OT SECURITY ASSIGNEMENT

01 OT Security Assignment

03 Practical Assignment

01 Security Framework Proposal:

1 Question

Security Framework Proposal

As OT Security manager, propose an IT-OT security framework based Purdue Model for a typical Industrial Control System (ICS), which comprises of PLC, DCS, HMI or SCADA. In your proposal, describe how you Identify, Protect, Detect, Respond, and Recover both applications and networks in such environment. Furnish the details on the tools used. Within your proposal, demonstrate practical adoption of at least two of the following standards: ISA 99/IEC 62443, GICSP, CSSA, NIST SP 800- 82, ISO 27001, and NCMS-ISP, preferably with real life examples.

Answer:

1. OT Security Strategy
2. Methodology OT Security using NIC & ISO 2007

OT Security Strategy

Strategy OT Security transformation (Mechanism)

Background

Implementation SMC (security management system and (ACS) Automation Cyber Security standard comprehensive with enhancement networking, firewall, device (embedded, host) and application. And also improve people development/team management ability and executive power, increase the operation efficiency.

Root Cause

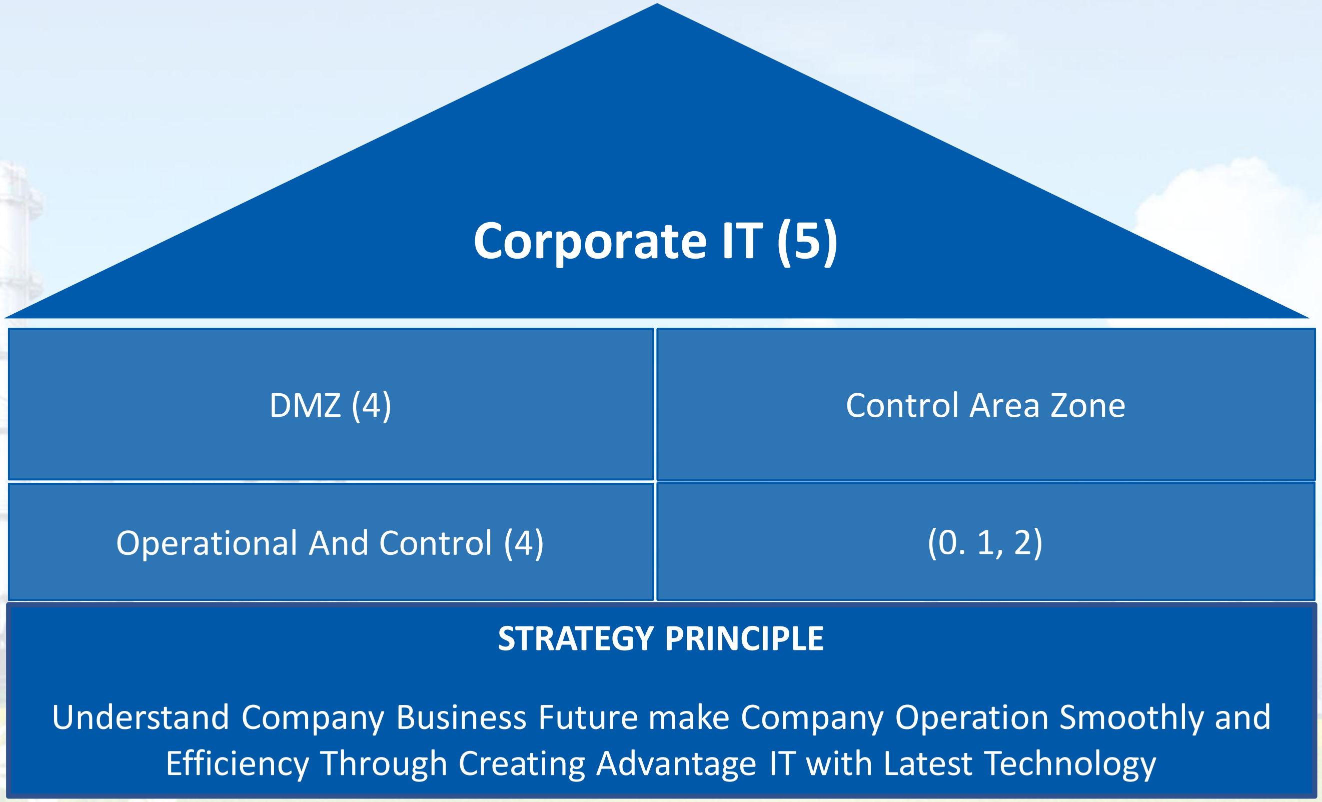
IT-OT Issue weakness security Device PLC and SCADA in line Production, Utility and Engineering and WWTP/WTP.

Goal

ISO 27001 is an international standard in implementing information security management systems or better known as Information Security Management Systems (ISMS). And IT-OT corporate Security to protect all device sustainability and integrate with process business.

