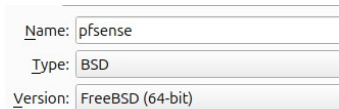


# Cybersecurity Home Lab Using Kali, pfSense, & Metasploitable2

## pfSense Install

1. Download the latest version of pfSense through the pfSense website's download page. Select "ISO Installer" option.

2. Create a new VM in Virtualbox. Set the type to "BSD" and version to "FreeBSD (64-bit)".

A screenshot of the VirtualBox VM creation wizard. It shows three input fields: 'Name' with the value 'pfsense', 'Type' with the value 'BSD', and 'Version' with the value 'FreeBSD (64-bit)'. The fields are arranged vertically and have a light gray background.

Name:	pfsense
Type:	BSD
Version:	FreeBSD (64-bit)

Choose the amount of RAM to allocate (min. 512 MB). Select "Create a virtual hard disk now" and choose "VDI (VirtualBox Disk Image)" and continue. Select "Dynamically allocated" and set the size of the virtual hard disk (min. 10 GB).

3. Navigate to the network settings for the VM. Enable "Adapter 1" and set it to "NAT", enable "Adapter 2" for LAN by setting it to "Internal Network" (using the "metpf" network), and enable "Adapter 3" for LAN by setting it to "Internal Network" (using the "kalpf" network). Save the settings.

4. Start the VM and follow the on-screen instructions to install pfSense. Select the default options for installation by pressing "Enter". Before rebooting the machine at the last step of the installation process, the ISO image has to be removed. This is achieved by clicking "Devices" > "Optical Drives" > (pfsenseISO) > "Force Unmount".

5. Reboot and reset the machine. The VM network adapters should automatically identify the LAN and WAN interfaces.

6. To configure pfsense using the web interface, install another VM on the same LAN network (I chose Ubuntu). On the Ubuntu VM, open a web browser and type in the LAN IP address. Log in by using the default credential: Username: admin Password: pfsense. Follow the installation Wizard to complete the process.

## Metasploitable 2 Install:

1. Download the Metasploitable 2 image from the Rapid7 Metasploitable page.
2. Extract the Metasploitable 2 Image. Using Ubuntu, I only had to right-click the file and select "Extract All".
3. Within VirtualBox, create a new virtual machine by clicking the "New" button. Set the type to "Linux" and version to "Ubuntu (64-bit)".

Name:	Metasploitable2
Type:	Linux
Version:	Other Linux (64-bit)

- Choose the amount of RAM to allocate (min. 512 MB). Select "Use an existing virtual hard disk file". Click on the folder icon to browse for the extracted Metasploitable 2 image
- Select the .vmdk file and click "Open". Then click "Create" to finish setting up the virtual machine.
4. Open the settings for the Metasploitable in the VM manager. Navigate to the "Network" tab and Ensure that "Adapter 1" is enabled and set to "Internal Network" (I created the name "metpf" to use).
  5. Use the default credentials to log in: Username: msfadmin Password: msfadmin.
  6. Verify network connectivity by checking the IP address using the ifconfig and ping command.

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:83:d3:d3
          inet addr:192.168.1.101  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe83:d3d3/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:41 errors:0 dropped:0 overruns:0 frame:0
          TX packets:80 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5923 (5.7 KB)  TX bytes:12038 (11.7 KB)
          Base address:0xd020 Memory:f0200000-f0220000

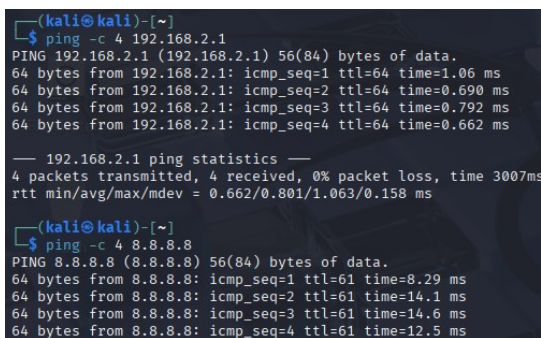
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:197 errors:0 dropped:0 overruns:0 frame:0
          TX packets:197 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:70953 (69.2 KB)  TX bytes:70953 (69.2 KB)
```

