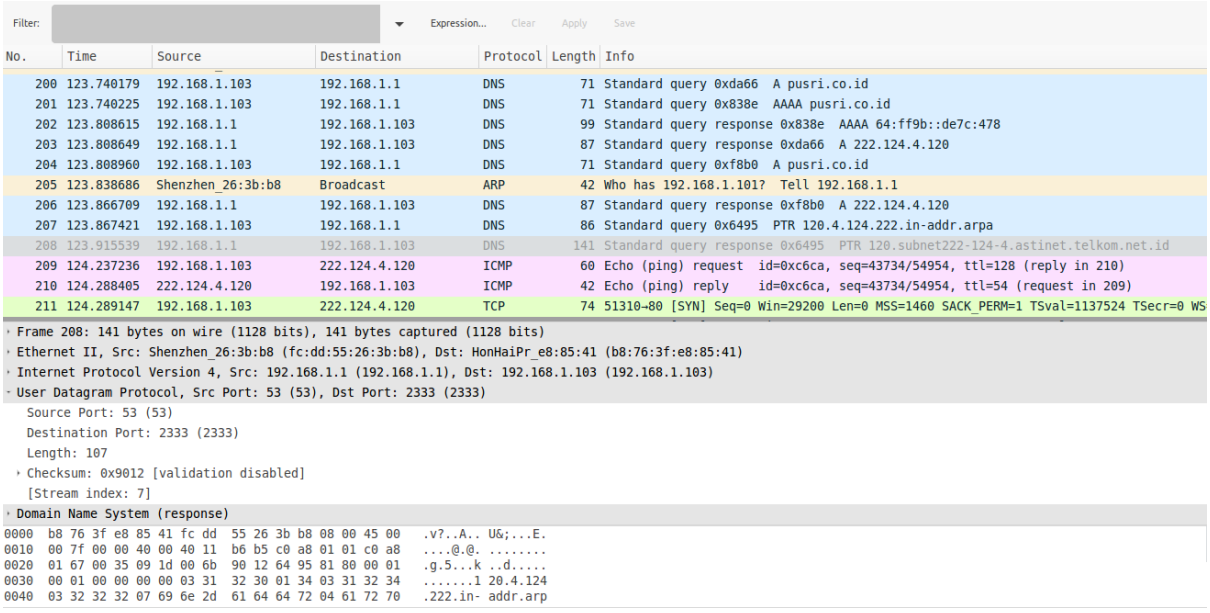
Time

- Percobaan ini dilakukan selama 48 menit 45 detik.

Step

1. Capture packet menggunakan Wireshark

Langkah pertama yang dilakukan yaitu capture packet menggunakan tools Wireshark.



2. Scanning menggunakan Nmap

Langkah kedua yang dilakukan yaitu network scanning menggunakan tools Nmap.

```
sam@sam-SVE14131CVW:~$ nmap pusri.co.id

Starting Nmap 6.47 ( http://nmap.org ) at 2017-02-22 19:32 WIB
Nmap scan report for pusri.co.id (222.124.4.120)
Host is up (0.056s latency).
rDNS record for 222.124.4.120: 120.subnet222-124-4.astinet.telkom.net.id
Not shown: 996 closed ports
PORT   STATE    SERVICE
22/tcp open     ssh
25/tcp filtered smtp
53/tcp filtered domain
80/tcp open     http

Nmap done: 1 IP address (1 host up) scanned in 5.05 seconds
```

