Lab 5: SIEM

The aim of this lab is to configure logging on network and host-based devices such as Pfsense firewall and Windows 2003 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.

Our first activity is to configure the pfSense firewall as performed in the previous labs to setup network connection. In the lab you will be provided
with network group in which you can select the LAN 192.168.x.0/24 and DMZ IP addresses 192.168.y.0/24 for configuration as shown in Figure 1.

Demo: https://youtu.be/Nla6ZDheBkU

The allocation of IP addresses is defined as Allocation A in:

http://asecuritysite.com/csn11128/nets

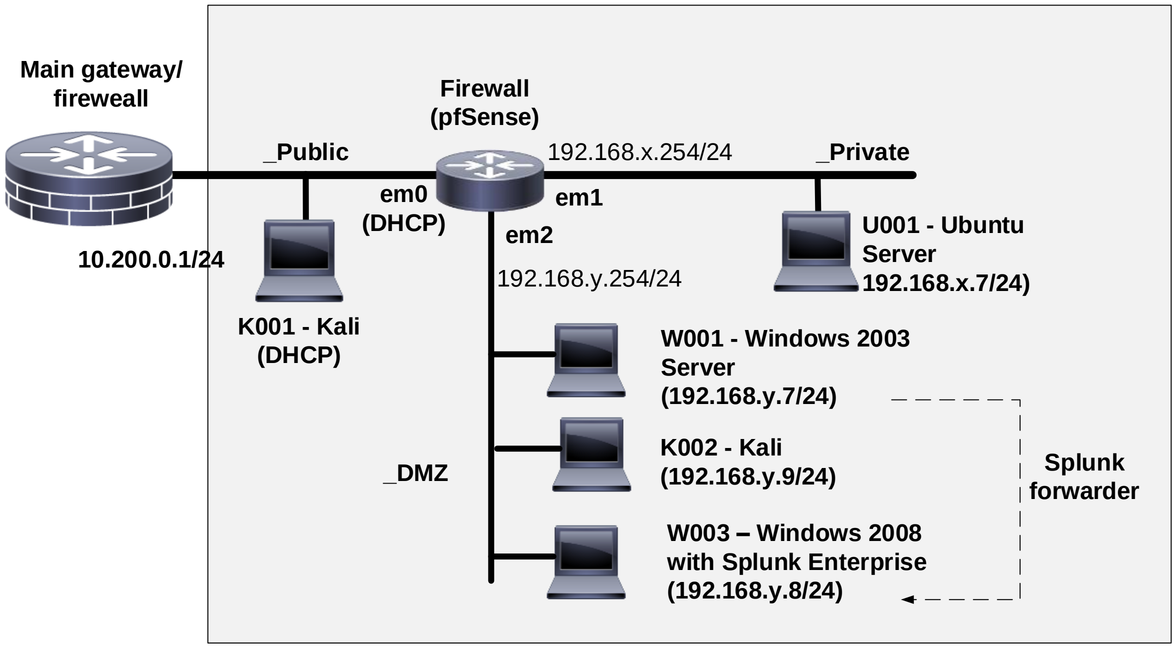
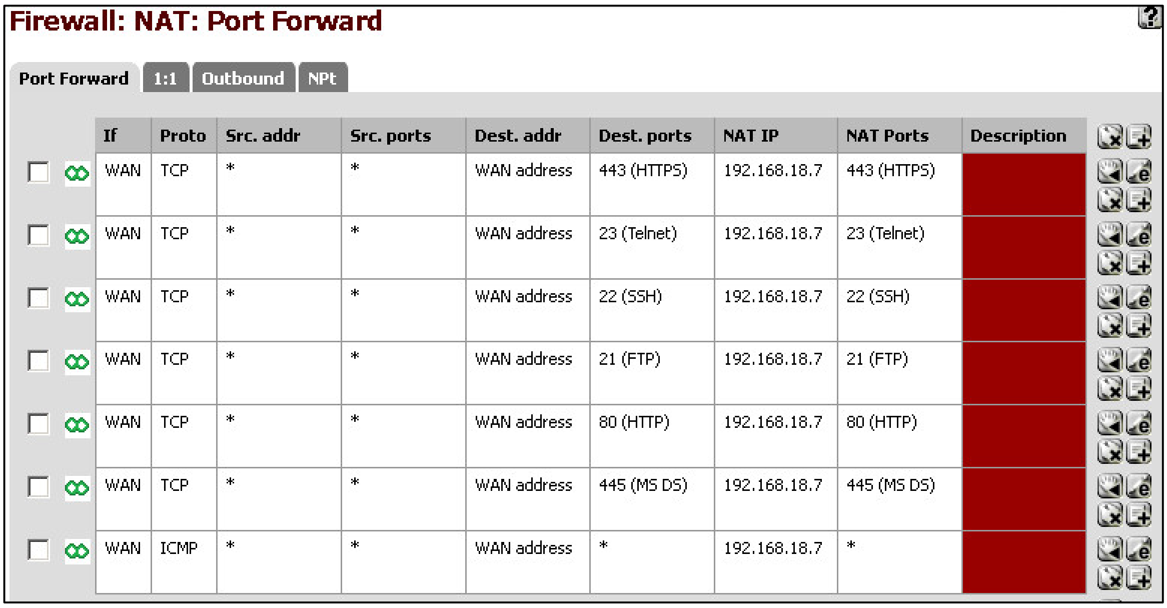

