Blue Team Playbook

198 Foxwell Road
Coomera QLD 4209 Australia

SERVICES PROVIDED

The Blue Team is responsible for providing guidance and make improvements to identify and stop sophisticated types of attacks and threats with the following scopes:

1. Assess the company’s capabilities to identify and determine impacts of cyber threats/attacks and implement recovery procedures in a time manner.

2. Assess effectiveness of the organization incident reporting as well as analysis for recognition and remediation of anomalies.

3. Determine the success of the attack.

4. Expose and correct weakness in the network infrastructure.

5. Update and highlight gaps in policies and procedures.

6. Develop a contingency plan.

7. Actions /reactions of services’ downtimes.

8. Develop a mitigation/recovery plan considering possible loss of IT services and systems.

Objectives

- Understand every phase of an incident and respond appropriately.

- Identify suspicious traffic patterns and analyse alerts to accurately differentiate and escalate real threats from false positives.

- Use forensic methods and tools on targeted systems.

Methods

- Perform traffic and data analysis (WireShark)
- Review and analyse logs (Splunk)
- Utilise SIEM technology (Splunk) for visibility and detection of intrusion in real-time
- Apply a SPAN (Switched Port Analyzer) feature on switches to mirror a copy of the network traffic going through the switch to a monitoring device.

RESPONSE HANDLING PLAN

This playbook is based on the NIST Cybersecurity Framework[1].

Identify

Scanning & vulnerabilities:

NMAP	
Ping sweep for network:	# nmap -sn -PE <IP ADDRESS OR RANGE>
Scan and show open ports:	# nmap --open <IP ADDRESS OR RANGE>
Determine open services:	# nmap -sV <IP ADDRESS>
Scan two common TCP ports, HTTP and HTTPS:	# nmap -p 80,443 <IP ADDRESS OR RANGE>
Scan common UDP port, DNS:	# nmap -sU -p 53 <IP ADDRESS OR RANGE>
Scan UDP and TCP together, be verbose on a single host and include optional skip ping:	# nmap -v -Pn -SU -ST -p U:53,111,137,T:21-25,80,139,8080 <IP ADDRESS>

Protect

Disable/stop services:

Get a list of services and disable or stop at Windows
C:\> sc query

[1] Reference: http://www.nist.gov/cyberframework/

C:\> sc config "<SERVICE NAME>" start= disabled
C:\> sc stop "<SERVICE NAME>"
C:\> wmic service where name='<SERVICE NAME>' call ChangeStartmode Disabled

Linux	
Services information:	# service --status-all # ps -ef # ps -aux
Get a list of upstart jobs:	# initctl list
List all Upstart services:	# ls /etc/init/*,conf
Show if a program is managed by upstart and the process ID:	# status ssh
If not managed by upstart:	# update-rc.d apache2 disable # service apache2 stop

System firewalls:

Windows	
Show all rules:	C:\> netsh advfirewall firewall show rule name=all
Set firewall on/off:	C:\> netsh advfirewall set currentprofile state on C:\> netsh advfirewall set currentprofile firewallpolicy blockinboundalways,allowoutbound C:\> netsh advfirewall set publicprofile state on C:\> netsh advfirewall set privateprofile state on C:\> netsh advfirewall set domainprofile state on C:\> netsh advfirewall set allprofile state on C:\> netsh advfirewall set allprofile state off
Setup togging location:	C:\> netsh advfirewall set currentprofile logging C:\<LOCATION>\<FILE NAME>
Display firewall logs:	PS C:\> Get-Content $env:systemroot\system32\LogFiles\Firewall\pfirewall .log

Linux	
Become root user	# sudo su
Delete all current firewall rules	# iptables –F

Block all connections:	# iptables -P INPUT DROP # iptables -P OUTPUT DROP # iptables -P FORWARD DROP
Log all denied iptables rules:	# iptables -I INPUT 5 -m limit --limit 5/min -j LOG --log-prefix "iptables denied: " --log-level 7
Save all current iptables rules:	# /etc/init.d/iptables save # /sbin/service iptables save
List all current iptables rules:	# iptables -L
Start/Stop ufw service:	# ufw enable # ufw disable
Start/Stop ufw logging:	# ufw logging on # ufw logging off
Backup all current ufw rules:	# cp /lib/ufw/{user.rules,user6.rules} /<BACKUP LOCATION> # cp /lib/ufw/{user.rules,user6.rules} ./

Passwords:

Windows	

Change password:	C:\> net user <USER NAME> * /domain
	C:\> net user <USER NAME> <NEW PASSWORD>

Change password remotely:	C:\> pspasswd.exe \\<IP ADDRESS or NAME OF REMOTE COMPUTER> -u <REMOTE USER NAME> -p <NEW PASSWORD>

Linux	
Change password:	$ passwd current (msfadmin) Enter new (refer to zip file) Retype new (refer to zip file)

Host file:

Application restrictions:

IP security:

Detect - Evidence Collection & Protection Process

Install the universal forwarder software

Install the universal forwarder on Windows

Download the universal forwarder software from https://www.splunk.com/en_us/download/universal-forwarder.html

Have credentials for the Splunk administrator user ready - You must create credentials for the Splunk administrator user when installing the universal forwarder. The user's credentials are not created by the installer. If you don't provide a password during a silent installation, the universal forwarder will install without any users configured, preventing login. You must then create a user-seed.conf file to fix the problem and restart the forwarder.

1. Double-click the MSI file to start the installation.

2. Select the Check this box to accept the License Agreement check box.

3. Click Install to install the software with the defaults.

4. In the Receiving Indexer pane, enter a host name or IP address and the receiving port for the receiving indexer that you want the universal forwarder to send data to and click Next.

5. When the installer prompts you to specify inputs, enable the event log inputs by checking the Event logs checkbox.

6. Click Install to proceed. The installer runs and displays the Installation Completed dialog. The universal forwarder starts automatically.

Install the universal forwarder on Ubuntu

Download the universal forwarder with this command:

```
wget -O splunkforwarder-8.2.1-ddff1c41e5cf-linux-2.6-amd64.deb
‘https://d7wz6hmoaavd0.cloudfront.net/products/universalforwarder’
```

To install the forwarder DEB package in the default directory /opt/splunkforwarder:

```
sudo dpkg -i splunkforwarder-8.2.1-ddff1c41e5cf-linux-2.6-amd64.deb
```

Install the universal forwarder on pfSense

To download the universal forwarder on freeBSD:

```
fetch https://d7wz6hmoaavd0.cloudfront.net/products/universalforwarder/releases/8.2.1/freebsd/splunkforwarder-8.2.1-ddff1c41e5cf-freebsd-11.3-amd64.txz
```

Install the universal forwarder on pfSense using the pkg command:

```
pkg install splunkforwarder-8.2.1-ddff1c41e5cf-freebsd-11.3-amd64.txz
```

If your host has less than 2GB of memory, reduce the kern.maxdsiz and kern.dfldsiz values accordingly.

Add the following to /boot/loader.conf:

```
kern.maxdsiz="2147483648" # 2GB

kern.dfldsiz="2147483648" # 2GB

machdep.hlt_cpus=0
```

Add the following to /etc/sysctl.conf:

```
vm.max_proc_mmap=2147483647
```

Start and configure the universal forwarder

After you install the universal forwarder, you must start it before it can forward data. If you make changes to the forwarder configuration using either files or the CLI, you must restart the forwarder.

Go to the /opt/splunkforwarder/bin directory and at the command prompt, type:

```
sudo ./splunk start
```

Create a username and password.

Run this command to configure the connection to the receiving indexer:

```
sudo ./splunk add forward-server 192.168.1.100:9997
```

Configure data inputs on the forwarder

From a command prompt on the host with the universal forwarder installed, run the command that enables that data input. The forwarder asks you to authenticate and begins monitoring the specified directory.

To monitor the /var/log directory:

```
sudo ./splunk add monitor /var/log
```

To monitor port 80 (HTTP):

```
sudo ./splunk add tcp 80 -sourcetype syslog
```

Restart the universal forwarder

After configuration changes you will need to restart the forwarder with this command:

```
sudo ./splunk restart
```

Monitor Metasploitable over SSH

To monitor Metasploitable's log files, mount a remote folder over SSH. From the Ubuntu with Splunk Enterprise installed, go to Files > Other Locations > Connect to Server and type in the following command:

```
ssh://192.168.1.101/
```

Once you click on the connect button, type in the SSH login credentials and the remote directory will be mounted at /run/user/1000/gvfs/sftp:host=192.168.1.101 which you can access via command line or through the Files GUI.

Honeypot techniques

In Kali Linux, download and install pentbox with the following commands:

```
git clone https://github.com/technicaldada/pentbox

cd pentbox

tar -xvfz pentbox.tar.gz

cd pentbox
```

Start the pentbox ruby script with the following command:

```
./pentbox.rb
```

From the menu, select 2 (for Networking tools) and then 3 (for Honeypot).