3. Scanning menggunakan Xprobe

Langkah ketiga yang dilakukan yaitu network scanning menggunakan tools Xprobe.

```
root@sam-SVE14131CVW:/home/sam# xprobe2 222.124.4.120

Xprobe2 v.0.3 Copyright (c) 2002-2005 fyodor@o0o.nu, ofir@sys-security.com, meder@o0o.nu

[+] Target is 222.124.4.120
[+] Loading modules.
[+] Following modules are loaded:
[x] [1] ping:icmp_ping  -  ICMP echo discovery module
[x] [2] ping:tcp_ping  -  TCP-based ping discovery module
[x] [3] ping:udp_ping  -  UDP-based ping discovery module
[x] [4] infogather:ttl_calc  -  TCP and UDP based TTL distance calculation
[x] [5] infogather:portscan  -  TCP and UDP PortScanner
[x] [6] fingerprint:icmp_echo  -  ICMP Echo request fingerprinting module
[x] [7] fingerprint:icmp_tstamp  -  ICMP Timestamp request fingerprinting module
[x] [8] fingerprint:icmp_amask  -  ICMP Address mask request fingerprinting module
[x] [9] fingerprint:icmp_port_unreach  -  ICMP port unreachable fingerprinting module
[x] [10] fingerprint:tcp_hshake  -  TCP Handshake fingerprinting module
[x] [11] fingerprint:tcp_rst  -  TCP RST fingerprinting module
[x] [12] fingerprint:smb  -  SMB fingerprinting module
[x] [13] fingerprint:snmp  -  SNMPv2c fingerprinting module
[+] 13 modules registered
[+] Initializing scan engine
[+] Running scan engine
[-] ping:tcp_ping module: no closed/open TCP ports known on 222.124.4.120. Module test failed
[-] ping:udp_ping module: no closed/open UDP ports known on 222.124.4.120. Module test failed
[-] No distance calculation. 222.124.4.120 appears to be dead or no ports known
[+] Host: 222.124.4.120 is up (Guess probability: 50%)
[+] Target: 222.124.4.120 is alive. Round-Trip Time: 0.47535 sec
[+] Selected safe Round-Trip Time value is: 0.95069 sec
[-] fingerprint:tcp_hshake Module execution aborted (no open TCP ports known)
[-] fingerprint:smb need either TCP port 139 or 445 to run
[-] fingerprint:snmp: need UDP port 161 open
[+] Primary guess:
[+] Host 222.124.4.120 Running OS: "FreeBSD 4.9" (Guess probability: 100%)
[+] Other guesses:
[+] Host 222.124.4.120 Running OS: "Linux Kernel 2.6.0" (Guess probability: 100%)
[+] Host 222.124.4.120 Running OS: "Linux Kernel 2.4.29" (Guess probability: 100%)
[+] Host 222.124.4.120 Running OS: "Linux Kernel 2.4.19" (Guess probability: 100%)
[+] Host 222.124.4.120 Running OS: "Linux Kernel 2.4.20" (Guess probability: 100%)
[+] Host 222.124.4.120 Running OS: "Linux Kernel 2.4.21" (Guess probability: 100%)
[+] Host 222.124.4.120 Running OS: "Linux Kernel 2.4.22" (Guess probability: 100%)
```

```
[+] Host 222.124.4.120 Running OS: "FreeBSD 5.4" (Guess probability: 100%)
[+] Host 222.124.4.120 Running OS: "FreeBSD 5.3" (Guess probability: 100%)
[+] Host 222.124.4.120 Running OS: "FreeBSD 5.2.1" (Guess probability: 100%)
[+] Cleaning up scan engine
[+] Modules deinitialized
[+] Execution completed.
root@sam-SVE14131CVW:/home/sam# nmap -SV -p 22 pusri.co.id
Failed to resolve/decode supposed IPv4 source address "V": Name or service not known
QUITTING!
root@sam-SVE14131CVW:/home/sam# nmap -sV -p 22 pusri.co.id

Starting Nmap 6.47 ( http://nmap.org ) at 2017-03-06 21:15 WIB
Nmap scan report for pusri.co.id (222.124.4.120)
Host is up (0.056s latency).
rDNS record for 222.124.4.120: 120.subnet222-124-4.astinet.telkom.net.id
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 5.5p1 Debian 6+squeeze5 (protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.51 seconds
^[[B^[[Broot@sam-SVE14131CVW:/home/sam# nmap -sV -p 80 pusri.co.id

Starting Nmap 6.47 ( http://nmap.org ) at 2017-03-06 21:15 WIB
Stats: 0:00:00 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
Ping Scan Timing: About 100.00% done; ETC: 21:15 (0:00:00 remaining)
Nmap scan report for pusri.co.id (222.124.4.120)
Host is up (0.064s latency).
rDNS record for 222.124.4.120: 120.subnet222-124-4.astinet.telkom.net.id
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.2.16 ((Debian))

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.54 seconds
root@sam-SVE14131CVW:/home/sam# nmap -sV -p 21 pusri.co.id
```

