

Dokumentation

ESXi & Pfsense & T-pot

Joakim Bjurehov

28 februari 2019

Innehåll

1	Introduktion	3
1.1	Syfte	3
2	Metoder	4
3	Teori	5
3.1	Ord lista & Förkortningar & Termer	5
3.2	ESXi 6.7	8
3.3	PfSense 2.4.4	8
3.4	T-pot	8
3.5	Nessus	9
3.6	Kali Linux	9
4	Physical Firewall	10
4.1	Konfiguration	10
5	ESXI	13
5.1	Installation	13
5.2	Konfiguration[1]	13
5.3	Härdning[2]	16
6	Pfsense[3]	19
6.1	Installation	19
6.2	Konfiguration	20
6.3	Härdning	20
7	Administrations host	22
8	T-pot	22
8.1	Installation[4]	22
8.2	Konfiguration[4]	23
9	Syslog-ng server	24
9.1	Konfiguration[?]	24
10	Testing	26
11	Resultat	27
12	References	28

1 Introduktion

Denna dokumentation handlar om att sätta upp en fungerande virtuell miljö som använder sig av ESXi 6.7 för ett fiktivt företag som kallas IT-SEC GRP. Denna virtuella miljö ska innehålla 10 virtuella switchar, 10 Pfsense brandväggar och 1 honey pot som använder sig av T-pot. Där varje operativ system(OS) som används ska vara härdnat på ett korrekt sätt så att attack ytor mot miljön ska vara minimerade.

1.1 Syfte

IT-SEC GRP vill använda denna virtuella miljö med T-pot för att kunna samla data från attacker som sker mot honey poten. Datan som samlas kommer endast att användas i utbildnings syfte.

2 Metoder

Metoden för att sätta upp ESXi:n och konfigurera denna sker genom att använda sig av dokumentation från VMware's installation och configurations guide[1]. Sedan för att härda ESXi:n på ett korrekt sätt så används VMware's säkerhets guide[2].

För pfsense kommer deras bok att användas vid konfiguration och till viss del vid hårdning[3]. Annars kommer internet artiklar och rfc:er användas för att kontrollera olika protokoll's funktioner och användnings områden. För att kunna fastställa vilka services som behöves för detta nätverket.

Vid konfiguration och hårdning av T-pot systemet så kommer dokumentationen via deras reposetori på github[4] och deras hemsida att användas[5].

För att testa att konfigurationen och implementation är så säker som möjligt så kommer dokumentation från us-cert att användas[6]. Sedan kommer Nessus att användas för att sårbarhetsskanna alla system som är inblandade i kommunikationen med Honey Pot servern[7]. Detta för att säkerställa att attack ytan är så liten eller stor som företaget vill ha den. Yttligare säkerhets testing kommer ske genom egna penetrations tester som genomförs från Os:et Kali Linux[8].

3 Teori

Teori delen beskriver de olika systemen, verktygen som används för uppsättningen av detta. Samt för att beskriva förkortningar, termer, ord och deras betydelser.

3.1 Ord lista & Förkortningar & Termer

- **ESXi** - Elastic Sky X Integrated
- **VLAN** - Virtual Local Area Network
- **LAN** - Local Area Network
- **WAN** - Wide Area Network
- **DMZ** - DeMilitarized Zone
- **OS** - Operating System
- **GUI** - Grafical User Interface
- **TCP** - Transmission Control Protocol
- **UDP** - User Datagram Protocol
- **HTTP** - Hyper Text Transfer Protocol
- **HTTPS** - Hyper Text Transfer Protocol Secure
- **MAC-address** - Media Access Control. MAC kan dock betyda olika saker beroende på sammanhanget, men i detta dokumentet så används det för att hänvisa till fysiska adresser som olika noder har.
- **Kryptering** - Används för att förvränga data och göra den oläslig för obehöriga.

