

Lab 4-2: SIEM

The aim of this lab is to configure logging on network and host-based devices such as pfSense firewall and Windows 2016 Server. Similarly, to create Snort intrusion detection system signatures to detect network-based intrusion and attacks. The Splunk SIEM application needs to be configured to receive logs from above mentioned devices for security monitoring and incident investigation purposes.

Network Number: 2 networks, namely **em1** (Private/LAN) and **em2** (DMZ/OPT1)

Your networks will be: 192.168.x.0/24 and 192.168.y.0/24

Host machines:

- Bodhi_Linux_Private (i.e., i_csn11128-9_Bodhi_Linux_Private_00x)
- Windows 10_DMZ (i.e., i_csn11128-9_Windows_10_DMZ_00x)
- Windows 2016 Server (i.e., i_csn11128-9_Windows_Server_2016_DMZ_00x)
- pfSense (i.e., i_csn11128-9_pfSense_00x)
- Bodhi_Linux_Public (i.e., i_csn11128-9_Bodhi_Linux_Public_00x)

User logins:

- Bodhi_Linux_Private (User: bodhi, Password: napier123)
- Windows 10_DMZ (User: Napier, Password: napier)
- Windows 2016 Server_DMZ (User: Napier, Password: Ankle123)
- pfSense (User: admin, Password: pfsense)
- Bodhi_Linux_Public (User: bodhi, Password: napier123)
- Splunk Enterprise: (User: napier, Password: Ankle123)

Our first activity is to configure the pfSense firewall as performed in the previous labs to setup network connection. You should have been assigned a set of IP addresses by the module leader in Week 1. In this lab, you will use the assigned IP addresses to configure the hosts in the Private (LAN) 192.168.x.0/24 and DMZ 192.168.y.0/24 respectively as shown in Figure 1.

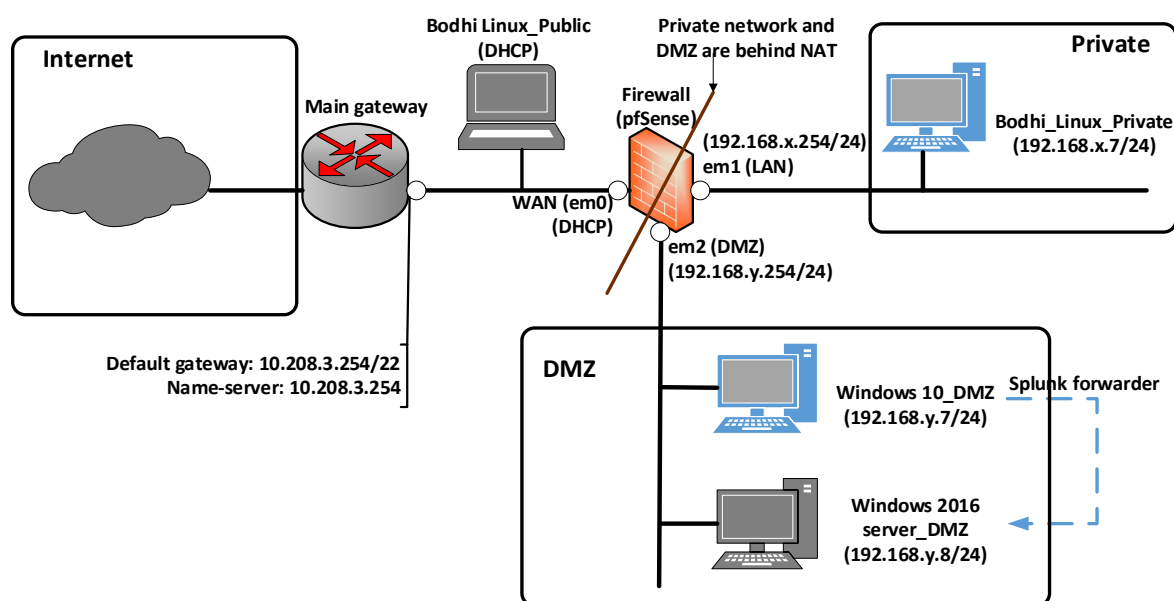


Figure 1: Lab infrastructure setup

A. NAT port forwarding to the Windows 10_DMZ

Port forwards allow access to a specific port, port range or protocol on a privately addressed internal network device. This is most used when hosting servers or using applications that require inbound connections from the Internet.

Port forwards take precedence over any services running locally on the firewall, such as the web interface, SSH, and so on. Port forwards also take precedence over 1:1 NAT.

Configure pfSense using NAT port forwarding to the *Windows 10_DMZ* host inside the DMZ, and make sure to check the firewall rules to enable logging on each rule. Figures 2 and 3 show the screenshots of how the rules look when they are configured.