4. Scanning menggunakan Netcat

Langkah keempat yang dilakukan yaitu port scanning menggunkan tools Netcat.

```
root@sam-SVE14131CVW:/home/sam# netcat -z -n -v 222.124.4.120 1-1000 2>&1 | grep succeeded
Connection to 222.124.4.120 22 port [tcp/*] succeeded!
Connection to 222.124.4.120 80 port [tcp/*] succeeded!
```

5. Scanning menggunakan Nessus

Langkah kelima yang dilakukan yaitu scanning vulnerability menggunkan tools Nessus.

Hosts > pusri.co.id > Vulnerabilities 46

Severity	Plugin Name	Plugin Family	Count
CRITICAL	Unix Operating System Unsupported Version Detection	General	1
MEDIUM	Apache mod_status /server-status Information Disclosure	Web Servers	1
MEDIUM	SSH Weak Algorithms Supported	Misc.	1
MEDIUM	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)	General	1
MEDIUM	SSL Certificate Cannot Be Trusted	General	1
MEDIUM	SSL Certificate Signed Using Weak Hashing Algorithm	General	1
MEDIUM	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)	Misc.	1
MEDIUM	SSL Medium Strength Cipher Suites Supported	General	1
MEDIUM	SSL Self-Signed Certificate	General	1
MEDIUM	SSL Version 2 and 3 Protocol Detection	Service detection	1
MEDIUM	SSL Weak Cipher Suites Supported	General	1
MEDIUM	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)	General	1
MEDIUM	Transport Layer Security (TLS) Protocol CRIME Vulnerability	General	1
LOW	SSH Server CBC Mode Ciphers Enabled	Misc.	1
LOW	SSH Weak MAC Algorithms Enabled	Misc.	1
LOW	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits	General	1
LOW	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	General	1
INFO	Nessus SYN scanner	Port scanners	3
INFO	Service Detection	Service detection	3
INFO	HTTP Server Type and Version	Web Servers	2
INFO	Apache Banner Linux Distribution Disclosure	Web Servers	1
INFO	Backported Security Patch Detection (PHP)	Web Servers	1
INFO	Backported Security Patch Detection (SSH)	General	1
INFO	Backported Security Patch Detection (WWW)	General	1
INFO	Common Platform Enumeration (CPE)	General	1
INFO	Device Type	General	1
INFO	Host Fully Qualified Domain Name (FQDN) Resolution	General	1
INFO	HyperText Transfer Protocol (HTTP) Information	Web Servers	1
INFO	ICMP Timestamp Request Remote Date Disclosure	General	1
INFO	Nessus Scan Information	Settings	1
INFO	OS Identification	General	1
INFO	PHP Version	Web Servers	1
INFO	SSH Algorithms and Languages Supported	Misc.	1
INFO	SSH Protocol Versions Supported	General	1

☐	INFO	SSH Server Type and Version Information	Service detection	1
☐	INFO	SSL / TLS Versions Supported	General	1
☐	INFO	SSL Certificate Information	General	1
☐	INFO	SSL Cipher Block Chaining Cipher Suites Supported	General	1
☐	INFO	SSL Cipher Suites Supported	General	1
☐	INFO	SSL Compression Methods Supported	General	1
☐	INFO	SSL Root Certification Authority Certificate Information	General	1
☐	INFO	TCP/IP Timestamps Supported	General	1
☐	INFO	Traceroute Information	General	1
☐	INFO	Web Server No 404 Error Code Check	Web Servers	1
☐	INFO	Web Server SSL Port HTTP Traffic Detection	Web Servers	1
☐	INFO	Webmin Detection	CGI abuses	1