Mid- Long-Term IT - OT Security Strategy

IT OT Security Strategy Position



Corporate IT (5)

DMZ (4)

Control Area Zone

Operational And Control (4)

(0. 1, 2)

STRATEGY PRINCIPLE

Understand Company Business Future make Company Operation Smoothly and Efficiency Through Creating Advantage IT with Latest Technology

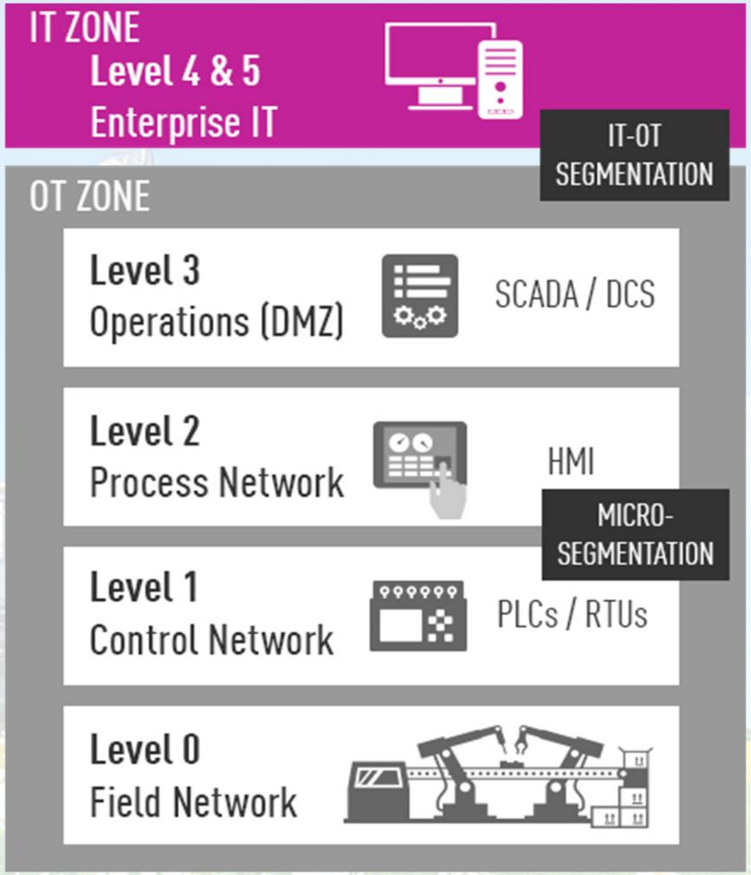
Methodology NIST AND ISA/IEC 62443 and ISO 2007

Answer:

For step Security Framework Proposal, Like this:

- Provide Device Fortinet 300 feature module ICS to monitoring SCADA and DCS system
- Deploy notification to IT-OT embedded PC area floor
- Remote server access deploy to support maker or vendor to external.

Methodology NIST AND ISA/IEC 62443 and ISO 2007



IT Zone
Activity Backup data, Firewall, DRC, Antivirus and The Industrial Revolution 4.0 affects we can optimize the Internet of Things system in factory systems. Opportunity to deploy smart factories using visibility, connectivity and autonomy to reduce manual work (automation), reduce overhead costs and improve operating efficiency.

OT Zone
SMC (security management system and (ACS) Automation Cyber Security standard comprehensive

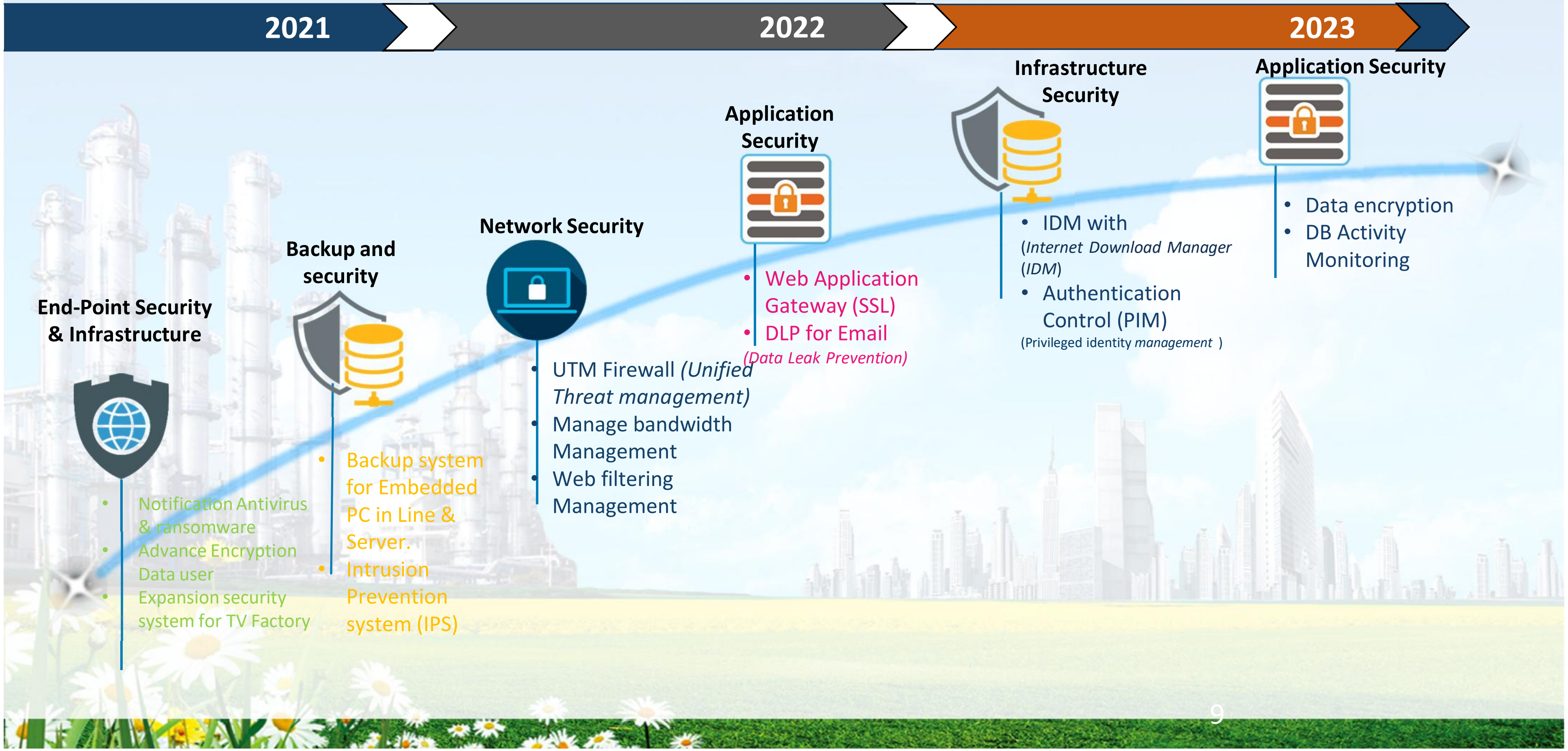
Level 2
Operator automation process network and device area in floor (production, utility, Engr,)