In the next menu, select 2 (for Manual Configuration), type a port to open, then save a log with intrusions. This will launch a honeypot listening on the port you specified, logging the connection attempt as well as the IP address.

Install a Splunk forwarder on this virtual machine and configure the honeypot log files as data inputs.

Download and install Wireshark on Ubuntu

Install Wireshark on Ubuntu using the following command:

```
sudo apt install wireshark
```

Select Yes in response to the question “Should non-superusers be able to capture packets?”, then add yourself to the ‘wireshark’ group by running:

```
sudo usermod -a -G wireshark {your username}
```

Log out and log back in again.

Start Wireshark and capture network traffic

Press Alt+F2 and type in wireshark, then press the return key to run the program.

Double click on the interface to start capturing packets.

Download Splunk

Download Splunk Enterprise from www.splunk.com/download

Install Splunk

You can install Splunk Enterprise on Linux using DEB packages or a tar file, depending on the version of Linux your host runs.

Deb file installation

Install the DEB file using the dpkg command:

```
sudo dpkg -i splunk-file.deb
```

Tar file installation

Expand the tar file into the /opt/splunk directory using the tar command:

```
sudo tar xvzf splunk_package_name.tgz -C /opt
```

Start Splunk

Go to the /opt/splunk/bin directory and at the command prompt, type:

```
sudo ./splunk start
```

Accept the license agreement, then create a username and password.

The very last line of the information you see when Splunk starts is:

```
The Splunk web interface is at http://hostname-Virtualbox:8000
```

Follow that link to the login screen. After you log in, the Welcome screen appears.

Configure data inputs on Splunk

To start receiving data from splunk forwarders, go to Settings > Forwarding and receiving > Configure receiving > New Receiving Port.

Enter a port to listen on and click Save.

To index data from log and pcap files, go to Add Data > upload.

Protect the collected data

A python script will copy all system and network logs to a shared folder on the host OS every 30 seconds.

Respond & Analysis

System information:

User information:

Network information:

Service information:

Policy, setting and patch information:

Autorun information:

File and disk information:

Recover & Remediate

Backup:

Tactics

EXERCISE INCIDENT RESPONSE PLAN

As the complexity and connectivity of an information system and the associated risk for this system increase, organizations must establish procedures for reacting to any incidents affecting their information systems.

The types of incidents, the reporting requirements, and processes to be utilized during the exercise are listed at Table 1. The table divides security incidents into three categories, based on their severity and possible impact on the exercise.

Reportable Incident / Event	Time to Report
Any attacks affecting critical assets. Denial-of-Service attacks that isolate or impede critical service or network performance. Malicious logic (virus) attacks that isolate enclaves. Administrator/root-level access obtained by unauthorized personnel.	Within 30 minutes

Significant trends suspected in incidents or events Indication of multiple suspected systems. Suspected e-mail spoofing. Unauthorized probes or scans of the network.	Within 1 hour
UNUSUAL SYSTEM PERFORMANCE OR BEHAVIOUR. UNPLANNED SYSTEM CRASHES, OUTAGES, OR CONFIGURATION CHANGES SUSPICIOUS FILES IDENTIFIED ON A SERVER. MISSING DATA, FILES, OR PROGRAMS UNEXPLAINED ACCESS PRIVILEGE CHANGES POOR SECURITY PRACTICES. UNUSUAL AFTER-HOURS SYSTEM ACTIVITY. SIMULTANEOUS LOGINS BY THE SAME USER FROM DIFFERENT IP ADDRESSES UNAUTHORIZED ACTIVITY BY PRIVILEGED USERS. MALICIOUS LOGIC (VIRUS).	WITHIN 2 HOURS

Table 1. Sample Incident Response Categories

Reporting Procedures

The Blue Team should report security incidents or suspicious activity to their security representative utilizing the incident reporting form (Appendix A). As incidents are resolved, the security representatives should update the report and master station log (Appendix B) appropriately. The security representatives should review events, perform analysis, develop responses, and provide reporting for the event to the exercise control group (ECG).