Firewall / NAT / Port Forward										
The changes have been applied successfully. The firewall rules are now reloading in the background. Monitor the filter reload progress.										
Port Forward 1:1 Outbound NPT										
Rules										
	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
<input type="checkbox"/>	WAN	ICMP	*	*	WAN address	*	192.168.138.7	*		Edit Copy Delete
<input type="checkbox"/>	WAN	TCP	*	*	WAN address	445 (MS DS)	192.168.138.7	445 (MS DS)		Edit Copy Delete
<input type="checkbox"/>	WAN	TCP	*	*	WAN address	80 (HTTP)	192.168.138.7	80 (HTTP)		Edit Copy Delete
<input type="checkbox"/>	WAN	TCP	*	*	WAN address	21 (FTP)	192.168.138.7	21 (FTP)		Edit Copy Delete
<input type="checkbox"/>	WAN	TCP	*	*	WAN address	22 (SSH)	192.168.138.7	22 (SSH)		Edit Copy Delete
<input type="checkbox"/>	WAN	TCP	*	*	WAN address	23 (Telnet)	192.168.138.7	23 (Telnet)		Edit Copy Delete
<input type="checkbox"/>	WAN	TCP	*	*	WAN address	443 (HTTPS)	192.168.138.7	443 (HTTPS)		Edit Copy Delete

[Add](#) [Add](#) [Delete](#) [Save](#) [Separator](#)

Figure 2: NAT rules on pfSense

Firewall / Rules / WAN

FloatingWANLANDMZ

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✗ 0 / 244 KiB	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	
<input type="checkbox"/>	✓ 0 / 46 KiB	IPv4 TCP	*	*	192.168.138.7	80 (HTTP)	*	none		To Webserver in DMZ	
<input type="checkbox"/>	✓ 0 / 4 KiB	IPv4 ICMP any	WAN net	*	DMZ net	*	*	none		Allow ICMP from WAN to DMZ	
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 ICMP any	WAN net	*	LAN net	*	*	none		Allow ICMP from WAN to LAN	
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 TCP	*	*	192.168.138.7	443 (HTTPS)	*	none		NAT	
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 TCP	*	*	192.168.138.7	23 (Telnet)	*	none		NAT	
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 TCP	*	*	192.168.138.7	22 (SSH)	*	none		NAT	
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 TCP	*	*	192.168.138.7	21 (FTP)	*	none		NAT	
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 TCP	*	*	192.168.138.7	80 (HTTP)	*	none		NAT	
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 TCP	*	*	192.168.138.7	445 (MS DS)	*	none		NAT	
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 ICMP	*	*	192.168.138.7	*	*	none		NAT	

Add

Add

Delete

Save

Separator

Figure 3: Firewall rules on pfSense

B. Configure syslog on the pfSense Firewall

The pfSense firewall needs to be configured to forward logs to the Splunk application on central monitoring server for security investigation purposes. The pfSense firewall comes with syslog daemon which can be enabled to forward logs to remote syslog server.

1. On the pfSense firewall, enable remote logging through options *Status > System logs > Settings > Remote Logging Options*.
2. Enable the checkbox on **Send log messages to remote syslog server** and **Firewall events** as shown in Figure 4, and
3. Enter the IP address as **192.168.y.8** of your *Windows 2016 Server_DMZ*.

Remote Logging Options	
Enable Remote Logging	<input checked="" type="checkbox"/> Send log messages to remote syslog server
Source Address	<div>Default (any)</div> <p>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.</p> <p>NOTE: If an IP address cannot be located on the chosen interface, the daemon will bind to all addresses.</p>
IP Protocol	<div>IPv4</div> <p>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.</p>
Remote log servers	<div>192.168.138.8</div> <div>IP[:port]</div> <div>IP[:port]</div>
Remote Syslog Contents	<div><input type="checkbox"/> Everything</div> <div><input type="checkbox"/> System Events</div> <div><input checked="" type="checkbox"/> Firewall Events</div> <div><input type="checkbox"/> DNS Events (Resolver/unbound, Forwarder/dnsmasq, filterdns)</div> <div><input type="checkbox"/> DHCP Events (DHCP Daemon, DHCP Relay, DHCP Client)</div> <div><input type="checkbox"/> PPP Events (PPPoE WAN Client, L2TP WAN Client, PPTP WAN Client)</div> <div><input type="checkbox"/> Captive Portal Events</div> <div><input type="checkbox"/> VPN Events (IPsec, OpenVPN, L2TP, PPPoE Server)</div> <div><input type="checkbox"/> Gateway Monitor Events</div> <div><input type="checkbox"/> Routing Daemon Events (RADVD, UPnP, RIP, OSPF, BGP)</div> <div><input type="checkbox"/> Server Load Balancer Events (relayd)</div> <div><input type="checkbox"/> Network Time Protocol Events (NTP Daemon, NTP Client)</div> <div><input type="checkbox"/> Wireless Events (hostapd)</div>

Figure 4: Enabling remote logging on pfSense firewall

C. Configuring the Windows 10_DMZ for auditing

It is important to audit logon attempts to a host, especially the failure logon attempts as they help to understand about attacks such as brute force, dictionary, and other password-based attacks against Web server.

On the Windows 10_DMZ, go to **Run > gpedit.msc > Local Computer Policy > Computer Configuration > Windows Settings > Security Settings > Local Policies > Audit Policy** and enable *Failure* audit logon events as shown in Figure 5.