```
          inet 192.168.1.101/24 brd 192.168.1.255 scope global eth0
          inet6 fe80::a00:27ff:fe83:d3d3/64 scope link
          valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ ping -c 4 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
 64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=7.42 ms
 64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=1.13 ms
 64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=1.36 ms
 64 bytes from 192.168.1.1: icmp_seq=4 ttl=64 time=1.25 ms

--- 192.168.1.1 ping statistics ---
 4 packets transmitted, 4 received, 0% packet loss, time 2997ms
rtt min/avg/max/mdev = 1.135/2.793/7.422/2.673 ms
```

## Kali OVA Install

1. Through the Kali Linux website, navigate to the Kali Linux download page and select and download the OVA file.
2. On VirtualBox, click on "File" from the menu bar, select "Import Appliance", and click on the folder icon to browse for the downloaded Kali Linux OVA file. Select the OVA file and click "Next". Review and adjust the settings for resource allocation. Click "Import" to start the import process.
3. Select the VM and navigate to the network settings. Ensure that "Adapter 1" is enabled and set to "Internal Network" (kalpf).
4. After booting up the VM, use the default credentials to log in: Username: kali Password: kali. Update the machine using the “sudo apt update && sudo apt upgrade” commands.
5. Verify the connectivity to the router using the ping command.



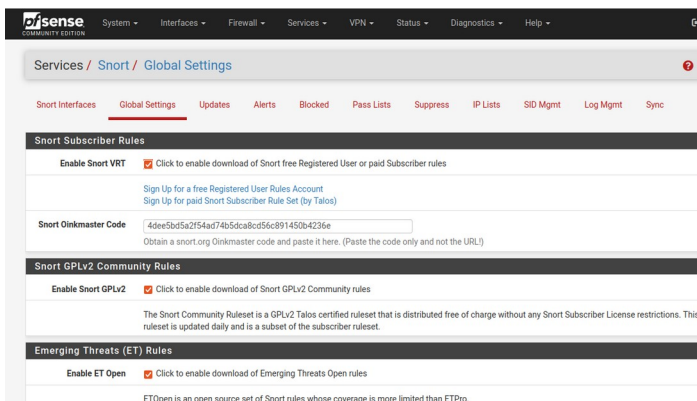
```
(kali㉿kali)-[~]
$ ping -c 4 192.168.2.1
PING 192.168.2.1 (192.168.2.1) 56(84) bytes of data:
64 bytes from 192.168.2.1: icmp_seq=1 ttl=64 time=1.06 ms
64 bytes from 192.168.2.1: icmp_seq=2 ttl=64 time=0.690 ms
64 bytes from 192.168.2.1: icmp_seq=3 ttl=64 time=0.792 ms
64 bytes from 192.168.2.1: icmp_seq=4 ttl=64 time=0.662 ms
— 192.168.2.1 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3007ms
rtt min/avg/max/mdev = 0.662/0.801/1.063/0.158 ms