6. Compile capture packet menggunakan Snort

Langkah keenam yang dilakukan yaitu mengcompile hasil dari capture packet Wireshark menggunakan tools snort.

```
root@sam-SVE14131CVW:/home/sam# snort -A fast -c /etc/snort/snort.conf -r capture_pusri_1.pcap
                                               !
                                               !
                                               !
+-------------------------------------------------------------------
[ Number of patterns truncated to 20 bytes: 1039 ]
pcap DAQ configured to read-file.
Acquiring network traffic from "capture_pusri_1.pcap".
Reload thread starting...
Reload thread started, thread 0x7fc05b167700 (1917)
WARNING: active responses disabled since DAQ can't inject packets.

        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.7.0 GRE (Build 149)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using libpcap version 1.6.2
           Using PCRE version: 8.35 2014-04-04
           Using ZLIB version: 1.2.8

           Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 2.4  <Build 1>
           Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
           Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
           Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
           Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
           Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
           Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
           Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
           Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
           Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
           Preprocessor Object: SF_POP  Version 1.0  <Build 1>
           Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
           Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
           Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
           Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
Commencing packet processing (pid=1908)
================================================================================
```

```
                 Filtered: 0
                Inspected: 0
                  Tracked: 744
===============================================================================
HTTP Inspect - encodings (Note: stream-reassembled packets included):
    POST methods:                         24
    GET methods:                          2896
    HTTP Request Headers extracted:       2947
    HTTP Request Cookies extracted:       840
    Post parameters extracted:            27
    HTTP response Headers extracted:      2890
    HTTP Response Cookies extracted:      2068
    Unicode:                              72
    Double unicode:                       0
    Non-ASCII representable:              34
    Directory traversals:                 413
    Extra slashes ("//"):                 34
    Self-referencing paths ("./"):        413
    HTTP Response Gzip packets extracted: 92
    Gzip Compressed Data Processed:       84262.00
    Gzip Decompressed Data Processed:     401861.00
    Total packets processed:              17505
===============================================================================
SMTP Preprocessor Statistics
  Total sessions                                   : 0
  Max concurrent sessions                          : 0
===============================================================================
dcerpc2 Preprocessor Statistics
  Total sessions: 0
===============================================================================
SSL Preprocessor:
   SSL packets decoded: 1179
          Client Hello: 164
          Server Hello: 164
           Certificate: 125
           Server Done: 373
   Client Key Exchange: 110
   Server Key Exchange: 71
         Change Cipher: 305
              Finished: 0
    Client Application: 169
```

```
    Server Application: 90
                 Alert: 38
  Unrecognized records: 401
  Completed handshakes: 0
        Bad handshakes: 15
      Sessions ignored: 68
    Detection disabled: 70
===============================================================================
SIP Preprocessor Statistics
  Total sessions: 9
  Total  dialogs: 9
  Requests: 12
          invite:    0
          cancel:    0
             ack:    0
             bye:    0
        register:    0
         options:    12
           refer:    0
       subscribe:    0
          update:    0
            join:    0
            info:    0
         message:    0
          notify:    0
           prack:    0
  Responses: 0
             1xx:    0
             2xx:    0
             3xx:    0
             4xx:    0
             5xx:    0
             6xx:    0
             7xx:    0
             8xx:    0
             9xx:    0
 Ignore sessions:    0
 Ignore channels:    0
===============================================================================
Snort exiting
```

Data

Daftar alert yang didapat dari hasil compile capture packet Wireshark mengguanakn tools Snort.