Level 1
Activity control Management Networking L1, L2 and L3 and disparate segment networking

Level)
Host device

IT Security Plan

(2021-2023) – Three Years IT Security Plan



End-Point Security & Infrastructure

- Notification Antivirus & ransomware
- Advance Encryption Data user
- Expansion security system for TV Factory

Backup and security

- Backup system for Embedded PC in Line & Server.
- Intrusion Prevention system (IPS)

Network Security

- UTM Firewall *(Unified Threat management)*
- Manage bandwidth Management
- Web filtering Management

Application Security

- Web Application Gateway (SSL)
- DLP for Email

(Data Leak Prevention)

Infrastructure Security

- IDM with

(*Internet Download Manager* (*IDM*)

- Authentication Control (PIM)

(Privileged identity *management*)

Application Security

- Data encryption
- DB Activity Monitoring

02 Practical Assignment:

2 Question

2. Practical Assignment:

a. Identify the top five threats to OT assets and rank them based on their levels of impact on the asset. Support your findings by quoting reputable sources of information.

Answer:

1. Stuxnet
2. Ransomware
3. Patch
4. Outdated Hardware
5. Ping Flood
6. DoS

Answer

Practical Assignment:

b. For one of the identified threats, pick one of the task below:

i. Write a program using any programming language to create a Proof of Concept that exploits the vulnerability.

Answer:

Often using cmd script for Exploits, requirement device operating system windows

❑ **ping ip - n 255**

```
@echo off
title My ping threats testing
ping <ip address> –n 255
```

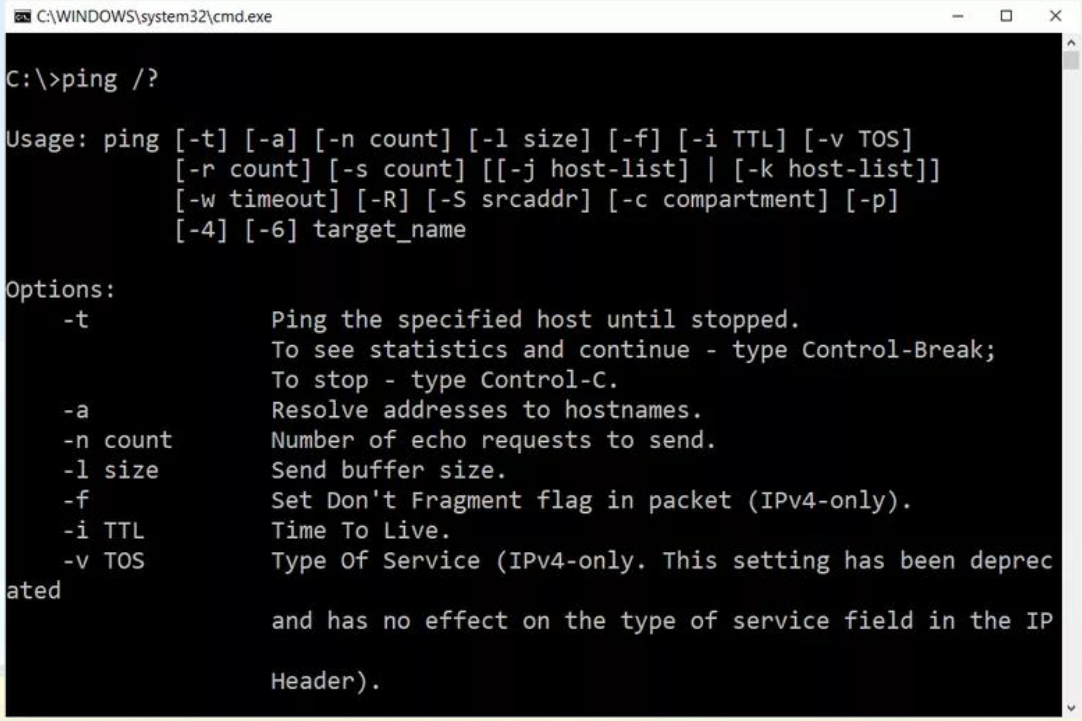
Answer

❑ **ping ip – l 265500**

@echo off
title My ping threats testing
ping <ip address> – l 265500

❑ **ping ip - t**

@echo off
title My ping threats testing
ping <ip address> – t



```
C:\>ping /?

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
            [-r count] [-s count] [[-j host-list] | [-k host-list]]
            [-w timeout] [-R] [-S srcaddr] [-c compartment] [-p]
            [-4] [-6] target_name

Options:
    -t             Ping the specified host until stopped.
                   To see statistics and continue - type Control-Break;
                   To stop - type Control-C.
    -a             Resolve addresses to hostnames.
    -n count       Number of echo requests to send.
    -l size        Send buffer size.
    -f             Set Don't Fragment flag in packet (IPv4-only).
    -i TTL         Time To Live.
    -v TOS         Type Of Service (IPv4-only. This setting has been deprec
ated
                   and has no effect on the type of service field in the IP

                   Header).
```

Answer

Practical Assignment:

b. For one of the identified threats, pick one of the task below:
ii. Write a program that can perform vulnerability discovery for the threat.