Main gateway/ fireweall
10.200.0.1/24
_Public
Firewall (pfSense)
em0 (DHCP)
em1
em2
192.168.x.254/24
_Private
192.168.y.254/24
U001 - Ubuntu Server 192.168.x.7/24)
K001 - Kali (DHCP)
W001 - Windows 2003 Server (192.168.y.7/24)
K002 - Kali (192.168.y.9/24)
_DMZ
W003 – Windows 2008 with Splunk Enterprise (192.168.y.8/24)
Splunk forwarder

Figure 1 : Lab infrastructure setup

Login credentials Passwords for Virtual Machines:

PfSense:	User:admin, Password:pfsense
Ubuntu:	User: napier, password: napier123
Windows 2003:	User: Administrator, Password: napier
Windows 2008:	User: Administrator, Password: Ankle123
Kali:	User: root, password: toor

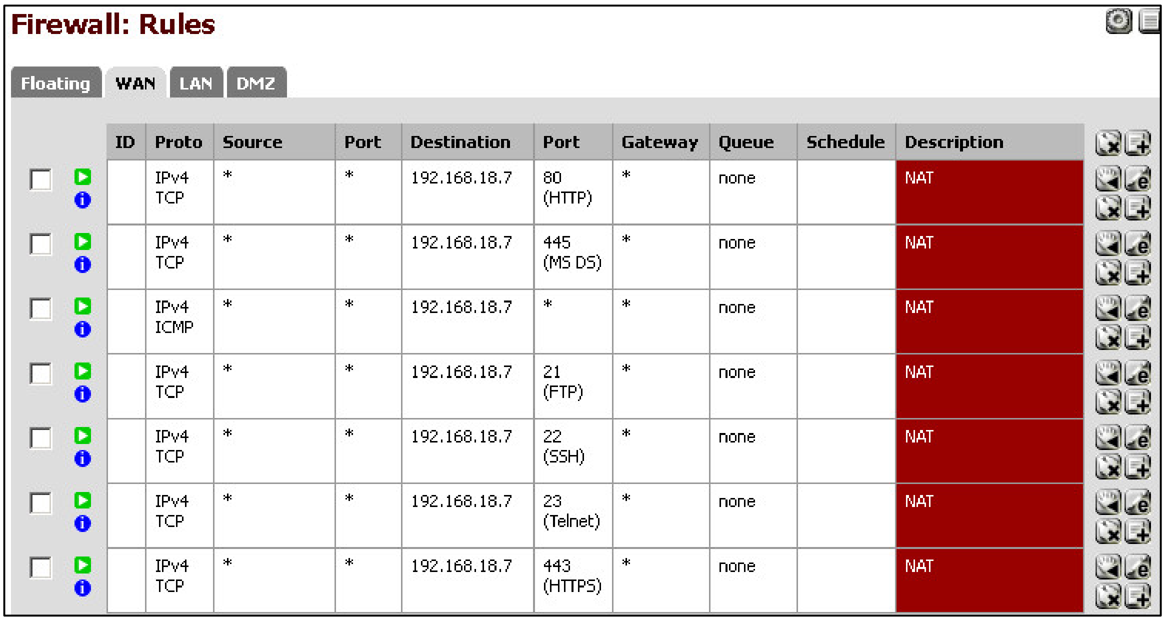
Configure pfSense using NAT port forwarding to the Windows 2003 server inside the DMZ and make sure to check the firewall rules to enable logging on each rule. Figure 2 and 3 shows the screenshot of how the rules look when they are configured.