(kali㉿kali)-[~]
$ ping -c 4 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data:
64 bytes from 8.8.8.8: icmp_seq=1 ttl=61 time=8.29 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=61 time=14.1 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=61 time=14.6 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=61 time=12.5 ms
```

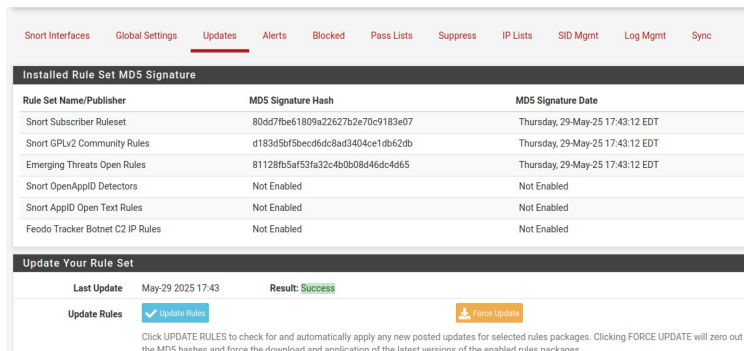
## Snort Install and Configuration on pfSense

1. Open the VM used to access the pfSense Web Interface. Enter the LAN IP address (192.168.1.1) in a web browser. Log in with the updated credentials.
2. Navigate to the Package Manager: Go to System > Package Manager. Click on the Available Packages tab and type “snort” in the search bar to find the Snort package. Click the Install button next to the Snort package and click confirm.

3. After installation, go to Services > Snort to access the package. From here, go to Global Settings. To configure rule subscriptions, check the box for Enable Snort VRT. Create a free account at Snort.org to get an "Oinkcode". This code will need to be inputted into the Snort Oinkmaster Code field. Check the box for Enable Snort GPLv2 Community Rules and Enable ET Open (emerging threats rules). Scroll to Rules Update Settings and set update interval to a frequency of your choosing. Save these changes.



4. Go to Updates on the right of Global Settings. Verify that Update Your Rule Set displays the enabled rule sets and click Update Rules.



5. Go to Snort Interfaces, left of Global Settings tab and click Add.

Check the Enable box and select LAN from the dropdown menu for Interface. Check the box for Send Alerts to System Log and Block Offenders. For Which IP to Block, select SRC from the dropdown. Save the settings.

192.168.1.1/snort/snort\_interfaces\_edit.php?id=0 67%

Enable

☒ Enable interface

Interface

LAN (em1)

Choose the interface where this Snort instance will inspect traffic.

Description

Snort on kalmetg!

Enter a meaningful description here for your reference.

Snap Length

1518

Enter the desired interface enaplen value in bytes. Default is 1518 and is suitable for most applications.

Alert Settings

Send Alerts to System Log

☒ Snort will send Alerts to the firewall's system log. Default is Not Checked.

System Log Facility

LOG\_AUTH

Select system log Facility to use for reporting. Default is LOG\_AUTH.

System Log Priority

LOG\_ALERT

Select system log Priority (Level) to use for reporting. Default is LOG\_ALERT.

Enable Packet Captures

☐ Checking this option will automatically capture packets that generate a Snort alert into a tcpdump compatible file

Enable Unified2 Logging

☐ Checking this option will cause Snort to simultaneously log alerts to a unified2 binary format log file in the logging subdirectory for this interface. Default is Not Checked.  
Log size and retention limits for the Unified2 log should be configured on the LOG MGMT tab when this option is enabled.

Block Settings

Block Offenders

☒ Checking this option will automatically block hosts that generate a Snort alert. Default is Not Checked.

IPS Mode

Legacy Mode

Select blocking mode operation. Legacy Mode inspects copies of packets while Inline Mode inserts the Snort inspection engine into the network stack between the NIC and the OS. Default is Legacy Mode.  
  
Legacy Mode uses the PCAP engine to generate copies of packets for inspection as they traverse the interface. Some "leakage" of packets will occur before Snort can determine if the traffic matches a rule and should be blocked. Inline mode instead intercepts and inspects packets before they are handed off to the host network stack for further processing. Packets matching DROP rules are simply discarded (dropped) and not passed to the host network stack. No leakage of packets occurs with Inline Mode. WARNING: Inline Mode only works with NIC drivers which properly support Netmap! Supported drivers: bnx2, cc, cxgb, cxl, em, ems, ena, ice, igb, igc, ix, iqbte, ixl, lem, re, vmx, vnet. If problems are experienced with Inline Mode, switch to Legacy Mode instead.

Kill States

☒ Checking this option will kill firewall established states for the blocked IP. Default is checked.