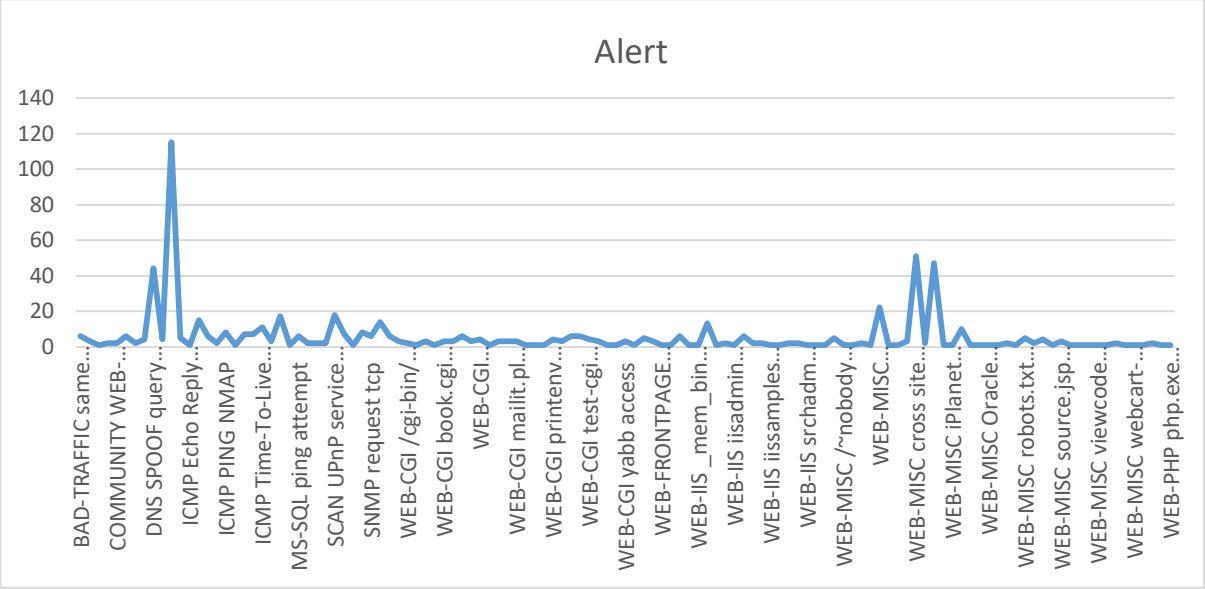
```
03/06-21:01:58.151585  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classification: Misc activity] [Priority: 3] {ICMP} 222.124.4.120 -> 192.168.1.103
03/06-21:01:59.082508  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classification: Misc activity] [Priority: 3] {ICMP} 222.124.4.120 -> 192.168.1.103
03/06-21:01:59.112640  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] {UDP} 192.168.1.103:47852 -> 239.255.255.250
03/06-21:01:59.112673  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] {UDP} 192.168.1.103:47852 -> 222.124.4.120:1
03/06-21:02:00.105612  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] {UDP} 192.168.1.103:47852 -> 239.255.255.250
03/06-21:02:00.105656  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] {UDP} 192.168.1.103:47852 -> 222.124.4.120:1
03/06-21:02:00.172291  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classification: Misc activity] [Priority: 3] {ICMP} 222.124.4.120 -> 192.168.1.103
03/06-21:02:01.109351  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] {UDP} 192.168.1.103:47852 -> 239.255.255.250
03/06-21:02:01.109375  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] {UDP} 192.168.1.103:47852 -> 222.124.4.120:1
03/06-21:02:01.157489  [**] [1:2049:4] MS-SQL ping attempt [**] [Classification: Misc activity] [Priority: 3] {UDP} 192.168.1.103:43125 -> 222.124.4.120:1434
03/06-21:02:01.166709  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classification: Misc activity] [Priority: 3] {ICMP} 222.124.4.120 -> 192.168.1.103
03/06-21:02:03.172474  [**] [1:2049:4] MS-SQL ping attempt [**] [Classification: Misc activity] [Priority: 3] {UDP} 192.168.1.103:43125 -> 222.124.4.120:1434
03/06-21:02:03.222173  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classification: Misc activity] [Priority: 3] {ICMP} 222.124.4.120 -> 192.168.1.103
03/06-21:02:03.228257  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classification: Misc activity] [Priority: 3] {ICMP} 222.124.4.120 -> 192.168.1.103
03/06-21:02:05.498468  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classification: Misc activity] [Priority: 3] {ICMP} 222.124.4.120 -> 192.168.1.103
03/06-21:02:05.505784  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classification: Misc activity] [Priority: 3] {ICMP} 222.124.4.120 -> 192.168.1.103
03/06-21:02:05.988178  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classification: Misc activity] [Priority: 3] {ICMP} 222.124.4.120 -> 192.168.1.103
03/06-21:02:07.689039  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classification: Misc activity] [Priority: 3] {ICMP} 222.124.4.120 -> 192.168.1.103
03/06-21:02:08.086622  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classification: Misc activity] [Priority: 3] {ICMP} 222.124.4.120 -> 192.168.1.103
03/06-21:02:09.464384  [**] [1:1413:10] SNMP private access udp [**] [Classification: Attempted Information Leak] [Priority: 2] {UDP} 192.168.1.103:51562 -> 222.124.4.120:161
03/06-21:02:09.464384  [**] [1:1417:9] SNMP request udp [**] [Classification: Attempted Information Leak] [Priority: 2] {UDP} 192.168.1.103:51562 -> 222.124.4.120:161
03/06-21:02:09.532138  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classification: Misc activity] [Priority: 3] {ICMP} 222.124.4.120 -> 192.168.1.103