Answer:

❑ Can use two ways: With script program command line and use software.

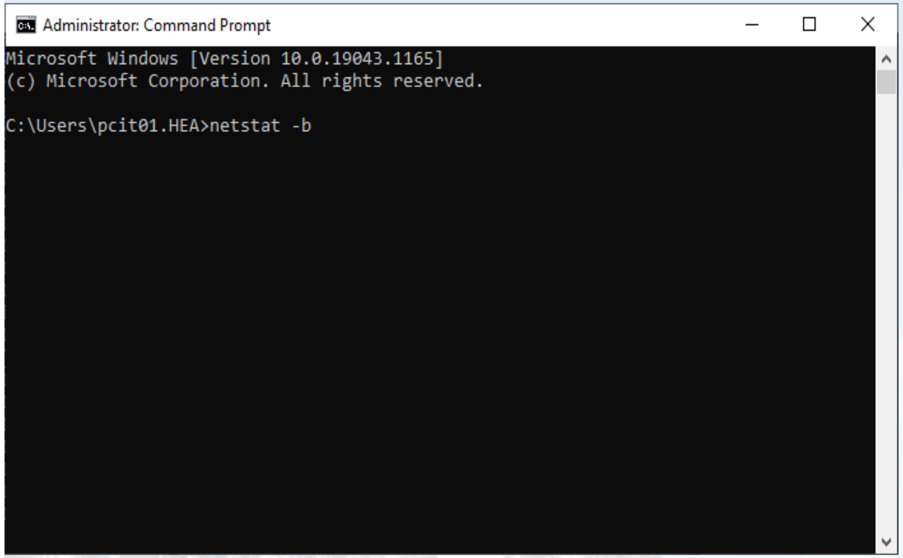
- Using basic script command line with protocol ICMP

netstat - b

```
@echo off
title Netstat Vulnerability Testing
netstat – b
```

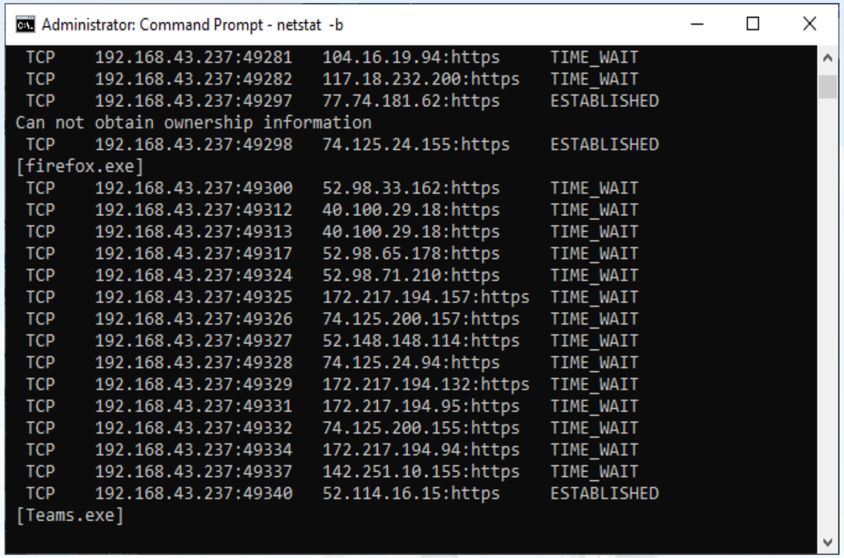
Answer

- **Result cmd “netstat –b”**



```
Microsoft Windows [Version 10.0.19043.1165]
(c) Microsoft Corporation. All rights reserved.

C:\Users\pcit01.HEA>netstat -b
```