- **OSI-modellen** - Denna modellen består av 7 lager och används främst för att logisk kunna visa vart de olika protokollen används för nätverks kommunikation. Dessa lager är:
Application - Detta lager används främst av HTTP, HTTPS och DNS används här.
Presentation - Detta lager kan vara för kryptering, text format med mera.
Session - Detta lager används främst för kommunikation mellan olika processer inom en dator för att kunna kommunicera mellan varandra.
Transport - Detta lager kan vara connection-less och använder sig då av UDP. Connection less betyder att datan inte kontrolleras om den har kommit fram. Detta lager kan också vara connection-oriented och använder sig då av TCP. Vid användning av TCP så kommer det ske kontroll för att kunna fastställa att PDU:er har kommit fram till mottagaren.
Network - Detta lager använder sig främst av IPV4 eller IPV6 för att kunna skicka trafiken mellan olika noder. Detta är logiska adresser som används för att kunna hitta olika noder oberoende av vart dem ligger.
Datalink - Detta lager används för de fysiska adresserna som varje nätverkskort har. Dessa adresser är då MAC-adresser och dessa används för att kunna skicka data mellan direkt anslutna noder som finns inom samma LAN.
Physical - Detta lager är det som översätter data:n som ska skickas till binär kod som är anpassad för det fysiska mediet som är ansluten till datorn.
- **Segmentering** - Detta betyder att man delar upp till exempel ett LAN i flera mindre nätverk. Dessa nätverk är inom olika subnät och behöver använda sig av lager 3 i OSI modellen för att kunna skicka trafik mellan dessa. Detta gör att man kan skapa regler där man blockerar eller tillåter trafik mellan dessa subnät.
- **Packet filter firewall** - En brandväg som filtrerar trafik utefter port nummer och ip-adresser. Den kontrollerar endast om ett packet stämmer överens med regler som är definierade på brandväggen.
- **Stateful firewall** - En brandvägg som fungerar som en packet filter firewall, men som sparar data för varje anslutning som görs. Om något förändras under anslutningen som inte är tillåtet så kommer denna att blockera trafiken.
- **IDS** - Intrusion Detection System
- **Honey pot** - En honey pot är en server som ska dra till sig skadlig trafik. Den loggar allt en angripare gör och skyddar andra resurser på ett

nätverk. Skyddet ges i form av att man kan insolera en attack och stänga in den i honey poten och analysera vad angriparen gör. Detta kan också vara för att kunna leda bort en angripare från andra servrar och således undvika attacker på dessa. Men det kan vara svårt att implementera en honey pot på ett korrekt sätt som gör att en angripare inte märker detta.

- **Docker** - Detta är en plattform för att kunna innesluta applikationer som körs av ett operativsystem i olika containers. Detta för att kunna skydda dem från varandra och göra så dessa inte kan påverka andra system eller applikationer.

3.2 ESXi 6.7

ESXi är ett typ 1 virtualiserings OS som är Open Source. Den används för att virtualisera andra OS som till exempel Linux, Windows eller Unix. Detta gör att man kan ha flera OS på samma dator och utför olika tjänster.

ESXi har en inbyggd host brandvägg, Web GUI, virtuella switchar med mera. Administration av ESXi sker främst ifrån web GUI, men man kan använda SSH för att konfigurera denna.

3.3 PfSense 2.4.4

PfSense är en open source brandvägg som är stateful direkt från start. Den har väldigt mycket funktionalitet och är lätt att sätta upp direkt från start för att få ut en begränsad säkerhet direkt vid start. Den har möjlighet att segmentera nätverket genom olika VLAN för att sedan kunna routa mellan dessa VLAN eller för att kunna blockera trafiken mellan dessa nät.

Funktionaliteten kräver dock att man har kunskap inom nätverkssäkerhet och inom nätverksteknik. För att kunna få ut maximal säkerhet ur PfSense så kräves en hel del tid. För den har mycket igång vid start av den som inte kräves av de flesta nätverken och den har en del säkerhets risker som man måste stänga av efter man satt upp den.

Fördelarna med PfSense är att den går att bygga upp och förändra genom deras inbyggda packet hantering som ger tillgångar till andra leverantörers lösningar. Som till exempel Snort en open source IDS, en proxy med stöd för dekryptering genom Squid och mycket mera.

Genom till exempel Squid så kan man få stöd för att kunna inspektera lager 7 i OSI-modellen. Sedan finns det tilläg för att kunna kontrollera om packet innehåller skadlig kod genom olika viruskydd som kan implementeras direkt i PfSense. Detta gör att PfSense kan bli väldigt dynamisk och mångsidig. Men detta är också en nackdel då olika leverantörer kan ha olika sårbarheter. Detta gör att en administratör för PfSense behöver kontrollera alla tillägg väldigt noga och endast använda det som kräves för verksamheten.