Incident documentation records all facts regarding the incident. Reports show:

- Summary of the incident (status, relation to other events, systems affected)
- Actions already taken
- Chain of custody (for forensic team)

Once the incident has been analysed and label as real attack, personnel need to be informed including but not limited to:

- CIO
- Head of Information Security
- Other IT teams within the organization

- Human Resources
- Stakeholders

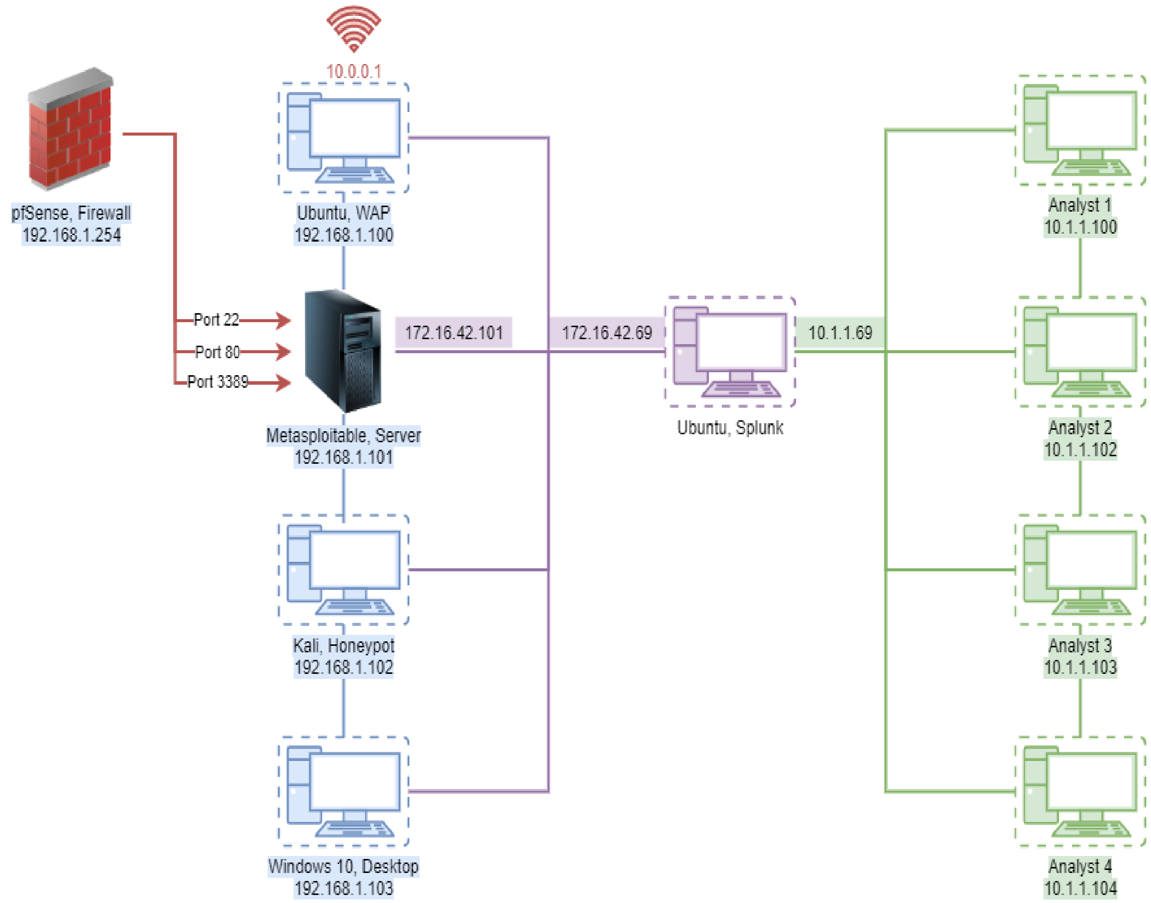
The communication methods available are:

- Email
- Phone Calls
- Meetings

Incident Response Process

1. Upon detection the user will disconnect the computer from the network.
2. The user will contact his/her security representative.
3. The security representative will complete the Incident Response form with the user and provide it to the cyber security team with a copy to the leader of the exercise.
4. The cyber security team will perform research to identify the source and level of threat before authorizing the security representative to proceed.
5. The security representative may remove the threat once approved by the cyber security team.
6. The security representative will finalize reporting in coordination with the cyber security team.

NETWORK DIAGRAM



Appendix A: Incident Response Form

Incident Response Form		
1	Date/Time	
2	Name/Organization	
3	Contact Information	
4	Location of system	
5	Type of Incident (Denial of service, Virus, Unauthorized access)	
6	System(s) involved	
7	How incident was detected	
8	Addition Details	

Appendix B: Master Station Log

Date/Time	Impact Yes / No	Description of Event	Action Taken	Initials