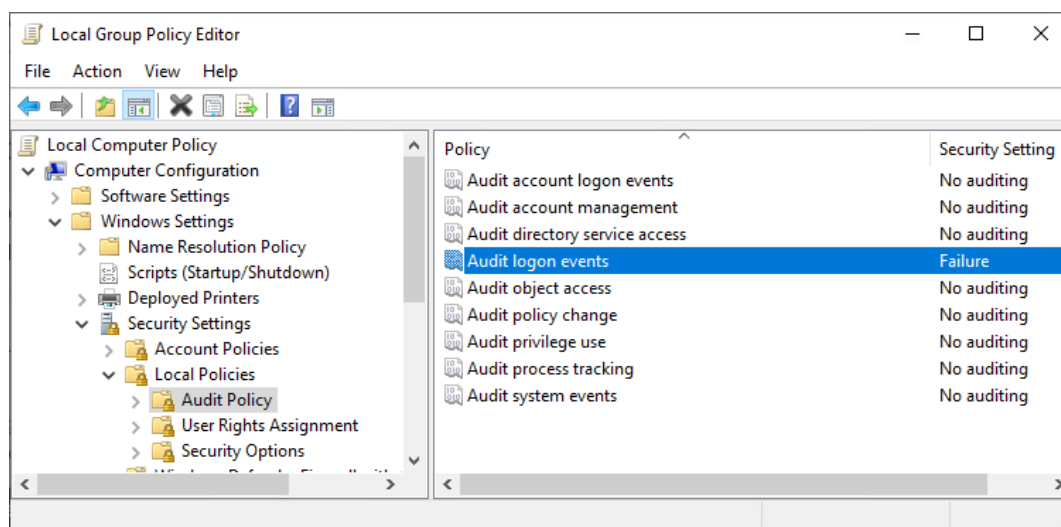


Figure 5: Audit Windows logon events using GPO Editor

In addition, the account lockout policy can be configured under **Windows Settings > Security Settings > Account Policies > Account Lockout Policy > Account lockout threshold** to disable a user account if the number of logon attempts exceeds some specified number of attempts.