3.4 T-pot

T-pot är en honey pot som är ett eget OS. T-pot använder sig av flera andra produkter för att ge en ökad funktionalitet. T-pot använder sig främst av en applikation som heter dockerized som gör att den kan innesluta olika applikationer och services. För att skydda dessa under en attack. Sedan använder den sig av andra honeypot applikationer för att kunna vara en mångsidig honeypot så den kan samla data från databaser, web-applikations attacker med mera.

För loggningen använder den sig av delar från Elastic Kibana Logstash(ELK-stack). ELK är open source och kan strukturera datan på ett enkelt sätt och sedan visa den genom ett web GUI.

3.5 Nessus

Nessus är en sårbarhets skanner som kan användas för att skanna olika serverar och noder efter sårbarheter[9]. Detta för att kunna hitta olika sårbarheter som finns i olika miljöer. Nessus kan antingen sättas upp för att skanna serverar automatiskt eller genom att användas manuellt. Den kan användas för att hitta känsliga dokument som ligger i en sårbar position, skadlig kod eller till exempel sårbarheter i form av dokumenterade sårbarheter som finns på grund av öppna portar på en server.

3.6 Kali Linux

Kali Linux är ett OS som används för penetrationstestning[8]. Den är utformad med en mängd olika verktyg för att kunna ta sig in på ett nätverk eller en server. Verktygen som används från Kali är dessa:

- Nessus
- Nmap

4 Physical Firewall

Detta är den fysiska brandväggen som hanterar kommunikation ut på publica nätverket och även kommunikation mellan de olika subnäten inom företaget[3].

4.1 Konfiguration

1. ESXi Managment interface:
VLAN: 999 Network: 172.25.1.0/30
Detta interface används för att administrera ESXi och är tillgänglig via lan:et.

Managment Interface IP: 172.25.1.1/30

2. DMZ interface för säker administration av sårbara system: VLAN: 3499
Network: 172.26.0.0/24
Interface IP: 172.26.0.1/24
Detta nätverket används för att administrera t-pot och syslog servern som ligger bakom en egen brandvägg. Detta finns för att kunna få direkt access via dessa maskiner till t-pot servern.

3. DMZ interface för honey pot mot publica nätverket:

Network: 172.27.0.0/24
Interface IP: 172.27.0.1/24
DHCP: Range: 172.27.0.100 - 172.27.0.254
DNS: 1.1.1.1
8.8.8.8

4. Skapa port och IP alias:

Göra alias i fysisk PfSense för att blockera LAN/ADMIN access från DMZ interface.

Networks i Alias:

10.1.8.0/21
10.1.16.0/21
10.1.24.0/21
10.1.32.0/21
10.1.40.0/21
172.25.1.0/30

Detta för att blockera access från dmz nätverket till administration och lan

5. Skapa port alias:

Gör Alias i fysisk för att tillåta dessa portar till t-pot server[4]:

Port alias:

Dionaea TCP : 21, 42, 135, 443, 445, 1433, 3306, 5060, 5061, 8080









Dionea UDP: 69, 5060

Kippo TCP: 22

Honeytrap TCP: 25, 110, 139, 3389, 4444, 4899, 5900, 21000



Glastopf TCP: 80

Detta för att skapa en portforward ut mot internet så honeypoten kan ta emot angrepps försök via dessa portar.

Firewall Aliases Ports			
Name	Values	Description	Actions
ADMIN_PORTS	22, 443	Admin Ports for HTTPS & SSH	 
Basic_network_Access	443, 80, 53, 123	Basic access for dmz machines	 
T_POT_FORWARD_DMZ_TCP	21, 42, 135, 443, 445, 1433, 3306, 5060, 5061, 8080...	DMZ t-pot o public network	 
T_POT_FORWARD_DMZ_UDP	69, 5060	T-pot forward to DMZ udp	 

6. Port forwarding för t-pot mot public IP:

Här används port aliases för att forwarda dessa portar till t-pot servern. Bilden nedan förevisar denna konfiguration:

Floating	WAN	LAN	PRIVATE_LAN	PRIVATE_WLAN	GUEST_WLAN	DEVICES_WLAN	LAB_LAN
DMZ_MANAGEMENT	DMZ_ESXi						
Rules (Drag to Change Order)							
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway Queue
<input type="checkbox"/>	 0 / 0 B	IPv4 *	DMZ_HONEY_POT net	*	DMZ_BLOCK_ACCESS_LAN	*	* none
<input type="checkbox"/>	 4 / 14.26 MIB	IPv4 *	DMZ_HONEY_POT net	*	*	*	* none

7. Interface kommunikation:

DMZ interface får endast kontakt ut på internet via publica ip x.x.x.x.

DMZ interface får inte kommunicera direkt med andra subnät via brandväggen.

Övriga interfaces får inte kommunicera via LAN till DMZ interface, de behöver gå via den publica IP x.x.x.x

Managment interface för ESXi kan endast kommunicera med PRIVATE_LAN interface för kommunikation, då detta är administrations nätverket på företaget.

Övriga interfaces blockeras via brandväggen för kommunikation med PRIVATE_LAN samt ESXi management interface.

8. NTP server:
Sät NTP servern till xxxxxxxx som är online NTP server som är säker.
9. Services som körs är:
DHCP 67,68
NTP 123
DNS 53
HTTPS 443
Dessa är dock inte access bara för samtliga subnät.

5 ESXI

I denna sectionen så kommer de tekniska delarna att specificeras genom steg. Där relevanta kommandon och förklaringar ges.

5.1 Installation

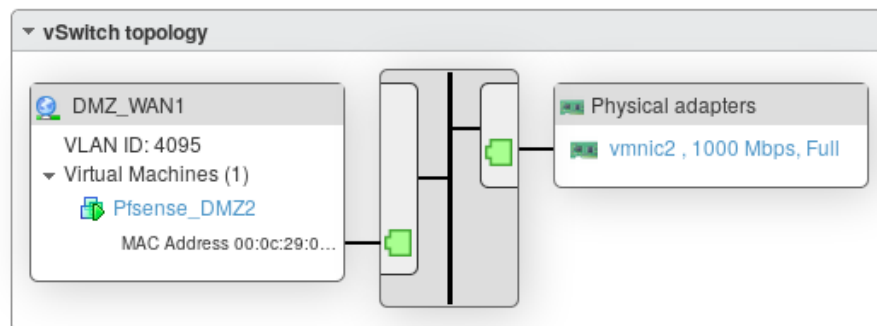
1. Ladda ner ISO för ESXI 6.7
2. Skapa en bootbar sticka genom valfritt program.
3. Använd standard installer genom ESXI 6.7.
Bilden nedan förevisar web gränssnittet efter installation:

5.2 Konfiguration[1]

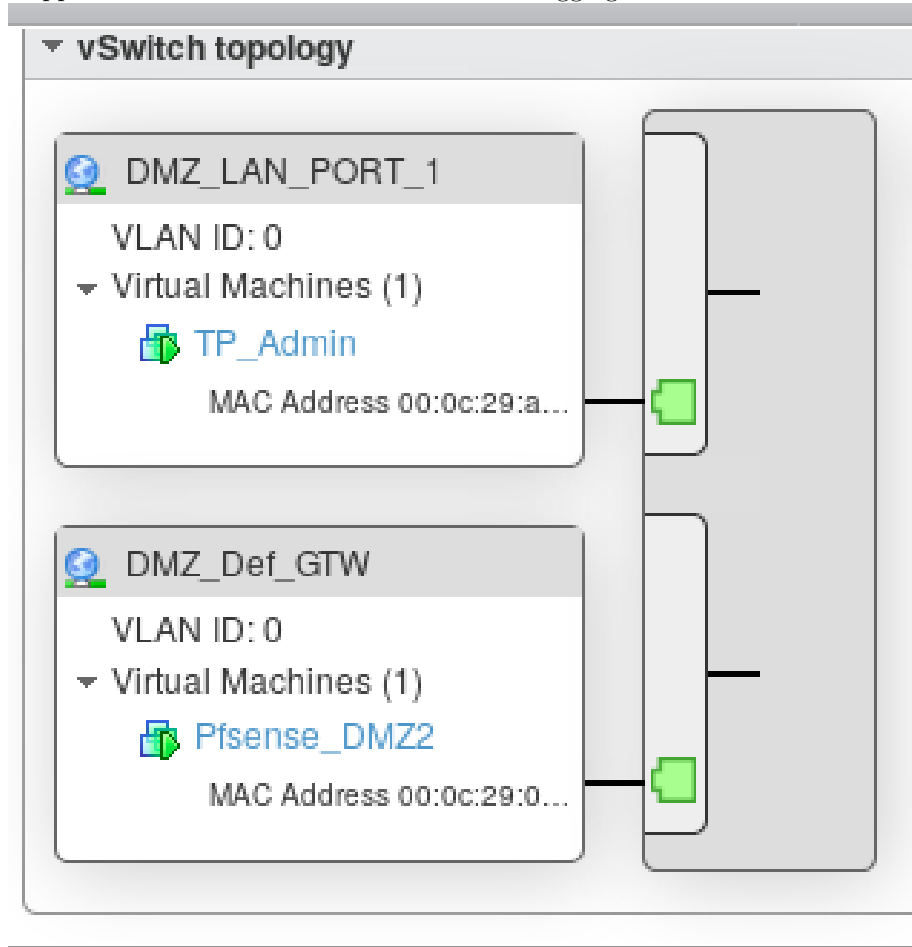
1. Managment interface konfiguration:
Managment virtual switch:
Default vid installation.