03/06-21:02:09.574770  [**] [1:1411:10] SNMP public access udp [**] [Classification: Attempted Information Leak] [Priority: 2] {UDP} 192.168.1.103:50743 -> 222.124.4.120:161
03/06-21:02:09.574770  [**] [1:1417:9] SNMP request udp [**] [Classification: Attempted Information Leak] [Priority: 2] {UDP} 192.168.1.103:50743 -> 222.124.4.120:161
03/06-21:02:09.625615  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classification: Misc activity] [Priority: 3] {ICMP} 222.124.4.120 -> 192.168.1.103
03/06-21:02:09.659716  [**] [1:1417:9] SNMP request udp [**] [Classification: Attempted Information Leak] [Priority: 2] {UDP} 192.168.1.103:42670 -> 222.124.4.120:161
03/06-21:02:10.663446  [**] [1:1417:9] SNMP request udp [**] [Classification: Attempted Information Leak] [Priority: 2] {UDP} 192.168.1.103:42670 -> 222.124.4.120:161
03/06-21:02:10.723009  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classification: Misc activity] [Priority: 3] {ICMP} 222.124.4.120 -> 192.168.1.103
03/06-21:02:11.060531  [**] [1:1417:9] SNMP request udp [**] [Classification: Attempted Information Leak] [Priority: 2] {UDP} 192.168.1.103:42670 -> 222.124.4.120:161
03/06-21:02:12.401967  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classification: Misc activity] [Priority: 3] {ICMP} 222.124.4.120 -> 192.168.1.103
03/06-21:02:13.015197  [**] [1:1417:9] SNMP request udp [**] [Classification: Attempted Information Leak] [Priority: 2] {UDP} 192.168.1.103:42670 -> 222.124.4.120:161
03/06-21:02:13.092362  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classification: Misc activity] [Priority: 3] {ICMP} 222.124.4.120 -> 192.168.1.103
03/06-21:02:16.594371  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classification: Misc activity] [Priority: 3] {ICMP} 222.124.4.120 -> 192.168.1.103
03/06-21:02:16.672152  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classification: Misc activity] [Priority: 3] {ICMP} 222.124.4.120 -> 192.168.1.103
03/06-21:02:48.166221  [**] [1:1411:10] SNMP public access udp [**] [Classification: Attempted Information Leak] [Priority: 2] {UDP} 192.168.1.103:56500 -> 222.124.4.120:161
03/06-21:02:48.166221  [**] [1:1417:9] SNMP request udp [**] [Classification: Attempted Information Leak] [Priority: 2] {UDP} 192.168.1.103:56500 -> 222.124.4.120:161
03/06-21:02:48.221116  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classification: Misc activity] [Priority: 3] {ICMP} 222.124.4.120 -> 192.168.1.103
03/06-21:02:50.919981  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classification: Misc activity] [Priority: 3] {ICMP} 222.124.4.120 -> 192.168.1.103
03/06-21:02:51.032595  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classification: Misc activity] [Priority: 3] {ICMP} 222.124.4.120 -> 192.168.1.103
03/06-21:02:53.351859  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classification: Misc activity] [Priority: 3] {ICMP} 222.124.4.120 -> 192.168.1.103
03/06-21:02:56.078879  [**] [1:254:4] DNS SPOOF query response with TTL of 1 min. and no authority [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 192.168.1.1:53 ->
03/06-21:02:58.489739  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classification: Misc activity] [Priority: 3] {ICMP} 222.124.4.120 -> 192.168.1.103
03/06-21:03:01.248030  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classification: Misc activity] [Priority: 3] {ICMP} 222.124.4.120 -> 192.168.1.103
```