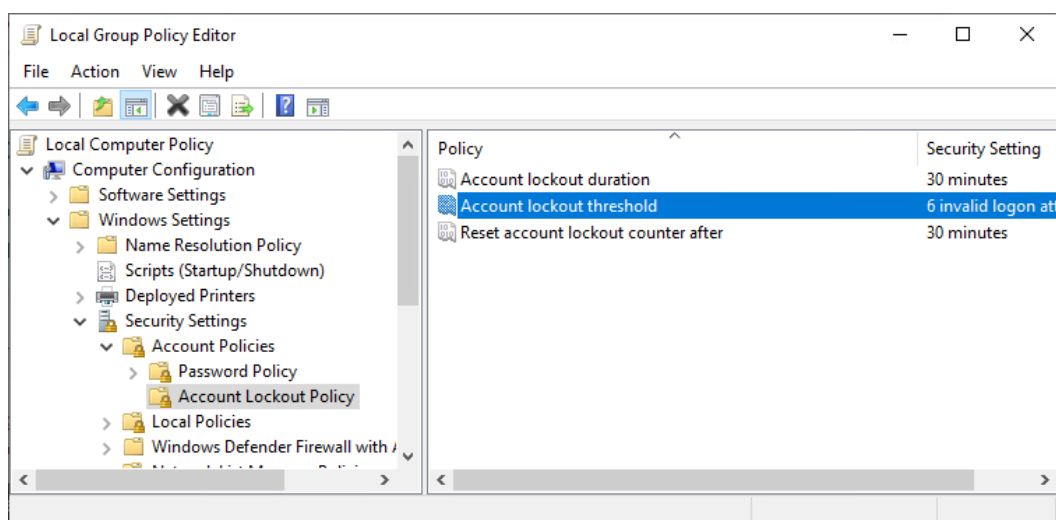


Figure 6: Account lockout threshold setting

D. Configure Snort to detect attacks on Web server

We can detect the presence of malicious activities on webserver using an agent-based Snort as IDS (Intrusion Detection System). The Snort agent is installed on the **Windows 10_DMZ**. Now go to the **C:\Snort\rules** folder and create a file (**rule.rules**) if not available with below details:

```
# Port scan
preprocessor sfportscan:\
  proto { all } \
  scan_type { all } \
  sense_level { high } \
  logfile { portscan.log }

# Bad logins
alert tcp any 21 -> any any (msg:"FTP Bad login"; content:"530 User "; nocase;
flow:from_server,established; sid:491;rev:5;)

# Telnet login
# alert tcp any any <> any 23 (flags:S; msg:"Telnet Login";sid:9000008;)
alert tcp any 23 -> any any (msg:"Telnet Invalid Login"; content:"Invalid Login";
sid:9000008;rev:1;)
alert tcp any 23 -> any any (msg:"Telnet Login -2 Welcome to Hadi Kiamarsi TELNET
Server"; content:"Welcome to Hadi Kiamarsi TELNET Server"; sid:9000009;rev:1;)

# DoS on Web server
alert tcp any any -> any 80 (msg:"DOS flood denial of service
attempt";flow:to_server; \
detection_filter:track by_dst, count 60, seconds 60; \
sid:25101; rev:1;)

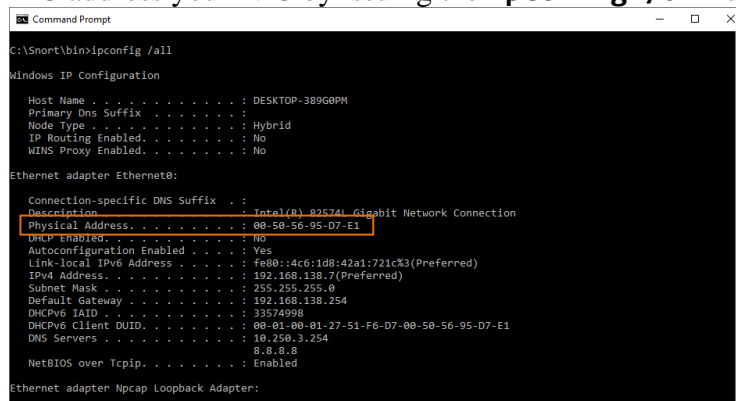
# ping sweep
alert icmp any any -> any any (msg:"ICMP Packet found";sid:9000000;)
alert icmp any any -> any any (itype: 0; msg: "ICMP Echo Reply";sid:9000001;)
alert icmp any any -> any any (itype: 3; msg: "ICMP Destination
Unreachable";sid:9000002;)
alert icmp any any -> any any (itype: 4; msg: "ICMP Source Quench Message
received";sid:9000003;)
alert icmp any any -> any any (itype: 5; msg: "ICMP Redirect message";sid:9000004;)
alert icmp any any -> any any (itype: 8; msg: "ICMP Echo Request";sid:9000005;)
alert icmp any any -> any any (itype: 11; msg: "ICMP Time Exceeded";sid:9000006;)

# Note you may have to add the following for the stream analysis
preprocessor stream5_global: track_tcp yes, \
  track_udp yes, \
  track_icmp no, \
  max_tcp 262144, \
  max_udp 131072, \
  max_active_responses 2, \
  min_response_seconds 5
preprocessor stream5_tcp: policy windows, detect_anomalies, require_3whs 180, \
  overlap_limit 10, small_segments 3 bytes 150, timeout 180, \
  ports_client 21 22 23 25 42 53 70 79 109 110 111 113 119 135 136 137 139 143 \
  161 445 513 514 587 593 691 1433 1521 1741 2100 3306 6070 6665 6666 6667 6668 6669 \
  7000 8181 32770 32771 32772 32773 32774 32775 32776 32777 32778 32779, \
  ports_both 80 81 82 83 84 85 86 87 88 89 90 110 311 383 443 465 563 591 593 631
636 901 989 992 993 994 995 1220 1414 1830 2301 2381 2809 \
  3037 3057 3128 3443 3702 4343 4848 5250 6080 6988 7907 7000 7001 7144 7145 7510
7802 7777 7779 \
  7801 7900 7901 7902 7903 7904 7905 7906 7908 7909 7910 7911 7912 7913 7914 7915
7916 \
  7917 7918 7919 7920 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180 8222
8243 8280 8300 8500 8800 8888 8899 9000 9060 9080 9090 \
  9091 9443 9999 10000 11371 34443 34444 41080 50000 50002 55555
preprocessor stream5_udp: timeout 180
```

E. Running Snort Program

When the Snort program is run using the detection rules located in **rule.rules** file as an input, it will log into the log folder within the directory where it runs, such as **c:\Snort\bin\log** directory (if we run Snort within c:\snort\bin). Using the following command, the alerts will be generated once the network traffic matches the defined Snort rule:

1. Find out the MAC address your NIC by issuing the **ipconfig /all** command in CMD



```
Command Prompt
C:\Snort\bin>ipconfig /all

Windows IP Configuration

Host Name . . . . . : DESKTOP-389G0PH
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

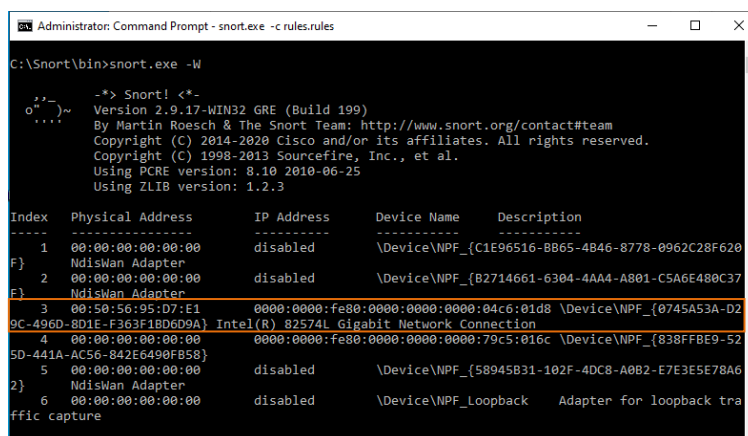
Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . . :
Description . . . . . : Intel(R) 82574L Gigabit Network Connection
Physical Address. . . . . : 00-50-56-95-D7-E1
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::4c6:1d8:42a1:721c%3(Prefered)
IPv4 Address. . . . . : 192.168.138.7(Prefered)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.138.254
DHCPv6 IAID . . . . . : 33579960
DHCPv6 Client DUID. . . . . : 00-01-00-01-27-51-F6-D7-00-50-56-95-D7-E1
DNS Servers . . . . . : 8.8.8.8
NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter Npcap Loopback Adapter:
```