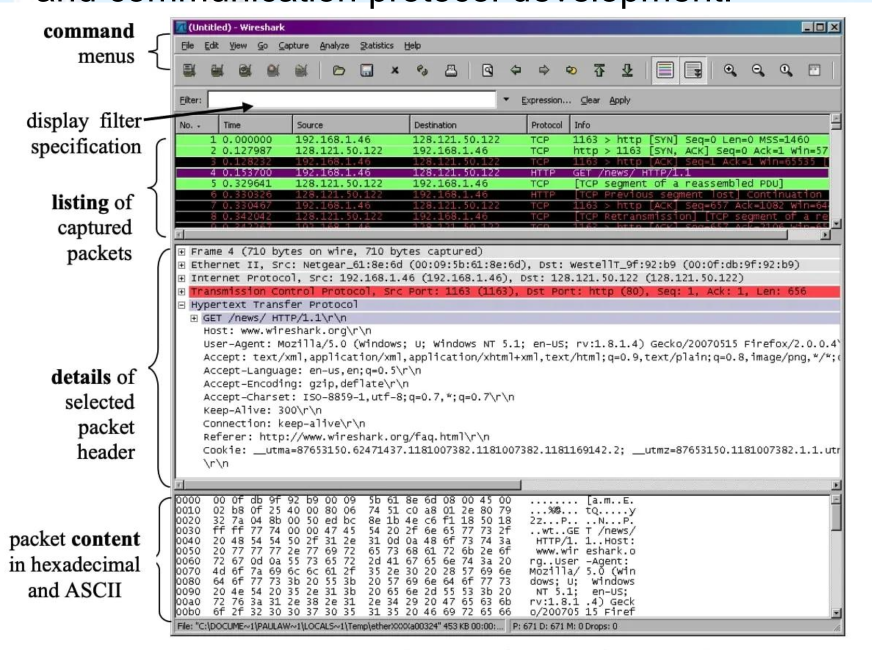
```
  TCP    192.168.43.237:49281   104.16.19.94:https     TIME_WAIT
  TCP    192.168.43.237:49282   117.18.232.200:https   TIME_WAIT
  TCP    192.168.43.237:49297   77.74.181.62:https     ESTABLISHED
 Can not obtain ownership information
  TCP    192.168.43.237:49298   74.125.24.155:https    ESTABLISHED
 [firefox.exe]
  TCP    192.168.43.237:49300   52.98.33.162:https     TIME_WAIT
  TCP    192.168.43.237:49312   40.100.29.18:https     TIME_WAIT
  TCP    192.168.43.237:49313   40.100.29.18:https     TIME_WAIT
  TCP    192.168.43.237:49317   52.98.65.178:https     TIME_WAIT
  TCP    192.168.43.237:49324   52.98.71.210:https     TIME_WAIT
  TCP    192.168.43.237:49325   172.217.194.157:https  TIME_WAIT
  TCP    192.168.43.237:49326   74.125.200.157:https   TIME_WAIT
  TCP    192.168.43.237:49327   52.148.148.114:https   TIME_WAIT
  TCP    192.168.43.237:49328   74.125.24.94:https     TIME_WAIT
  TCP    192.168.43.237:49329   172.217.194.132:https  TIME_WAIT
  TCP    192.168.43.237:49331   172.217.194.95:https   TIME_WAIT
  TCP    192.168.43.237:49332   74.125.200.155:https   TIME_WAIT
  TCP    192.168.43.237:49334   172.217.194.94:https   TIME_WAIT
  TCP    192.168.43.237:49337   142.251.10.155:https   TIME_WAIT
  TCP    192.168.43.237:49340   52.114.16.15:https     ESTABLISHED
 [Teams.exe]
```

With the *nestat -b* parameter we can see the name of the program that accesses the network service. It can be seen from the example above that the program that accesses internet is firefox. With this *command we can also detect if there is malware on our computer.*

Answer

- **Using Software tool Wireshark generated situation device universal**

The Wireshark application itself is one of the Network Analyzer tools commonly used by Network Administrators for network troubleshooting, analysis vulnerability network , software and communication protocol development.