Tabel dan grafik dari daftar alert yang didapat dari hasil compile capture packet Wireshark mengguanakn tools Snort.

No	Alert	Jumlah
1	BAD-TRAFFIC same SRC/DST	6
2	BAD-TRAFFIC tcp port 0 traffic	3
3	COMMUNITY WEB-IIS RSA WebAgent access	1
4	COMMUNITY WEB-MISC JBoss web-console access	2
5	COMMUNITY WEB-MISC mod_jrun overflow attempt	2
6	COMMUNITY WEB-MISC Test Script Access	6
7	COMMUNITY WEB-PHP XSS attempt	2
8	DDOS mstream client to handler	4
9	DNS SPOOF query response with TTL of 1 min. and no authority	44
10	ICMP Address Mask Request	4
11	ICMP Destination Unreachable Port Unreachable	115
12	ICMP Echo Reply	5
13	ICMP Echo Reply undefined code	1
14	ICMP PING	15
15	ICMP PING *NIX	6
16	ICMP PING BSDtype	2
17	ICMP PING NMAP	8
18	ICMP PING undefined code	1
19	ICMP Timestamp Reply	7
20	ICMP Timestamp Request	7
21	ICMP Time-To-Live Exceeded in Transit	11
22	MISC AFS access	3
23	MISC UPnP malformed advertisement	17
24	MISC xdmcp info query	1
25	MS-SQL ping attempt	6
26	P2P GNUTella client request	2
27	P2P Outbound GNUTella client request	2
28	SCAN Amanda client version request	2
29	SCAN UPnP service discover attempt	18
30	SNMP AgentX/tcp request	7
31	SNMP private access udp	1
32	SNMP public access udp	8
33	SNMP request tcp	6
34	SNMP request udp	14
35	SNMP trap tcp	6
36	TFTP Get	3
37	WEB-CGI /cgi-bin/ access	2
38	WEB-CGI /cgi-bin/ access	1
39	WEB-CGI admin.pl access	3
40	WEB-CGI bigconf.cgi access	1
41	WEB-CGI book.cgi access	3
42	WEB-CGI calendar access	3