Which IP to Block

SRC

Go back to Snort Interfaces and click the Edit icon beside the newly created LAN interface.

Under the LAN Categories tab, check the box for Use IPS Policy.

From the IPS Policy Selection dropdown, select a policy ( I chose Security), and save the settings.

Services / Snort / Interface Settings / LAN - Categories

Snort Interfaces

Global Settings

Updates

Alerts

Blocked

Pess Lists

Suppress

IP Lists

SID Mgmt

Log Mgmt

Sync

LAN Settings

LAN Categories

LAN Rules

LAN Variables

LAN Preprocs

LAN IP Rep

LAN Logs

Automatic Flowbit Resolution

Resolve Flowbits

☒ If checked, Snort will auto-enable rules required for checked flowbits. Default is Checked.  
Snort will examine the enabled rules in your chosen rule categories for checked flowbits. Any rules that set these dependent flowbits will be automatically enabled and added to the list of files in the interface rules directory.

Auto-Flowbit Rules

☐ View  
Disabling auto-flowbit rules is strongly discouraged for security reasons. Auto-enabled flowbit rules that generate unwanted alerts should have their GID:SID added to the Suppression List for the interface instead of being disabled.

Snort Subscriber IPS Policy Selection

Use IPS Policy

☒ If checked, Snort will use rules from one of three pre-defined IPS policies in the Snort Subscriber rules. Default is Not Checked.  
Selecting this option disables manual selection of Snort Subscriber categories in the list below, although Emerging Threats categories may still be selected if enabled on the Global Settings tab. These will be added to the pre-defined Snort IPS policy rules from the Snort VRT.

IPS Policy Selection

Security

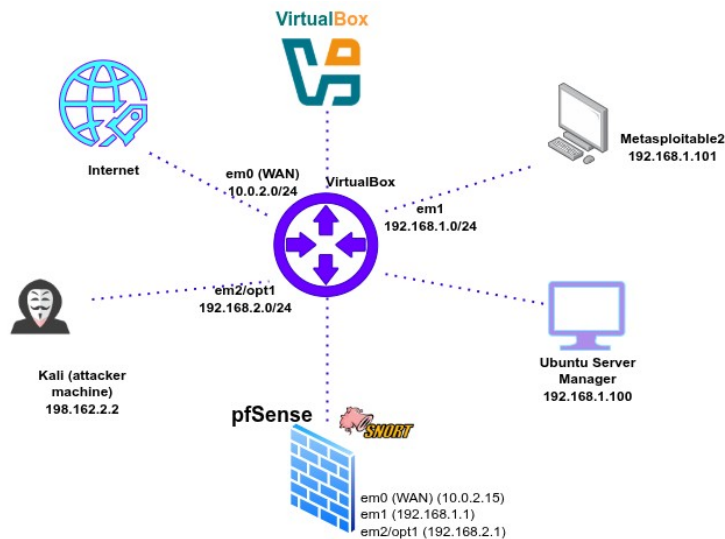
Snort IPS policies are: Connectivity, Balanced, Security or Max Detect.  
Connectivity blocks most major threats with few or no false positives. Balanced is a good starter policy. It is speedy, has good base coverage level, and covers most threats of the day. It includes all rules in Connectivity. Security is a stringent policy. It contains everything in the first two plus policy-type rules such as a Flash object in an Excel file. Max-Detect is a policy created for testing network traffic through your device. This policy should be used with caution on production systems!

6. Once again, go back to Snort Interfaces. On the same LAN interface, click the Start icon Status column to begin the service.

7. To access the logs that will generate, : go to Status > System Logs and select Firewall.

Action	Time	Interface	Rule	Source	Destination	Protocol
✗	May 30 15:35:59	OPT1	Block snort2c hosts (1000000118)	192.168.2.2	192.168.1.101	ICMP
✗	May 30 15:35:59	OPT1	Block snort2c hosts (1000000118)	192.168.2.2:56490	192.168.1.101:443	TCP-S
✗	May 30 15:35:59	OPT1	Block snort2c hosts (1000000118)	192.168.2.2:56490	192.168.1.101:80	TCP-A
✗	May 30 15:35:59	OPT1	Block snort2c hosts (1000000118)	192.168.2.2	192.168.1.101	ICMP
✗	May 30 15:35:57	OPT1	Block snort2c hosts (1000000118)	192.168.2.2	192.168.1.101	ICMP
✗	May 30 15:35:57	OPT1	Block snort2c hosts (1000000118)	192.168.2.2:56488	192.168.1.101:80	TCP-A
✗	May 30 15:35:57	OPT1	Block snort2c hosts (1000000118)	192.168.2.2:56488	192.168.1.101:443	TCP-S
✗	May 30 15:35:57	OPT1	Block snort2c hosts (1000000118)	192.168.2.2	192.168.1.101	ICMP
✗	May 30 15:35:11	OPT1	Block snort2c hosts (1000000118)	192.168.2.2	192.168.1.101	ICMP
✗	May 30 15:35:11	OPT1	Block snort2c hosts (1000000118)	192.168.2.2:62609	192.168.1.101:443	TCP-S
✗	May 30 15:35:11	OPT1	Block snort2c hosts (1000000118)	192.168.2.2:62609	192.168.1.101:80	TCP-A

In the screenshot of the Snort logs above, ping and nmap (-sS, -sA) commands used against the Metasploitable2 VM that were blocked by Snort is displayed.



This figure is the topology for the lab setup.

## Metasploit Vulnerability Scanning Using WMAP

In this example, WMAP, a web application scanner, will be used within the Kali VM within Metasploit.

1. From the terminal, initialize the Metasploit database by running the ‘msfdb init’ command, start the Postgres database server with the ‘service postgresql start’ command, and then launch msfconsole with the ‘msfconsole’ command.