Figure 7: The MAC address of the NIC

2. Look for the index of your NIC using the command, **C:\Snort\bin>snort -W**



```
Administrator: Command Prompt - snort.exe -c rules.rules
C:\Snort\bin>snort.exe -W

-*> Snort! <*-
Version 2.9.17-WIN32 GRE (Build 199)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2020 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using PCRE version: 8.10 2010-06-25
Using ZLIB version: 1.2.3

Index  Physical Address      IP Address      Device Name      Description
-----
1      00:00:00:00:00:00      disabled       \Device\NPF_{C1E96516-BB65-4B46-8778-0962C28F620}
F} NdisWan Adapter
2      00:00:00:00:00:00      disabled       \Device\NPF_{B2714661-6304-4AA4-A801-C5A6E480C37}
F} NdisWan Adapter
3      00:50:56:95:D7:E1      0000:0000:fe80:0000:0000:0000:04c6:01d8 \Device\NPF_{0745A53A-D2
9C-496D-8D1E-F363F18D6D9A} Intel(R) 82574L Gigabit Network Connection
4      00:00:00:00:00:00      0000:0000:fe80:0000:0000:0000:79c5:016c \Device\NPF_{838FFBE9-52
5D-441A-AC56-842E6490F850}
5      00:00:00:00:00:00      disabled       \Device\NPF_{58945831-102F-4DC8-A0B2-E7E3E5E78A6}
2} NdisWan Adapter
6      00:00:00:00:00:00      disabled       \Device\NPF_Loopback Adapter for loopback tra
ffic capture
```

Figure 8: The index of the NIC

3. Start Snort to monitor your NIC using the command, **C:\Snort\bin>snort -dev -i 3 -p -k none -c C:\Snort\rules\rule.rules**

Snort will store its alerts in the **alerts.ids** file into the **log** folder below where you run it from. Make a note of the place that Snort will save its file to:

F. Splunk forwarder on Windows 10_DMZ

The Windows 10_DMZ's Web Server is accessible to the public network, and it additionally runs services such as FTP, Telnet and others. It is well known that storing logs on the public facing server is not secure as they are prone to attacks. Hence, the security logs need to be forwarded to another preferably management server with limited user access and more security configuration.

The Splunk SIEM provides a free forwarder tool which can be utilised to forward logs from multiple remote systems to the Splunk indexing and consolidation system. In our case, the **Windows 10_DMZ** has had an installed Splunk forwarder instance yet.

You can find the Splunk forwarder from **C:\Users\Napier\Desktop\IR&MA_Tools\Splunk forwarder** and install it.