Network : 172.25.1.0/30 Interface IP: 172.25.1.2/30
Default Gateway: 172.25.1.1/30
DNS: 1.1.1.1

2. DMZ interface konfiguration:
DMZ virtual switch DMZ_ switch1:
Upplink physical adapter vmnic2
Port DMZ_ WAN1: till PfSense
Sätt VLAN på DMZ_ wan1 till 4095 för att trunka trafiken.
Sätt VLAN 3499 på virtual interface för WAN porten på PfSense.
Koppla PfSense till DMZ_ LAN_ switch på port DMZ_ Def_ gateway



3. DMZ virtual DMZ_ LAN_ SWITCH: Skapa portart:
DMZ_ DEF_ GTW
DMZ_ LAN_ PORT_ 1
Koppla dessa till administrations datorn och logging switchen.



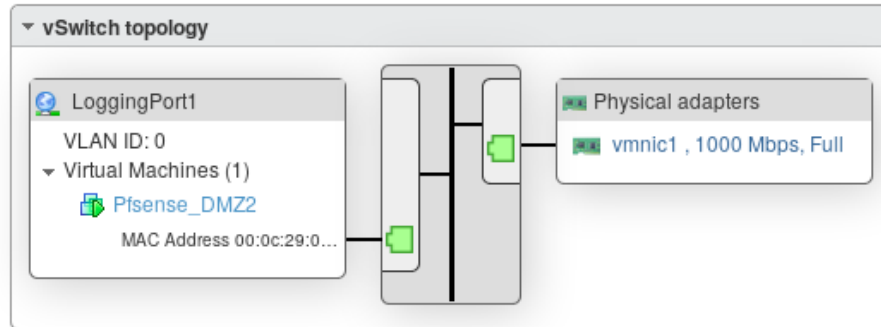
4. Logging virtual switch:

Skapa en virtuel switch med namnet LoggingSwitch.

Lägg till två virtuella portar som heter:

LoggingPort1

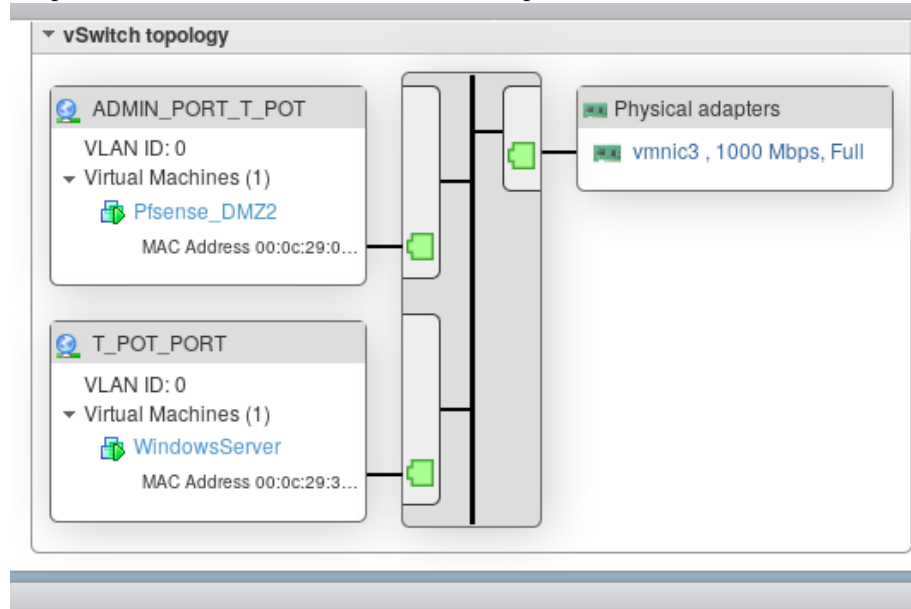
Logging switchen är sedan kopplad till ett fysiskt interface och detta interface är kopplad till en Ubuntu server som har syslog-ng installerat och kan ta emot loggarna.



5. DMZ Switch för t-pot:

Skapa ADMIN_PORT_T_POT för att ansluta mot administrations nätverket bakom virtuell pfsense.

Skapa T_POT_PORT för att ansluta till t-pot servern.



5.3 Härdning[2]

1. Uppdatera ESXI:
Sker genom omvärds bevakning och via företaget.
2. Skapa ny administratör:
Name: ADMIN
Passowrd: XXXXXXXXXX
Gå in i maintenece mode
Välj premissions och add user
Lägg till roll Administrator
3. ta bort användare:
Ta bort behörigheter för root.
Ta bory behörigheter för dcui användaren.
Detta för att minimera attackytan.
4. Stäng/Start av services:
DCUI avstängd.
SSH avstängt.
NTP starta, sätt till 172.25.1.1 som är den fysiska brandväggen som NTP server.
SNMP avstängt.
5. Logging:
Loggning sker endast intärnt på ESXi:n och bör konfigureras av beställaren.
6. Lockdown mode:
Lägg till ADMIN i exceptions list för lockdown mode.
Aktivera strict-lockdown-mode.

7. Firewall rules:

Name ▲	Key	Incoming Ports	Outgoing Ports
DVFilter	DVFilter	2222	
DVSSync	DVSSync	8301, 8302	8301, 8302
esxupdate	esxupdate		443
Fault Tolerance	faultTolerance	8300	80, 8300

Öppna ports:
80 - Update Manager

123 - Ntp client
 443 - Https access via web interfacet.
 902 - Denna porten används för att managera hosts och av heartbeat servicen som kontrollerar om hosts är aktiva och även för NFC.
 2012 - Denna porten används för RPC kommunikation och single sign-on genom en Windows appliance för att kunna logga in till en virtuell maskin.
 2014 - RPC port för VMCA (VMware Certificate authity) API för att kunna administrera maskiner via en plugin.
 2015 - DNS managment för ESXi
 2020 - VCenter server använder denna för Node till Node kommunikation.
 5480 - hanterar XMLRPS, JSON-RPC förfrågningar till ESXi:n genom HTTPS.
 6500 - ESXi Dump Collector port genom VCenter server installation på Windows.
 6501 - Auto Deploy service för Windows insallation och appliance för utrullning via vCenter Server.
 6502 - Auto Deploy Managment för Windows installationer och appliance utrullning av VCenter Server.
 7080, 1272, 1 - Secure Token Service som används av Windows installationer och appliance utrullning av Platform Service Controller
 7081 - VMware Platform Services Controller Web Client och används för Windows installaioner och appliance utrullning av Platform services controller
 7475, 7476 - Vmware vSphere Authencation Proxy och används för utrullning av appliance för vCenter Server
 8000 - vMotion 8200, 8201, 8300, 8301 - Appliance management för Platform services controller och VCenter Server
 8084 - vSphere Update Manager SOAP port, VSphere Update Manager client plug-in för att ansluta sig till vSphere Update Manager SOAP server. Krävs för att används vCenter Server
 9000 - Update Manager
 9084 - Update manager Web server port, HTTP port som används av ESXi hosts för att acceptera patch filer.
 9087 - vSphere update manager web SSL port, används för HTTPS update manager client plug-in för att ladda upp uppggradera filer via update manager server på ESXi:n.
 9443 - vSphere Web Client HTTPS.