```
kali@kali:~$ service postgresql start
*
kali@kali:~$ sudo suconsole
Metasploit tip: Use the edit command to open the currently active
in your editor

{ it looks like you're trying to run a
module

}

[
  @
  |
  |
  ||
  ||
  |
  |
  |
  |
]

--=[ metasploit v6.4.56-dev ]
+ --=[ 2584 exploits - 1291 auxiliary - 393 post ]
+ --=[ 1687 payloads - 49 encoders - 13 nops ]
+ --=[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/
msf6 > |
```

Start WMAP by entering 'load wmap'.

```
msf6 > load wmap

[WMAP 1.5.1] == et [ ] metasploit.com 2012
[*] Successfully loaded plugin: wmap
msf6 > wmap_sites -a http://192.168.1.101
[*] Site created.
msf6 > wmap_sites -l
[*] Available sites

  Id  Host      Vhost      Port  Proto  # Pages  # Forms
  --  -
  0   192.168.1.101 192.168.1.101 80    http   0        0

msf6 >
```

Add the target site (metasploitable2) with 'wmap\_sites -a http://192.168.1.101'. Load the vulnerabilities using the module (mutillidae) 'wmap\_targets -t

http://192.168.68.12/mutillidae/index.php' and confirm that the target has been successfully added using 'wmap\_targets -l'.

```
msf6 > wmap_targets -t http://192.168.1.101/mutillidae/index.php
msf6 > wmap_targets -l
[*] Defined targets

  Id  Vhost      Host      Port  SSL  Path
  --  -
  0   192.168.1.101 192.168.1.101 80    false /mutillidae/index.php

msf6 >
```

Before we scan the target, run 'wmap\_run -t' to list all the enabled modules.

```
msf6 > wmap_run -t
[*] Testing target:
[*] Site: 192.168.1.101 (192.168.1.101)
[*] Port: 80 SSL: false

[*] Testing started. 2025-05-30 19:04:51 -0400
[*] Loading wmap modules...
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/logging-2.4.0/lib/logging.rb:10: warning: /usr/lib/x86_64-linux-gnu/ruby3.3.0/syslog.so was loaded from the standard library, but will no longer be part of the default gems starting from Ruby 3.4.0.
You can add syslog to your Gemfile or gemspec to silence this warning.
Also please contact the author of logging-2.4.0 to request adding syslog into its gemspec.
[*] 39 wmap enabled modules loaded.
[*]

- [ SSL testing ] -

[*] Target is not SSL. SSL modules disabled.
[*]

- [ Web Server testing ] -

[*] Module auxiliary/scanner/http/http_version
[*] Module auxiliary/scanner/http/open_proxy
[*] Module auxiliary/admin/http/tomcat_administration
[*] Module auxiliary/admin/http/tomcat_utf8_traversal
[*] Module auxiliary/scanner/http/drupal_views_user_enum
[*] Module auxiliary/scanner/http/frontpage_login
[*] Module auxiliary/scanner/http/host_header_injection
[*] Module auxiliary/scanner/http/options
[*] Module auxiliary/scanner/http/robots.txt
[*] Module auxiliary/scanner/http/scraper
[*] Module auxiliary/scanner/http/svn_scanner
[*] Module auxiliary/scanner/http/trace
[*] Module auxiliary/scanner/http/vhost_scanner
[*] Module auxiliary/scanner/http/webdav_internal_ip
[*] Module auxiliary/scanner/http/webdav_scanner
[*] Module auxiliary/scanner/http/webdav_website_content
[*]