1. Double click and run the Splunk forwarder installation
2. Select **Customise Options** (Figure 9) and

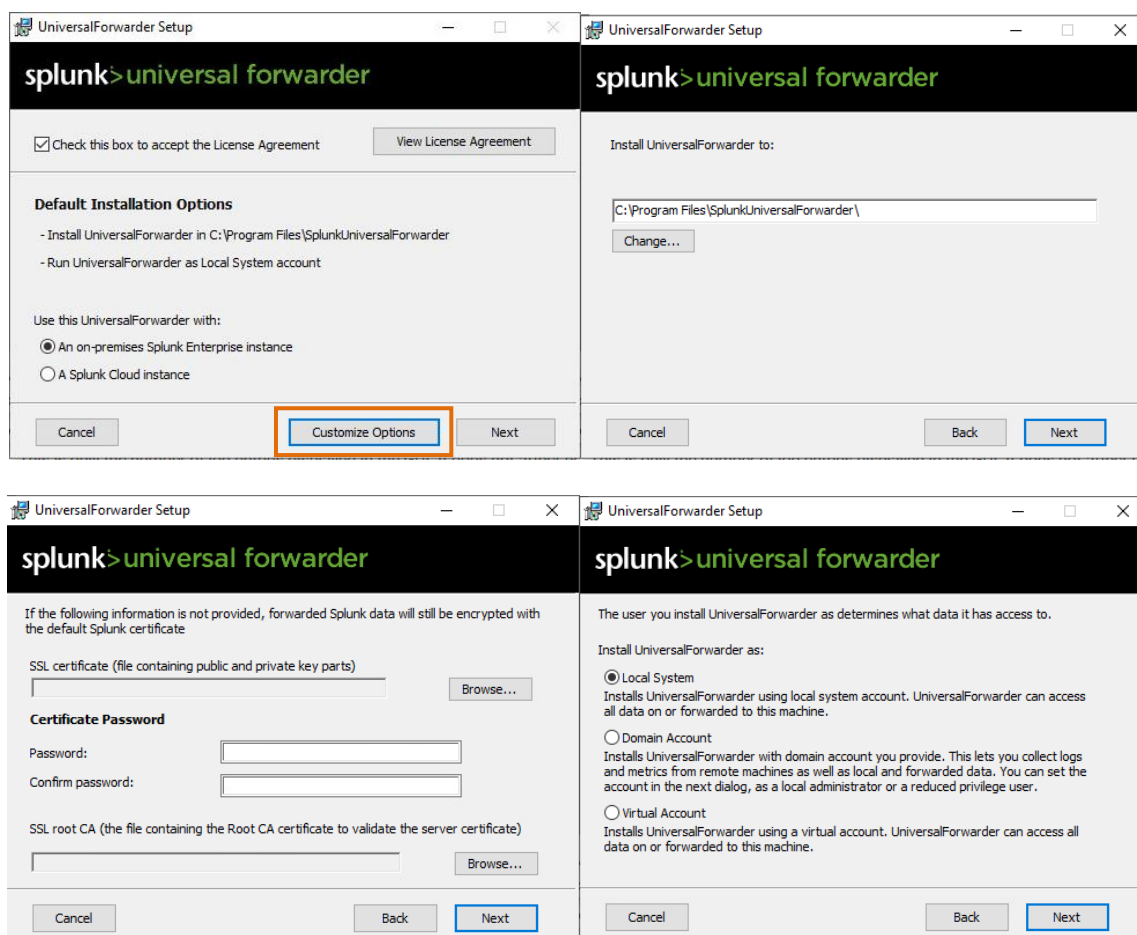


Figure 9: Setup of Splunk forwarder

3. Then select Windows Events logs options, and the **Path to Monitor** to the place where the **alert.ids** file is stored as shown in Figure 10. The filename will be the name of the alert.ids file that we defined in the previous section. For example, if you run it in

c:\snort\bin, then alert.ids will be stored in c:\snort\bin\log\alert.ids.

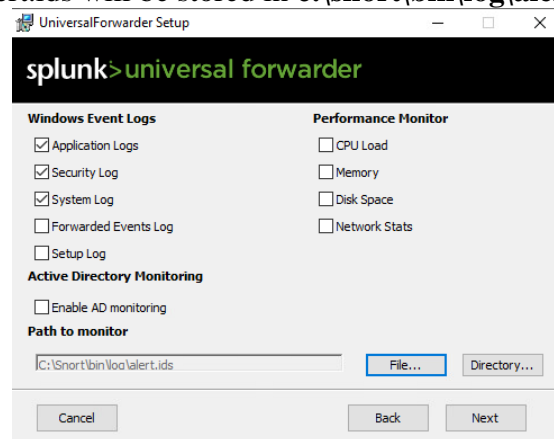


Figure 10: Select Windows Events logs and Path to Monitor

4. Create credentials (Username: napier, Password: napier123) for the administrator account as shown in Figure 11.

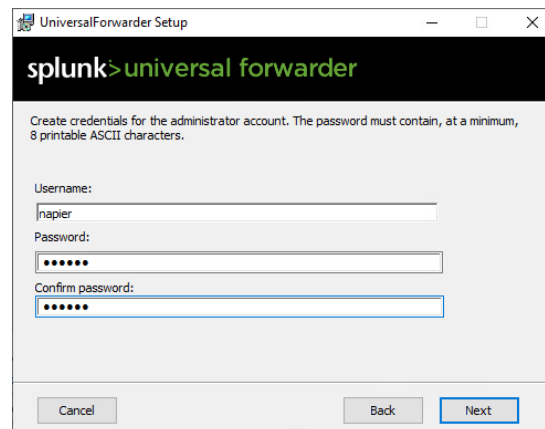


Figure 11: Create credentials

5. Now, the Splunk forwarder running on the Windows 10_DMZ is configured to collect Windows audit logs and Snort logs from the local system. In the next step, the forwarder needs to be configured to forward logs to the Splunk program running on the management server / Windows 2016 Server_DMZ.
6. Finally, skip the setting for Deployment Server and process with the setup of Receiving Indexer at your Windows 2016 Server_DMZ (192.168.y.8) on port 9997 (Figure 12).