Det som inte har specificerats i öppna portar ska vara stängda och är oanvända vid nuvarande konfiguration.

8. Policy configurations:
 - AccountLockFailures: 3
 - AccountUnlockTime: 900

Policyn för account hanterar misslyckade inloggningar och försvårar brute-force attacker mot inloggning till ESXi:ns webb interface.

Interactive shell timeout: 900

Shell timeout: 900

Shell policyn gör så användaren automatiskt loggas ut vid inaktivitet efter 900 sekunder.

NetBlockGuestBPDU: 1

BPDU syftar till rammar som hanteras av spanning-tree för att kunna hantera loppar, detta protokollet är sårbart och man skyddar det genom NetBlockGuestBPDU policyn.

6 Pfsense[3]

6.1 Installation

1. Download ISO från www.pfsense.org/download/
Välj Version 2.4.4-p1
Installer CD Image (ISO) Installer
Välj mirror valfritt.
2. Installera på ESXI:
Från host välj Create/register VM
Select creation type välj create new virtual machine.

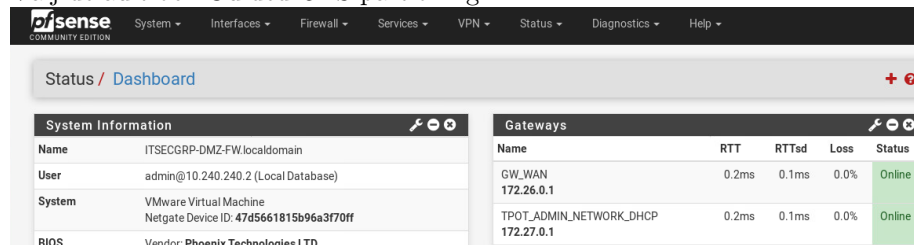
Select a name and guest os:
Namn: Pfsense_ DMZ
Copability: ESXI 6.7 virtual machine.
Guest OS family: Other
Guest OS version: FreeBSD 11(64-bit)

Select storage:
Välj datastore efter behag

Customize settings:
CPU: 2 virtual cores
Memory: 8 GB
Hard disk 1: 50 GB
SCASI controller 0 : LSI Logic SAS
Network adapter 1: LoggingPort1(Port till logg server)
Network adapter 2: DMZ_ DEF_ GTW(Till T-pot admin Datorn)
Network adapter 4: DMZ_ WAN1 (Port till DMZ switch)
Resten default.

3. Install pfsense:

Välj default och Guided UFS partitioning.



The screenshot shows the pfSense Community Edition dashboard. The top navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The main content area is divided into two panels. The left panel, titled 'System Information', displays details about the system, including the name 'ITSECGRP-DMZ-FW.localdomain', user 'admin@10.240.240.2 (Local Database)', system type 'VMware Virtual Machine', Netgate Device ID '47d5661815b96a3f70ff', and BIOS vendor 'Phoenix Technologies LTD'. The right panel, titled 'Gateways', shows a table of active gateways with columns for Name, RTT, RTTsd, Loss, and Status. Two gateways are listed: 'GW_WAN 172.26.0.1' and 'TPOT_ADMIN_NETWORK_DHCP 172.27.0.1', both showing low latency and 0% loss, and are marked as 'Online'.

System Information	
Name	ITSECGRP-DMZ-FW.localdomain
User	admin@10.240.240.2 (Local Database)
System	VMware Virtual Machine Netgate Device ID: 47d5661815b96a3f70ff
BIOS	Vendor: Phoenix Technologies LTD

Gateways				
Name	RTT	RTTsd	Loss	Status
GW_WAN 172.26.0.1	0.2ms	0.1ms	0.0%	Online
TPOT_ADMIN_NETWORK_DHCP 172.27.0.1	0.2ms	0.1ms	0.0%	Online