Firewall: NAT: Port Forward

If	Proto	Src. addr	Src. ports	Dest. addr	Dest. ports	NAT IP	NAT Ports	Description
WAN	TCP	*	*	WAN address	443 (HTTPS)	192.168.18.7	443 (HTTPS)	
WAN	TCP	*	*	WAN address	23 (Telnet)	192.168.18.7	23 (Telnet)	
WAN	TCP	*	*	WAN address	22 (SSH)	192.168.18.7	22 (SSH)	
WAN	TCP	*	*	WAN address	21 (FTP)	192.168.18.7	21 (FTP)	
WAN	TCP	*	*	WAN address	80 (HTTP)	192.168.18.7	80 (HTTP)	
WAN	TCP	*	*	WAN address	445 (MS DS)	192.168.18.7	445 (MS DS)	
WAN	ICMP	*	*	WAN address	*	192.168.18.7	*	

Figure 2: NAT rules on pfSense



Firewall: Rules

ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
	IPv4 TCP	*	*	192.168.18.7	80 (HTTP)	*	none		NAT
	IPv4 TCP	*	*	192.168.18.7	445 (MS DS)	*	none		NAT
	IPv4 ICMP	*	*	192.168.18.7	*	*	none		NAT
	IPv4 TCP	*	*	192.168.18.7	21 (FTP)	*	none		NAT
	IPv4 TCP	*	*	192.168.18.7	22 (SSH)	*	none		NAT
	IPv4 TCP	*	*	192.168.18.7	23 (Telnet)	*	none		NAT
	IPv4 TCP	*	*	192.168.18.7	443 (HTTPS)	*	none		NAT

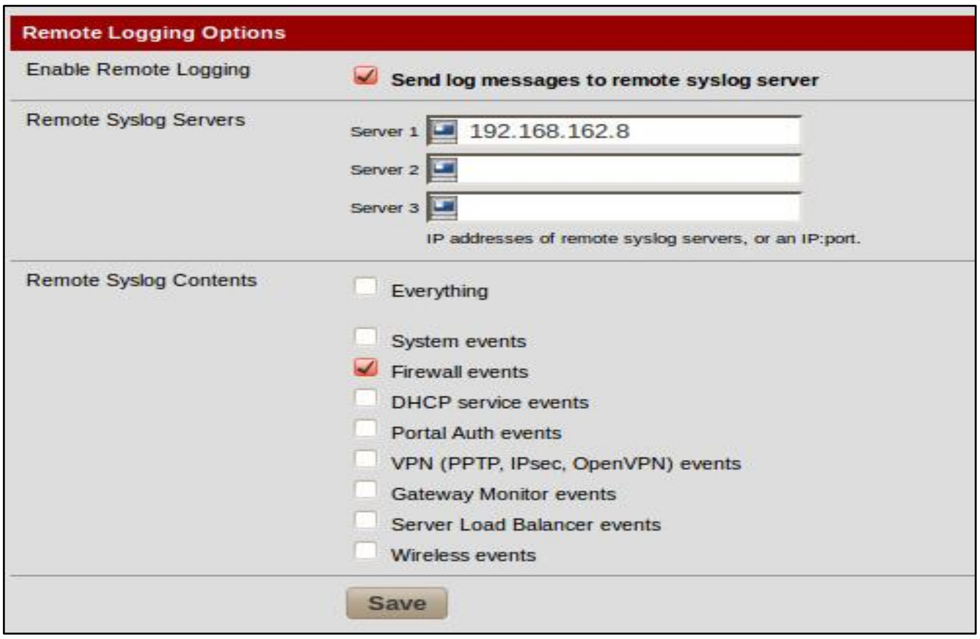
Figure 3: Firewall rules on pfSense

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.