- [ File/Dir testing ] -
```

Running the 'wmap\_run -e' command will run all of the modules

```
msf6 > wmap_run -e
[*] Using ALL wmap enabled modules.
[*] NO WMAP NODES DEFINED. Executing local modules
[*] Testing target:
[*] Site: 192.168.1.101 (192.168.1.101)
[*] Port: 80 SSL: false

[*] Testing started. 2025-05-30 19:28:53 -0400
[*]

- [ SSL testing ] -

[*] Target is not SSL. SSL modules disabled.
[*]

- [ Web Server testing ] -

[*] Module auxiliary/scanner/http/http_version
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.16/lib/recog/fingerprint/regexp_factory.rb:34: warning: nested repeat operator '+' and '?' was replaced with '*' in regular expression
[*] 192.168.1.101:80 Apache/2.2.8 (Ubuntu) DAV/2 ( Powered by PHP/5.2.4-2ubuntu5.10 )
[*] Module auxiliary/scanner/http/host_header_injection
[*] Module auxiliary/admin/http/tomcat_administration
[*] Module auxiliary/admin/http/tomcat_utf8_traversal
[*] Attempting to connect to 192.168.1.101:80
[*] No File(s) found
[*] Module auxiliary/scanner/http/drupal_views_user_enum
192.168.1.101 does not appear to be vulnerable, will not continue
[*] Module auxiliary/scanner/http/frontpage_login
[*] 192.168.1.101:80 - http://192.168.1.101/ may not support FrontPage Server Extensions
[*] Module auxiliary/scanner/http/host_header_injection
[*] Module auxiliary/scanner/http/options
[*] Module auxiliary/scanner/http/robots.txt
[*] Module auxiliary/scanner/http/scraper
[*] [192.168.1.101] / [Metasploitable2 - Linux]
[*] Module auxiliary/scanner/http/svn_scanner
[*] Using code '404' as not found.
[*] Module auxiliary/scanner/http/trace
[*] 192.168.1.101:80 is vulnerable to Cross-Site Tracing
[*] Auxiliary failed: Mef::ValidationError Failed to report vuln for 192.168.1.101:80 to the database
```



Use the 'wmap\_vulns -l' command to display the results of the scan. These results provide pivot points for a variety of attacks that can be performed on the machine ( ex: /phpMyAdmin directory; an open-source administration tool for MySQL database systems).