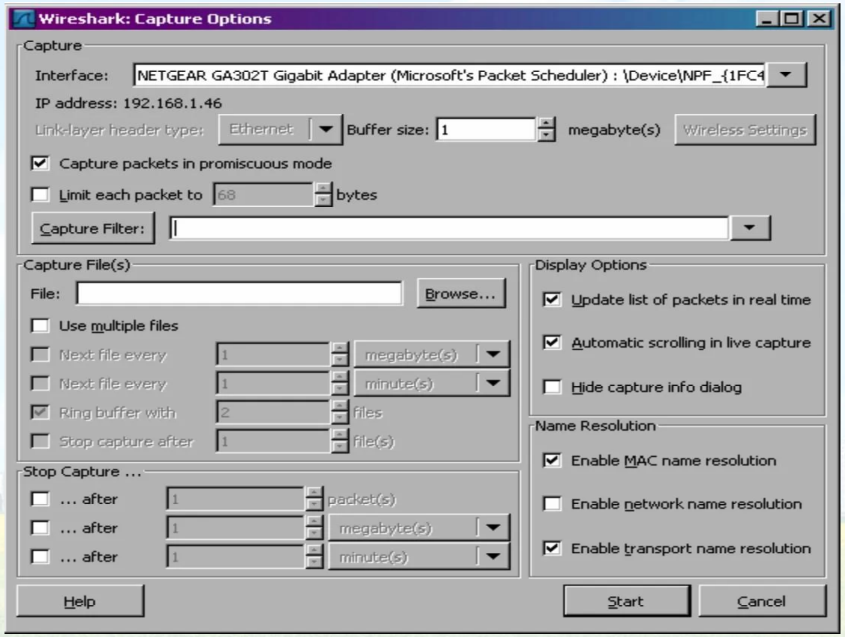

command menus
display filter specification
listing of captured packets
details of selected packet header
packet content in hexadecimal and ASCII
(Untitled) - Wireshark
File
Edit
View
Go
Capture
Analyze
Statistics
Help
Filter:
Expression...
Clear
Apply

```
No. -  Time        Source            Destination       Protocol  Info
     1 0.000000    192.168.1.46      128.121.50.122    TCP       1163 > http [SYN] Seq=0 Len=0 MSS=1460
     2 0.127987    128.121.50.122    192.168.1.46      TCP       http > 1163 [SYN, ACK] Seq=0 Ack=1 Win=57
     3 0.128232    192.168.1.46      128.121.50.122    TCP       1163 > http [ACK] Seq=1 Ack=1 Win=65535 [
     4 0.153700    192.168.1.46      128.121.50.122    HTTP      GET /news/ HTTP/1.1
     5 0.329641    128.121.50.122    192.168.1.46      TCP       [TCP segment of a reassembled PDU]
     6 0.330326    128.121.50.122    192.168.1.46      HTTP      [TCP Previous segment lost] Continuation
     7 0.330467    192.168.1.46      128.121.50.122    TCP       1163 > http [ACK] Seq=657 Ack=1082 Win=64
     8 0.342042    128.121.50.122    192.168.1.46      TCP       [TCP Retransmission] [TCP segment of a re
```

```
⊞ Frame 4 (710 bytes on wire, 710 bytes captured)
⊞ Ethernet II, Src: Netgear_61:8e:6d (00:09:5b:61:8e:6d), Dst: WestellT_9f:92:b9 (00:0f:db:9f:92:b9)
⊞ Internet Protocol, Src: 192.168.1.46 (192.168.1.46), Dst: 128.121.50.122 (128.121.50.122)
⊞ Transmission Control Protocol, Src Port: 1163 (1163), Dst Port: http (80), Seq: 1, Ack: 1, Len: 656
⊟ Hypertext Transfer Protocol
  ⊞ GET /news/ HTTP/1.1\r\n
    Host: www.wireshark.org\r\n
    User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.1.4) Gecko/20070515 Firefox/2.0.0.4
    Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;
    Accept-Language: en-us,en;q=0.5\r\n
    Accept-Encoding: gzip,deflate\r\n
    Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n
    Keep-Alive: 300\r\n
    Connection: keep-alive\r\n
    Referer: http://www.wireshark.org/faq.html\r\n
    Cookie: __utma=87653150.62471437.1181007382.1181007382.1181169142.2; __utmz=87653150.1181007382.1.1.utr
    \r\n
```

```
0000   00 0f db 9f 92 b9 00 09  5b 61 8e 6d 08 00 45 00   ........ [a.m..E.
0010   02 b8 0f 25 40 00 80 06  74 51 c0 a8 01 2e 80 79   ...%@... tQ.....y
0020   32 7a 04 8b 00 50 ed bc  8e 1b 4e c6 f1 18 50 18   2z...P.. ..N...P.
0030   ff ff 77 74 00 00 47 45  54 20 2f 6e 65 77 73 2f   ..wt..GE T /news/
0040   20 48 54 54 50 2f 31 2e  31 0d 0a 48 6f 73 74 3a    HTTP/1. 1..Host:
0050   20 77 77 77 2e 77 69 72  65 73 68 61 72 6b 2e 6f    www.wir eshark.o
0060   72 67 0d 0a 55 73 65 72  2d 41 67 65 6e 74 3a 20   rg..User -Agent: 
0070   4d 6f 7a 69 6c 6c 61 2f  35 2e 30 20 28 57 69 6e   Mozilla/ 5.0 (Win
0080   64 6f 77 73 3b 20 55 3b  20 57 69 6e 64 6f 77 73   dows; U;  Windows
0090   20 4e 54 20 35 2e 31 3b  20 65 6e 2d 55 53 3b 20    NT 5.1;  en-US; 
00a0   72 76 3a 31 2e 38 2e 31  2e 34 29 20 47 65 63 6b   rv:1.8.1 .4) Geck
00b0   6f 2f 32 30 30 37 30 35  31 35 20 46 69 72 65 66   o/200705 15 Firef
```

File: "C:\DOCUME~1\PAULAW~1\LOCALS~1\Temp\etherXXXXa00324" 453 KB 00:00:... | P: 671 D: 671 M: 0 Drops: 0



Interface: NETGEAR GA302T Gigabit Adapter (Microsoft's Packet Scheduler) : \Device\NPF_{1FC4

IP address: 192.168.1.46

Link-layer header type: Ethernet Buffer size: 1 megabyte(s) Wireless Settings

☑ Capture packets in promiscuous mode

□ Limit each packet to 68 bytes

Capture Filter:

File:

□ Use multiple files

□ Next file every 1 megabyte(s)

□ Next file every 1 minute(s)

☑ Ring buffer with 2 files

□ Stop capture after 1 file(s)

□ ... after 1 packet(s)

□ ... after 1 megabyte(s)

□ ... after 1 minute(s)