On the Pfsense firewall enable remote logging through options ***Status* -> *System logs* -> *Settings* -> *Remote Logging Options***. Enable the checkbox on **Send log messages to remote**

syslog server and **Firewall events** as shown below and enter the IP address as 192.168.y.8 of your Windows 2008 server.



Remote Logging Options

Enable Remote Logging: ☑ Send log messages to remote syslog server

Remote Syslog Servers:
Server 1: 192.168.162.8
Server 2:
Server 3:
IP addresses of remote syslog servers, or an IP:port.

Remote Syslog Contents:
□ Everything
□ System events
☑ Firewall events
□ DHCP service events
□ Portal Auth events
□ VPN (PPTP, IPsec, OpenVPN) events
□ Gateway Monitor events
□ Server Load Balancer events
□ Wireless events

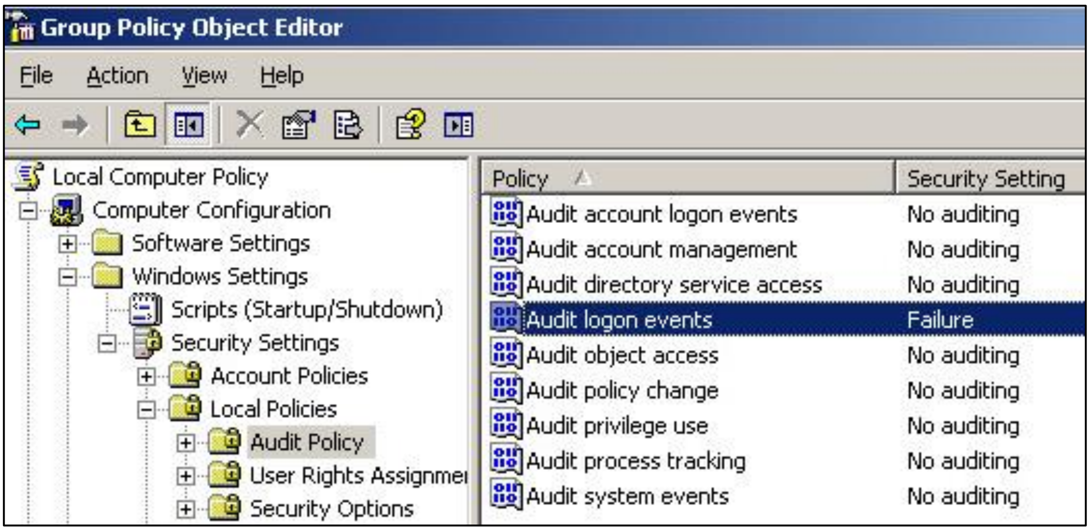
Figure 4 : Enabling remote logging on pfSense firewall

Configuring the Windows 2003 Server for auditing

The aim of this lab is to configure logging on network and host---based devices such as Pfsense firewall, Snort intrusion detection system, and Windows 2003 server. Similarly, to configure the Splunk SIEM application to receive logs from above mentioned devices for security monitoring and incident investigation purposes.

It is important to audit logon attempts to Server 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 2003 Server go to **Run -> gpedit.msc -> Windows Settings -> Local Policies -> Audit Policy** and enable Failure audit logon events as shown below in the Figure 5.

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.



Policy	Security Setting
Audit account logon events	No auditing
Audit account management	No auditing
Audit directory service access	No auditing
Audit logon events	Failure
Audit object access	No auditing
Audit policy change	No auditing
Audit privilege use	No auditing
Audit process tracking	No auditing
Audit system events	No auditing

Figure 5: Audit Windows logon events using GPO Editor

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 2003 server. Now go to the C:\Snort\rules folder and create a file (rule.rules) if not available with below details:

Get the file [http://asecuritysite.com/blue.txt]

```
# 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:9000005;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
```