```
msf6 > wmap_vulns -l
[*] + [192.168.1.101] (192.168.1.101): scraper /
[*] scraper Scraper
[*] GET Metasploitable2 - Linux
[*] + [192.168.1.101] (192.168.1.101): directory /dav/
[*] directory Directory found.
[*] GET Res code: 200
[*] + [192.168.1.101] (192.168.1.101): directory /doc/
[*] directory Directory found.
[*] GET Res code: 200
[*] + [192.168.1.101] (192.168.1.101): directory /cgi-bin/
[*] directory Directory found.
[*] GET Res code: 403
[*] + [192.168.1.101] (192.168.1.101): directory /icons/
[*] directory Directory found.
[*] GET Res code: 200
[*] + [192.168.1.101] (192.168.1.101): directory /index/
[*] directory Directory found.
[*] GET Res code: 200
[*] + [192.168.1.101] (192.168.1.101): directory /phpMyAdmin/
[*] directory Directory found.
[*] GET Res code: 200
[*] + [192.168.1.101] (192.168.1.101): directory /test/
[*] directory Directory found.
[*] GET Res code: 200
[*] + [192.168.1.101] (192.168.1.101): file /index.php
[*] file File found.
[*] GET Res code: 404
[*] + [192.168.1.101] (192.168.1.101): file /dav
[*] file File found.
[*] GET Res code: 404
[*] + [192.168.1.101] (192.168.1.101): file /index
[*] file File found.
[*] GET Res code: 404
[*] + [192.168.1.101] (192.168.1.101): file /phpMyAdmin
[*] file File found.
[*] GET Res code: 404
[*] + [192.168.1.101] (192.168.1.101): file /test
```

It is worth noting that the previous settings configured on Snort via pfsense did NOT detect nor prevent these scans from being performed on the metasploitable2 VM.

## Kali

Kali is a Linux distribution for penetration testing and ethical hacking, equipped with numerous tools for a range of security tasks including: nmap, metasploit, wireshark, aircrack-ng, burpsuite, etc.

Nmap, which stands for network mapper, is a powerful network scanning tool that discovers hosts and services on a computer network. It can be used for tasks such as managing service upgrade schedules, monitoring service uptime, detect vulnerabilities within systems, and perform OS detection. The Metasploit framework is a penetration testing platform that allows security professionals to find and exploit vulnerabilities in systems, write and execute exploit code, test security vulnerabilities, and conduct security assessments. Wireshark is network protocol analyzer

that captures and displays data packets in real-time. It can be used for a variety of cases such as network troubleshooting, analysis, and protocol development. It helps in understanding network traffic and identifying issues. Aircrack-ng has a suite of tools for assessing the security of Wi-Fi networks. Its used for cracking WEP,WPA, and WPA2 encryption keys, monitoring wireless traffic, and performing packet injection. Burp Suite is web application security testing tool that provides a range of features for testing web applications from intercepting and modifying web traffic, scanning for vulnerabilities, to performing automated attacks on web applications.

### **pfSense**

pfSense is an open-source firewall and router software distribution based on FreeBSD. It is designed to provide a robust and flexible platform for network security and management, and is widely used for its comprehensive features, including stateful packet inspection, VPN support, and traffic shaping. Its open-source meaning that it can be customized to meet specific needs of a business.

### **Snort**

Snort is an open-source network intrusion detection and prevention system developed by Cisco. It analyzes network traffic in real-time and can log packets or alert users to suspicious activities.

Snort is crucial for identifying and mitigating threats in network environments by using a rule-based language to detect various types of attacks, including denial-of-service attacks, buffer overflows, and stealth port scans. The service also provides real-time alerts and logging capabilities, in order to maintain security and respond to incidents in an effective manner.

Intrusion Detection Systems and Intrusion Prevention Systems are vital components of cybersecurity strategies, as they aid in threat detection and incident response. The goal f these systems is to help organizations quickly identify and respond to potential security breaches, minimizing damage and data loss.

## References

- Drd. (2018, September 26). *How to use Metasploit's WMAP module to scan web applications for common vulnerabilities*. Null Byte. <https://null-byte.wonderhowto.com/how-to/use-metasploits-wmap-module-scan-web-applications-for-common-vulnerabilities-0187572/>
- Garn, D. (2025, February 7). *Top 21 Kali Linux tools and how to use them*. Search Security. <https://www.techtarget.com/searchsecurity/tip/Top-Kali-Linux-tools-and-how-to-use-them>
- GeeksforGeeks. (2025, April 2). *How to install Metasploitable 2 in VirtualBox*. GeeksforGeeks. <https://www.geeksforgeeks.org/how-to-install-metasploitable-2-in-virtualbox/>
- Patil, M. (2022, June 26). How to install pfsense on your PCs and virtual machines? *Medium*. <https://medium.com/@meghraj312002/how-to-install-pfsense-on-your-pcs-and-virtual-machines-76434758e024>
- PfSense Documentation* | *PfSense Documentation*. (n.d.). <https://docs.netgate.com/pfsense/en/latest/>
- Romano, J., & Christensen, J. (n.d.). *Network Monitoring – Snort Network IDS/IPS*. Pressbooks. <https://eaglepubs.erau.edu/mastering-enterprise-networks-labs/chapter/intrusion-detection-system/>
- Satish, S. (2025, May 13). *18 Best Kali Linux tools and how to use them*. Simplilearn.com. <https://www.simplilearn.com/top-kali-linux-tools-article>
- Zenarmor. (2024, August 28). *ZenArmor Documentation*. <https://www.zenarmor.com/docs/network-security-tutorials/what-is-snort>