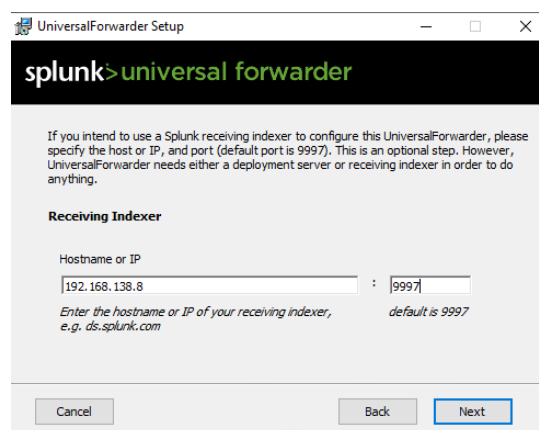
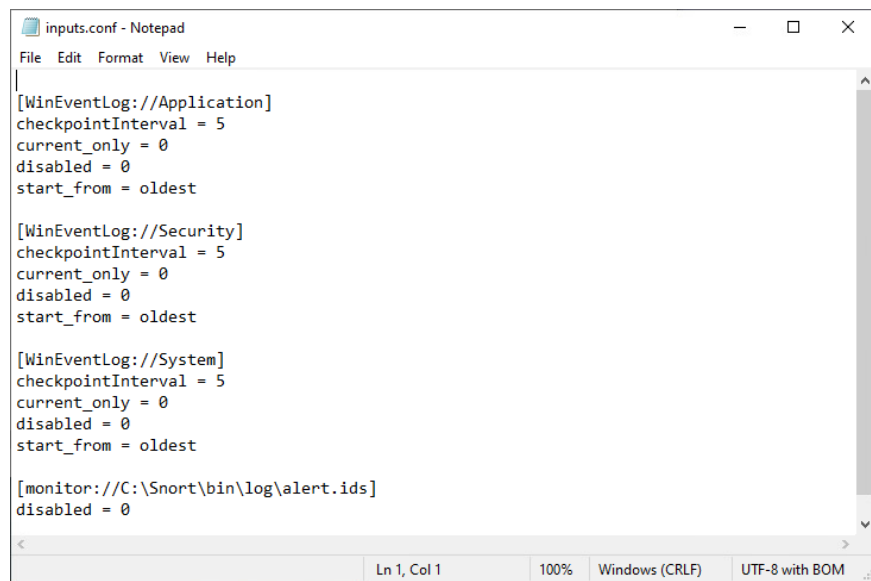


Figure 12: Set up Receiving Indexer

7. Open the **inputs.conf** file located in the directory
“C:\Program Files\SplunkUniversalForwarder\etc\apps\SplunkUniversalForwarder\local\”
and check if **disabled** is set to **0**, as shown in Figure 13.



```
inputs.conf - Notepad
File Edit Format View Help

[WinEventlog://Application]
checkpointInterval = 5
current_only = 0
disabled = 0
start_from = oldest

[WinEventlog://Security]
checkpointInterval = 5
current_only = 0
disabled = 0
start_from = oldest

[WinEventlog://System]
checkpointInterval = 5
current_only = 0
disabled = 0
start_from = oldest

[monitor://C:\Snort\bin\log\alert.ids]
disabled = 0

Ln 1, Col 1    100%    Windows (CRLF)    UTF-8 with BOM
```

Figure 13: Inputs.conf

G. Configure Splunk on Windows 2016 Server to receive Windows 10 audit logs, Snort alerts and pfSense syslog

In order to receive the logs forwarded by the Splunk forwarder running on the **Windows 10_DMZ** and **pfSense** syslog daemon, the Splunk application needs to be configured to receive data as shown in Figures 14 and 15.

First, the Splunk server needs to be configured to receive data from the **Windows 10_DMZ** for audit logs

- Use the Receive Data under the **Settings > Forwarding and receiving > Configure receiving > Add new > 9997**.

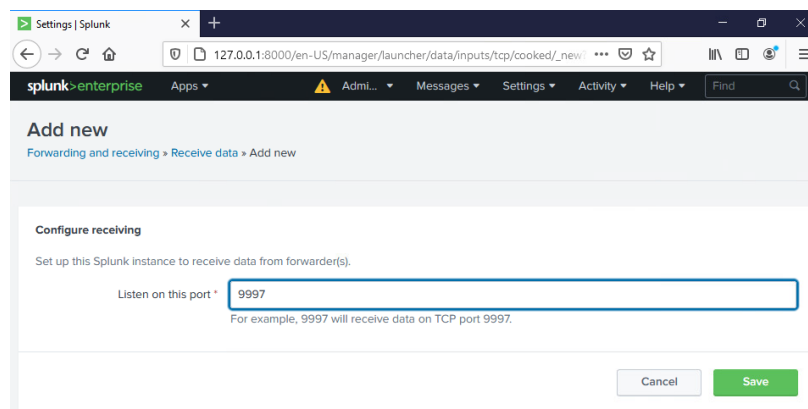


Figure 14: Configure listen on port 9997 for receiving forwarder logs

Once the Windows audit logs are generated, they can be seen on the Splunk application. Similarly, in case of any alert got generated while running Snort they can be seen using the Splunk web interface. In addition, the Snort app can be used to check statistics using its built-in search commands.

Next, the Splunk server needs to be configured to receive data from the **pfSense** firewall.

- Use **Settings > Data Inputs > Local inputs > UDP > New**. Enter Port 514 and then press **Next** button. As shown in Figure 15, type in “pfsense_pf” for sourcetype. This is important as this requests the pfSense add-on app installed on Splunk to format the received pfSense data.