Running Snort Program

When the Snort program is run using the detection rule file located at rule.rules as input, it will log into the log folder below the place it is run, 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:

```
C:\Snort\bin> snort -dev -i 1 -p -K ascii -c 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:

Splunk forwarder on Windows 2003 Server

The Windows 2003 Web Server is accessible to the public network and additionally runs other services such as FTP, Telnet and other services. 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 server preferably management server with limited user access and more security configuration.

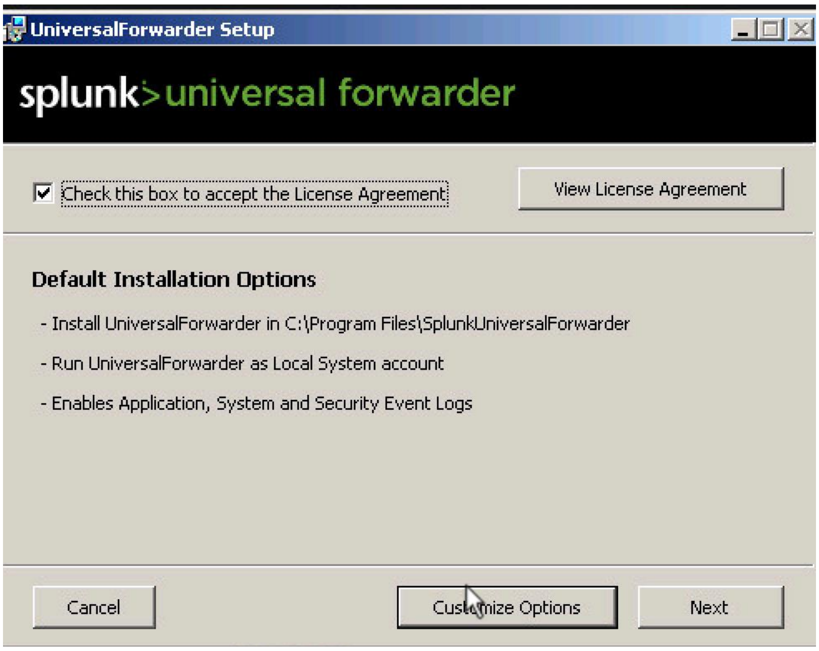
The Splunk SIEM provides a free forwarder tool which can be utilised to forward logs from multiple remote systems to the Splunk indexing and consolidation system. In our case the Windows 2003 Server does not contain Splunk forwarder instance installed. You can download and install the Splunk forwarder from the link provided below:

```
https://enusec.org/cyber/splunk-forwarder.msi
```

Now, the Splunk forwarder running on the Windows 2003 Server 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 2008 server.

Select ***Customise Options*** (Figure 6) and then select Windows Events logs options, and also the ***Path to Monitor*** to the place where the alert.ids file is stored (Figure 7). 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.

Finally setup the Receiving Indexer at your Windows 2008 server (192.168.y.8) on port 9997 (Figure 8).

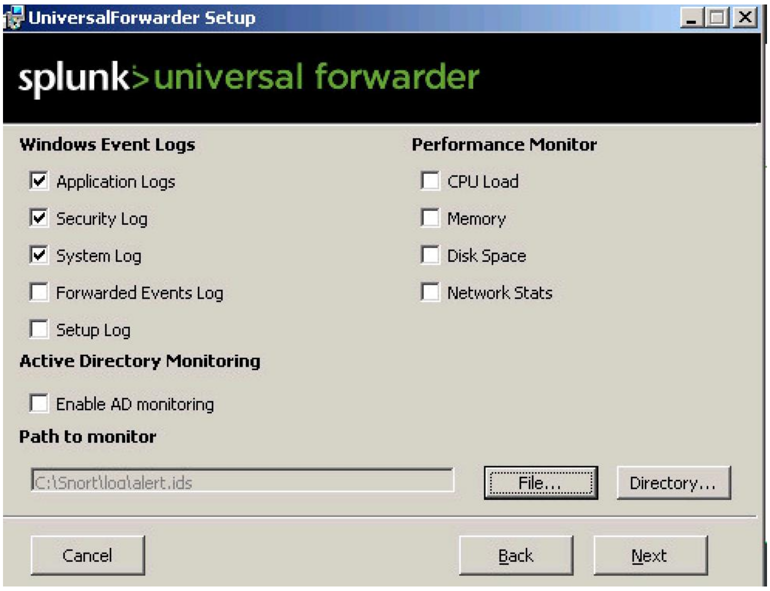


☑ Check this box to accept the License Agreement

Default Installation Options

- Install UniversalForwarder in C:\Program Files\SplunkUniversalForwarder
- Run UniversalForwarder as Local System account
- Enables Application, System and Security Event Logs

Figure 6: Setup of Splunk forwarder



Windows Event Logs

☑ Application Logs
☑ Security Log
☑ System Log
□ Forwarded Events Log
□ Setup Log

Performance Monitor

□ CPU Load
□ Memory
□ Disk Space
□ Network Stats

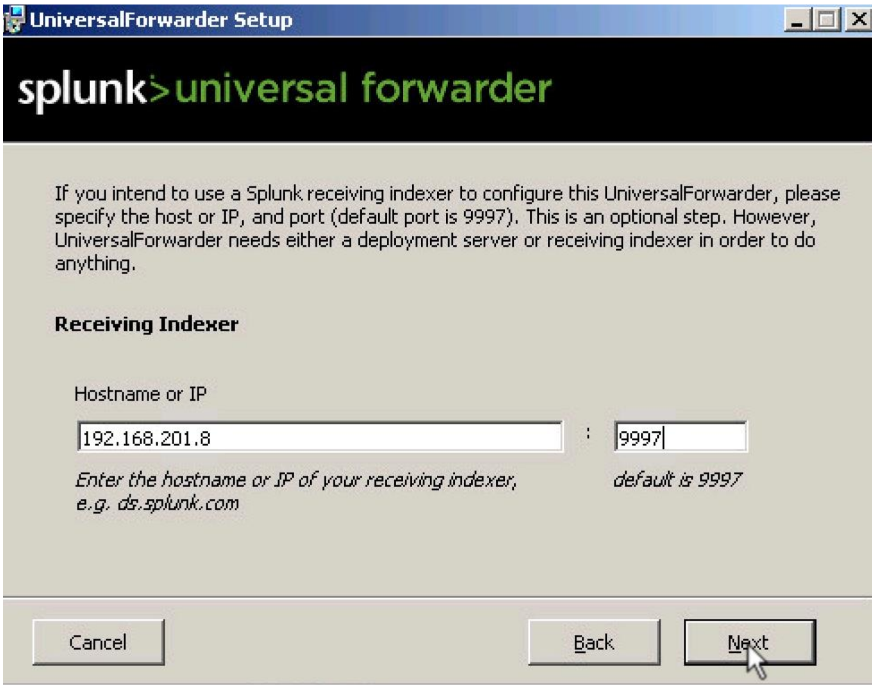
Active Directory Monitoring

□ Enable AD monitoring

Path to monitor

C:\Snort\log\alert.ids

Figure 7: Setup of Splunk forwarder



If you intend to use a Splunk receiving indexer to configure this UniversalForwarder, please specify the host or IP, and port (default port is 9997). This is an optional step. However, UniversalForwarder needs either a deployment server or receiving indexer in order to do anything.

Receiving Indexer

Hostname or IP: 192.168.201.8 : 9997

Enter the hostname or IP of your receiving indexer, e.g. ds.splunk.com

default is 9997

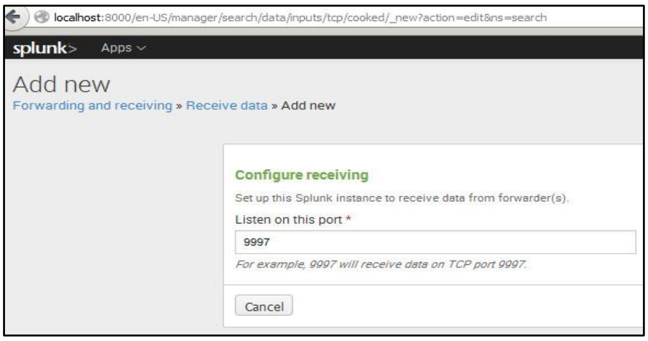
Figure 8: Setup of Splunk forwarder

Configure Splunk on Windows 2008 to receive Windows 2003 audit logs, Snort alerts and PfSense syslog

In order to receive the logs forwarded by the Splunk forwarder running on the Windows 2003 Server and pfSense syslog daemon. The Splunk application needs to be configured to receive data. For example, use the Receive Data under the ***Settings -> Forwarding and receiving -> Configure receiving -> Add new -> 9997***.

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 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 -> New -> UDP***. Enter port 514 and for sourcetype select as “pfsense_pf”. This is important as this request the pfSense add-on app installed on Splunk to format the received PfSense data.


localhost:8000/en-US/manager/search/data/inputs/tcp/cooked/_new?action=edit&ns=search

Add new

Forwarding and receiving » Receive data » Add new