☑ Update list of packets in real time

☑ Automatic scrolling in live capture

□ Hide capture info dialog

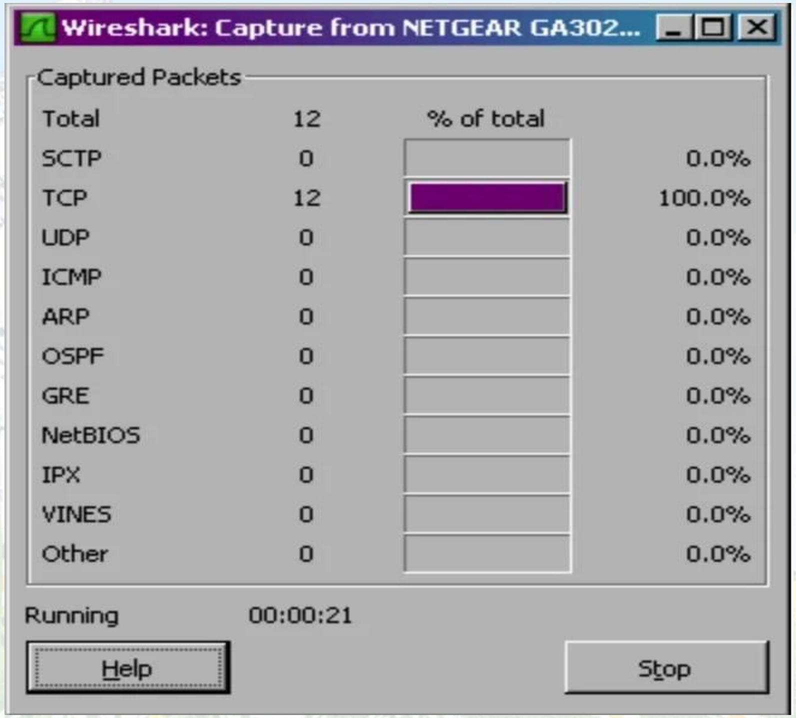
☑ Enable MAC name resolution

□ Enable network name resolution

☑ Enable transport name resolution

Answer

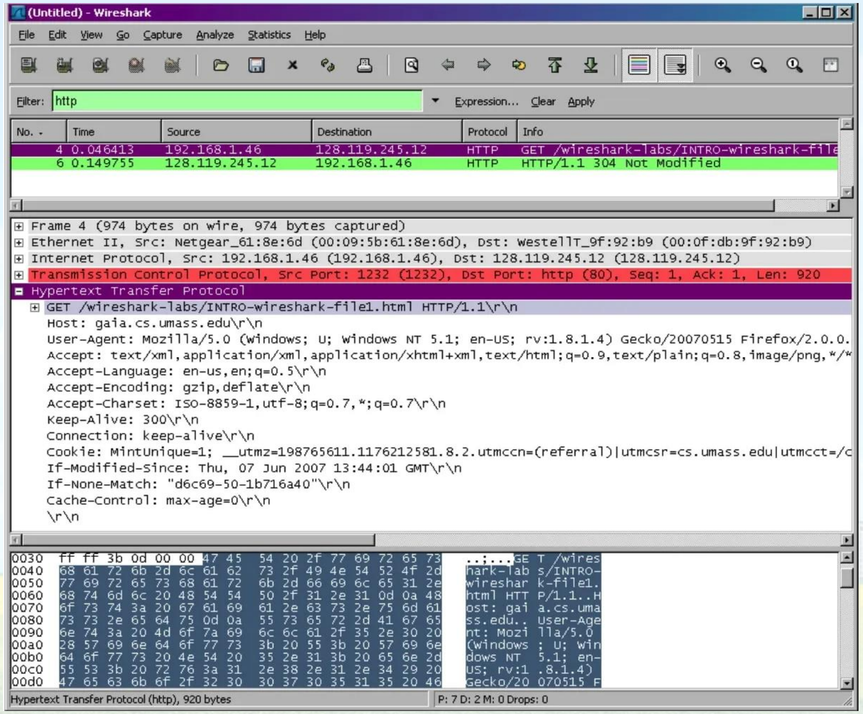
Insert protocol pick one to scan with Wireshark, so software will show automatic analytic perform vulnerability . Please see below capture



Captured Packets

		% of total	
Total	12		
SCTP	0		0.0%
TCP	12		100.0%
UDP	0		0.0%
ICMP	0		0.0%
ARP	0		0.0%
OSPF	0		0.0%
GRE	0		0.0%
NetBIOS	0		0.0%
IPX	0		0.0%
VINES	0		0.0%
Other	0		0.0%

Running 00:00:21



Filter: http

No.	Time	Source	Destination	Protocol	Info
4	0.046413	192.168.1.46	128.119.245.12	HTTP	GET /wireshark-labs/INTRO-wireshark-file
6	0.149755	128.119.245.12	192.168.1.46	HTTP	HTTP/1.1 304 Not Modified

```
⊞ Frame 4 (974 bytes on wire, 974 bytes captured)
⊞ Ethernet II, Src: Netgear_61:8e:6d (00:09:5b:61:8e:6d), Dst: WestellT_9f:92:b9 (00:0f:db:9f:92:b9)
⊞ Internet Protocol, Src: 192.168.1.46 (192.168.1.46), Dst: 128.119.245.12 (128.119.245.12)
⊞ Transmission Control Protocol, Src Port: 1232 (1232), Dst Port: http (80), Seq: 1, Ack: 1, Len: 920
⊟ Hypertext Transfer Protocol
  ⊞ GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.1.4) Gecko/20070515 Firefox/2.0.0.
    Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*
    Accept-Language: en-us,en;q=0.5\r\n
    Accept-Encoding: gzip,deflate\r\n
    Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n
    Keep-Alive: 300\r\n
    Connection: keep-alive\r\n
    Cookie: MintUnique=1; __utmz=198765611.1176212581.8.2.utmccn=(referral)|utmcsr=cs.umass.edu|utmcct=/c
    If-Modified-Since: Thu, 07 Jun 2007 13:44:01 GMT\r\n
    If-None-Match: "d6c69-50-1b716a40"\r\n
    Cache-Control: max-age=0\r\n
    \r\n
```

```
0030  ff ff 3b 0d 00 00 47 45  54 20 2f 77 69 72 65 73   ..;...GE T /wires
0040  68 61 72 6b 2d 6c 61 62  73 2f 49 4e 54 52 4f 2d   hark-lab s/INTRO-
0050  77 69 72 65 73 68 61 72  6b 2d 66 69 6c 65 31 2e   wireshar k-file1.
0060  68 74 6d 6c 20 48 54 54  50 2f 31 2e 31 0d 0a 48   html HTT P/1.1..H
0070  6f 73 74 3a 20 67 61 69  61 2e 63 73 2e 75 6d 61   ost: gai a.cs.uma
0080  73 73 2e 65 64 75 0d 0a  55 73 65 72 2d 41 67 65   ss.edu.. User-Age
0090  6e 74 3a 20 4d 6f 7a 69  6c 6c 61 2f 35 2e 30 20   nt: Mozi lla/5.0 
00a0  28 57 69 6e 64 6f 77 73  3b 20 55 3b 20 57 69 6e   (Windows ; U; Win
00b0  64 6f 77 73 20 4e 54 20  35 2e 31 3b 20 65 6e 2d   dows NT  5.1; en-
00c0  55 53 3b 20 72 76 3a 31  2e 38 2e 31 2e 34 29 20   US; rv:1 .8.1.4) 
00d0  47 65 63 6b 6f 2f 32 30  30 37 30 35 31 35 20 46   Gecko/20 070515 F
```

Hypertext Transfer Protocol (http), 920 bytes   P: 7 D: 2 M: 0 Drops: 0

Answer

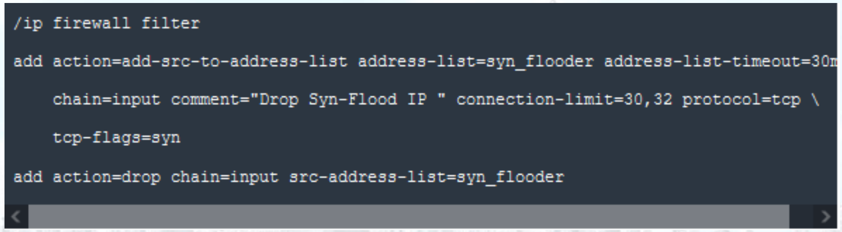
- **Using Software scrip depend on device Mikrotik**

Mikrotik firewall configuration for network or router security protection.