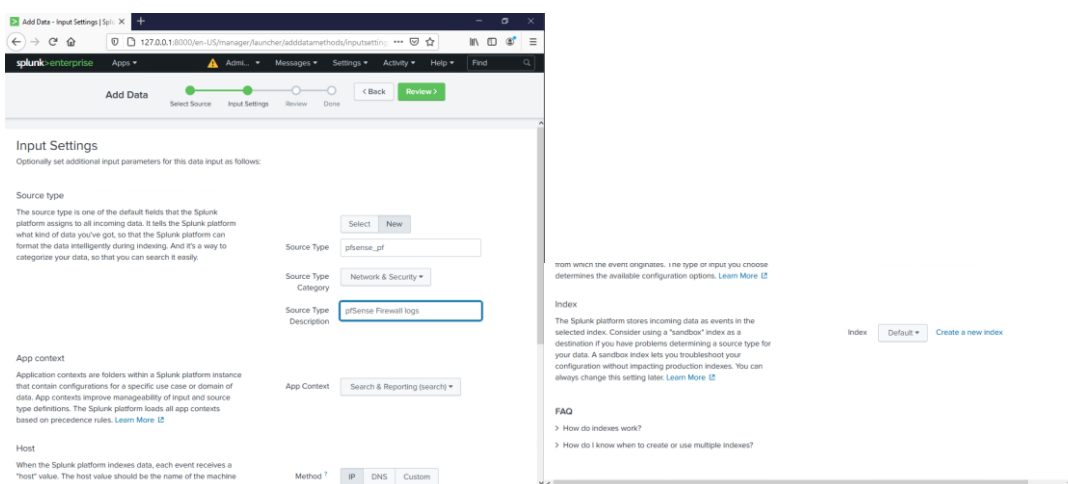


Figure 15: Add new local pfSense firewall input

Review

Input Type UDP Port
Port Number 514
Source name override N/A
Restrict to Host N/A
Source Type pfsense_pf
App Context search
Host (IP address of the remote server)
Index default

Figure 16: New input summary

H. Perform an assessment of the Splunk configuration

Now, perform an assessment to verify the configuration of Splunk Enterprise. **Windows 10_DMZ**, **Bodhi_Linux_Private** and **Bodhi_Linux_Public** will be used in this task. Before the assessment, please make sure Snort is running on your **Windows 10_DMZ**. (Be aware that the Snort alerts will be written into alert.ids after the Snort stops, and the updates will then be forwarded to Splunk Enterprise on Windows 2016 Server_DMZ by the Splunk forwarder.)

Then, use the Splunk searching skills that you have learnt from Lab 04-1 to complete the tasks 1 to 6 below. There are 5 **sourcetypes** that you could use in your search.

- sourcetype = ids
- sourcetype="WinEventLog:Security"
- sourcetype="WinEventLog:Application"
- sourcetype="WinEventLog:System"
- sourcetype=pfsense_pf

[Tips: If you do not see any alerts, please first check if the host firewall on your Windows 2016 Server_DMZ has been configured to allow the traffic, addressed to ports 514 and 9997, to pass through.]

1. The Snort rule should detect a login to **Telnet** into the **Windows 10_DMZ**. From a host on your network, Telnet into the **Windows 10_DMZ** and check that alerts appear in the Splunk interface.

Outline how you observe from Splunk

2. The Snort rule should detect a **bad login** into **FTP** (Username: Napier, Password: napier) on the **Windows 10_DMZ**. Login into the FTP server using a valid login and an invalid one.

Outline how you observe from Splunk:

3. The Snort rule should detect a **Ping** on the **Windows 10_DMZ**, so test it with pings from a host on your network.

Outline how you observe from Splunk:

4. The Snort rule should detect a **port scan** on the **Windows 10_DMZ**. Perform an **NMAP** scan (`nmap -sV 192.168.y.7`) and see if Splunk will detect it.

Outline how you observe from Splunk:

5. The Snort rule should detect DoS traffic against the **Windows 10_DMZ**. From the **Bodhi_Linux_Private**, test using **Hping** against the **Windows 10_DMZ**.

Outline how you observe from Splunk:

6. The Snort rules should detect a **port scan** on the host. Now open-up your firewall to allow all TCP ports to be allowed from the WAN to your **Windows 10_DMZ** (which you have done in Task A). Next, use **NMAP** to perform a port scan of your **Windows 10_DMZ**, from your **Bodhi_Linux_Public**. The NMAP traffic should address to the **WAN port** of the pfSense firewall, on which ports have been mapped to the responding ports of **Windows 10_DMZ**.

Outline how you observe from Splunk:

7. Check if you the alerts and logs sent from **pfSense** and your **Windows 10_DMZ**.

Outline how you observe from Splunk:

I. Red v Blue

We will now do a basic Red v Blue exercise. If you are in a lab, ask your neighbour what IP address they have mapped their **Windows 10_DMZ** to (which is their **WAN address**). If you are studying remotely, see if you can “buddy” up with another distance student (or ask your tutor to test your setup).

Now ask them to monitor the Splunk interface. Perform the following, but do it in a random order, and ask your neighbour to identify you when they see a trace:

1. Ping their server. Did your neighbour correctly identify it?
2. NMAP their server. Did your neighbour correctly identify it?
3. Login into their Telnet server. Did your neighbour correctly identify it?
4. Create an incorrect FTP login. Did your neighbour correctly identify it?
5. NMAP their server. Did your neighbour correctly identify it?

J. Splunk

Using Splunk at <https://asecuritysite.com:8000> determine the following. You will be allocated a login.

Now go to: <http://asecuritysite.com/tests/tests?sortBy=siem> for the test.

Some tests on the asecuritysit.com are password protected. To access them please use the following credential.

- Username: napier
- Password: napier