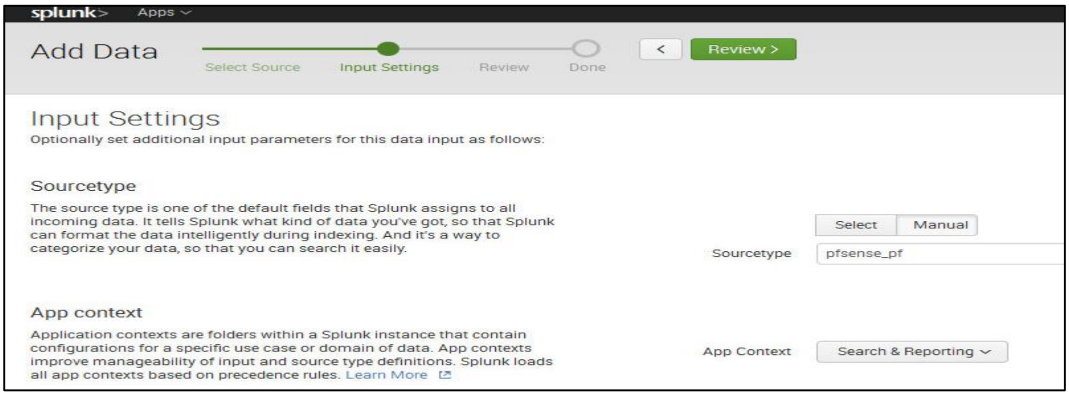
Configure receiving

Set up this Splunk instance to receive data from forwarder(s).

Listen on this port *: 9997

For example, 9997 will receive data on TCP port 9997.

Figure 9: Configure listen on port 9997 for receiving forwarder logs



Input Settings

Optionally set additional input parameters for this data input as follows:

Sourcetype

The source type is one of the default fields that Splunk assigns to all incoming data. It tells Splunk what kind of data you've got, so that Splunk can format the data intelligently during indexing. And it's a way to categorize your data, so that you can search it easily.

Select | Manual

Sourcetype: pfsense_pf

App context

Application contexts are folders within a Splunk instance that contain configurations for a specific use case or domain of data. App contexts improve manageability of input and source type definitions. Splunk loads all app contexts based on precedence rules. Learn More

App Context: Search & Reporting

Figure 10: Listen on a UDP port for incoming syslog data

Perform the assessment

1. The Snort rule should detect a login to Telnet into the Windows 2003 server. From a host on your network, log into the Windows 2003 server, and check that it appears in the Splunk interface.

Outline how you observe from Splunk:

2. The Snort rule should detect a bad login into FTP on Windows 2003. Login into FTP 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 2003 computer, so test it with a ping.

Outline how you observe from Splunk:

4. The Snort rule should detect a port scan on the Windows 2003 server. Perform an NMAP scan, and see if Splunk will detect it.

Outline how you observe from Splunk:

5. The Snort rule should detect a DoS against the Windows 2003. Test using hping against the Windows 2003.

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 2003 host. Next, using NMAP, perform a port scan of your Windows 2003 server, from your Kali host.

Outline how you observe from Splunk:

Red v Blue

We will now do a basic Red v Blue exercise. If you are in a lab, ask your neighour what IP address they have mapped their Windows 2003 server 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 you neighour correctly identify it?
2. NMAP their server. Did you neighour correctly identify it?
3. Login into their Telnet server. Did you neighour correctly identify it?
4. Create an incorrect FTP login. Did you neighour correctly identify it?
5. NMAP their server. Did you neighour correctly identify it?

M Splunk

Using Splunk at **http:// 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.