43	WEB-CGI count.cgi access	6
44	WEB-CGI faqmanager.cgi access	3
45	WEB-CGI FormHandler.cgi access	4
46	WEB-CGI FormHandler.cgi external site redirection attempt	1
47	WEB-CGI formmail access	3
48	WEB-CGI guestbook.cgi access	3
49	WEB-CGI mailit.pl access	3
50	WEB-CGI perl command attempt	1
51	WEB-CGI perl.exe access	1
52	WEB-CGI perl.exe command attempt	1
53	WEB-CGI printenv access	4
54	WEB-CGI quickstore.cgi access	3
55	WEB-CGI search.cgi access	6
56	WEB-CGI test.cgi access	6
57	WEB-CGI test-cgi access	4
58	WEB-CGI upload.cgi access	3
59	WEB-CGI way-board access	1
60	WEB-CGI www-sql access	1
61	WEB-CGI yabb access	3
62	WEB-COLDFUSION administrator access	1
63	WEB-FRONTPAGE .... request	5
64	WEB-FRONTPAGE /_vti_bin/ access	3
65	WEB-FRONTPAGE _vti_rpc access	1
66	WEB-FRONTPAGE shtml.dll access	1
67	WEB-IIS .htr access	6
68	WEB-IIS /iisadmpwd/aexp2.htr access	1
69	WEB-IIS _mem_bin access	1
70	WEB-IIS Directory transversal attempt	13
71	WEB-IIS fpcount access	1
72	WEB-IIS global.asa access	2
73	WEB-IIS iisadmin access	1
74	WEB-IIS iisadmpwd attempt	6
75	WEB-IIS IISProtect access	2
76	WEB-IIS IISProtect siteadmin.asp access	2
77	WEB-IIS iissamples access	1
78	WEB-IIS ISAPI .ida access	1
79	WEB-IIS ISAPI .idq access	2
80	WEB-IIS ISAPI .idq attempt	2
81	WEB-IIS srchadm access	1
82	WEB-IIS trace.axd access	1
83	WEB-MISC .DS_Store access	1
84	WEB-MISC /.... access	5
85	WEB-MISC /~nobody access	1
86	WEB-MISC /~root access	1
87	WEB-MISC /CVS/Entries access	2
88	WEB-MISC /doc/ access	1

89	WEB-MISC /etc/passwd	22
90	WEB-MISC active.log access	1
91	WEB-MISC Admin_files access	1
92	WEB-MISC backup access	3
93	WEB-MISC cross site scripting attempt	51
94	WEB-MISC DB4Web access	2
95	WEB-MISC http directory traversal	47
96	WEB-MISC intranet access	1
97	WEB-MISC iPlanet Search directory traversal attempt	1
98	WEB-MISC login.htm access	10
99	WEB-MISC mod_gzip_status access	1
100	WEB-MISC mod-plsql administration access	1
101	WEB-MISC Oracle Dynamic Monitoring Services dms access	1
102	WEB-MISC Oracle Java Process Manager access	1
103	WEB-MISC oracle portal demo access	2
104	WEB-MISC perl post attempt	1
105	WEB-MISC robots.txt access	5
106	WEB-MISC server-info access	2
107	WEB-MISC server-status access	4
108	WEB-MISC ServletManager access	1
109	WEB-MISC source.jsp access	3
110	WEB-MISC Tomcat servlet mapping cross site scripting attempt	1
111	WEB-MISC Tomcat SnoopServlet servlet access	1
112	WEB-MISC TRACE attempt	1
113	WEB-MISC viewcode access	1
114	WEB-MISC VirusWall FtpSave access	1
115	WEB-MISC webalizer access	2
116	WEB-MISC webcart access	1
117	WEB-MISC webcart-lite access	1
118	WEB-MISC WebDAV search access	1
119	WEB-MISC WEB-INF access	2
120	WEB-MISC WebLogic ConsoleHelp view source attempt	1
121	WEB-PHP php.exe access	1


Alert
140
120
100
80
60
40
20
0
BAD-TRAFFIC same...
COMMUNITY WEB-...
DNS SPOOF query...
ICMP Echo Reply...
ICMP PING NMAP
ICMP Time-To-Live...
MS-SQL ping attempt
SCAN UPnP service...
SNMP request tcp
WEB-CGI /cgi-bin/...
WEB-CGI book.cgi...
WEB-CGI...
WEB-CGI mailit.pl...
WEB-CGI printenv...
WEB-CGI test-cgi...
WEB-CGI yabb access
WEB-FRONTPAGE...
WEB-IIS _mem_bin...
WEB-IIS iisadmin...
WEB-IIS iissamples...
WEB-IIS srchadm...
WEB-MISC /~nobody...
WEB-MISC...
WEB-MISC cross site...
WEB-MISC iPlanet...
WEB-MISC Oracle...
WEB-MISC robots.txt...
WEB-MISC source.jsp...
WEB-MISC viewcode...
WEB-MISC webcart-...
WEB-PHP php.exe...