Drop Syn Flood Attack

SYN Flood is a form of Denial Of Service (DOS) attack where the attacker will send a SYN request to the proxy router with the aim of spending router resources until the router "hangs" or cannot function normally. The "ACK" code is not sent back to the router, the attacker just keeps repeating the SYN Request which keeps the router busy to respond to the request without the attacker completing the connection between the client and server.

/ip firewall filter add action=add-src-to-address-list address-list=syn_flooder address-list-timeout=30m \ chain=input comment="Drop Syn-Flood IP " connection-limit=30,32 protocol=tcp \ tcp-flags=syn add action=drop chain=input src-address-list=syn_flooder



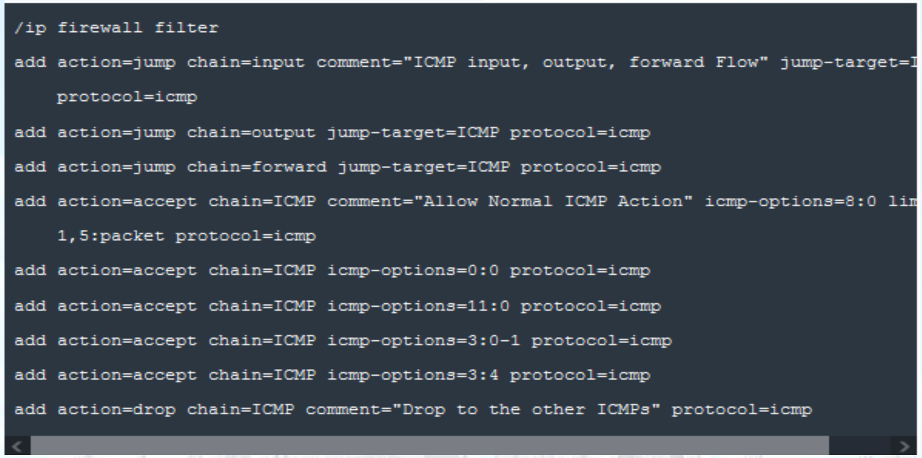
```
/ip firewall filter
add action=add-src-to-address-list address-list=syn_flooder address-list-timeout=30m
    chain=input comment="Drop Syn-Flood IP " connection-limit=30,32 protocol=tcp \
    tcp-flags=syn
add action=drop chain=input src-address-list=syn_flooder
```

Answer

Drop ICMP Flood Attack

ICMP FLOOD is another type of Denial of Service attack (DDOS). By sending ICMP (ping) packets in very large numbers to the target machine with the aim of making an error on the target pc.

/ip firewall filter add action=jump chain=input comment="ICMP input, output, forward Flow" jump-target=ICMP \ protocol=icmp add action=jump chain=output jump-target=ICMP protocol=icmp add action=jump chain=forward jump-target=ICMP protocol=icmp add action=accept chain=ICMP comment="Allow Normal ICMP Action" icmp-options=8:0 limit=\ 1,5:packet protocol=icmp add action=accept chain=ICMP icmp-options=0:0 protocol=icmp add action=accept chain=ICMP icmp-options=11:0 protocol=icmp add action=accept chain=ICMP icmp-options=3:0-1 protocol=icmp add action=accept chain=ICMP icmp-options=3:4 protocol=icmp add action=drop chain=ICMP comment="Drop to the other ICMPs" protocol=icmp



```
/ip firewall filter
add action=jump chain=input comment="ICMP input, output, forward Flow" jump-target=I
    protocol=icmp
add action=jump chain=output jump-target=ICMP protocol=icmp
add action=jump chain=forward jump-target=ICMP protocol=icmp
add action=accept chain=ICMP comment="Allow Normal ICMP Action" icmp-options=8:0 lim
    1,5:packet protocol=icmp
add action=accept chain=ICMP icmp-options=0:0 protocol=icmp
add action=accept chain=ICMP icmp-options=11:0 protocol=icmp
add action=accept chain=ICMP icmp-options=3:0-1 protocol=icmp
add action=accept chain=ICMP icmp-options=3:4 protocol=icmp
add action=drop chain=ICMP comment="Drop to the other ICMPs" protocol=icmp
```

Reference

- https://www.nist.gov/publications/industrial-control-system-cybersecurity-performance-testbed
- http://pustaka.unp.ac.id/file/abstrak_kki/EBOOKS/58%20-%20ISO%2017799%20Standar%20Sistem%20Manajemen%20Keamanan%20Informasi.pdf
- https://www.isa.org/certification/certificate-programs/cybersecurity
- https://www.checkpoint.com/cyber-hub/network-security/what-is-operational-technology-ot-security/
- https://ilmukomputer.org/wp-content/uploads/2015/01/yama-icmp.pdf
- https://www.modalsemangat.com/2019/04/script-firewall-dasar-mikrotik-router.html

THANK YOU !