6.2 Konfiguration

1. Wizard vid inloggning för grund inställningar:

Hostname: ITSECGRP-DMZ-FW

Primary DNS Server: 1.1.1.1

Secondary DNS Server: 8.8.8.8

Time server: 172.26.0.1

Timezone: Eurpoe/Stockholm

Username: admin

Passowrd: xxxxxxxx

2. Konfigurera interfaces:

Välj VMX0.3499 till WAN interface:

Network: 172.26.0.0/22

Interface IP: 172.26.0.2/22

Upstream Gateway: 172.26.0.1/22

DNS: 1.1.1.1

Välj vmx1 LOGGING:

Network: 10.200.200.0/24

Interface IP: 10.200.200.2/24

Välj vmx2 TPOT_ ADMIN:

Network: 10.240.240.0/30

Interface IP: 10.240.240.1/30

välj vmx3 ADMIN_ PORT_ T_ POT:

Network 172.26.0.0/24

Interface IP: 172.26.0.10

6.3 Härdning

1. Administrations access av FW:

Stäng av http direct via web gui, för att endast tillåta https.

Stäng av default regeln för FW access och lägg en regel för access via admin nätverket 10.240.240.0/30 till FW.

Blockera admin access via övriga interfaces genom block regler.

2. Interface kommunikation:
 - Sätt regel Blocka på Logging interface att den inte får access till Firewall interfaces direkt och blockera administration.
 - Sätt regel att t_ pot admin får access till firwall interfaces, den får också access till logging nätet och t-pot nätet.
 - Sätt regler för att admin porten ut mot t-pot ska kunna kommunicera med servern, men servern ska inte kunna skicka tillbaka trafik.
3. NTP server:
 - Sät NTP servern till 172.26.0.1 som är fysiska brandväggen för korrelerade loggar.
4. Services som körs är:
 - DHCP 67,68
 - NTP 123
 - DNS 53
 - HTTPS 443
 - Dessa är dock inte access bara för samtliga subnät.

7 Administrations host

Skapa en host för att administrera T-pot servern och den virtuella brandväggen.

1. Skapa nätverks interface på Pfsense_ dmz med ip 10.240.240.1/30
Koppla interface till DMZ_ DEF_ GTW.
Skapa virtuellt interface på standard switch DMZ_ LAN_ Switch med namnet DMZ_ LAN_ PORT_ 1.
Installera valfri distrubution och anslut till interface DMZ_ LAN_ PORT2 och sätt statisk ip 10.240.240.2/30.
2. Installera Debian 9.5 och lägg till network adapter 1 med DMZ_ LAN_ PORT_ 1

8 T-pot

8.1 Installation[4]

1. Download T-pot iso från <https://github.com/dtag-dev-sec/tpotce/releases>
2. T-pot behöver en DHCP server vid installation så den ansluter sig mot nätverket 10.255.255.0/24.
3. Select A name and Guest OS:
Name: WindowsServer
Copability: ESXI 6.7 virtual machine
Guest OS family: Linux
Guest OS version: Ubuntu Linux (64-bit)
Select Store: default

Customize settings:
CPU: 2
Memory: 8 GB
Hard disk: 300 GB
USB controller: Remove
Network Adapter 1: T_ POT_ PORT
CD/DVD drive 1: Datastore ISO file: t-pot
Video card: default
4. Installation:
Choose T-pot 19.03

Välj plats: Sweden
Välj tangentbord: Swedish
Välj Standard installation för T-pot

Console login:
Username: tsec
Password: xxxxxx

Web login:
username: webuser
Password: xxxxxxxx

5. Console interface:

6. Web GUI interface:

8.2 Konfiguration[4]

1. T-pot funkar out of the box och är färdig att köras direkt efter installation.
2. Skapa en statisk mappning i dhcp servern till t-pot servern via fysiska brandväggen:
IP: 172.27.0.99
Default-gateway: 172.27.0.1
DNS server: 1.1.1.1, 8.8.8.8
NTP-server: 172.27.0.1 (Fysisk brandvägg)
3. Konfigurera loggning:
Loggningen kommer ske manuellt var 29 dag i månaden.
Där man hämtar ner /data katalogen som ligger i root.
Den innehåller alla relevanta loggar och raderas automatiskt var 30 dag.

9 Syslog-ng server

Syslog-ng servern använder sig av en Ubuntu server 16.4. Denna är konfigurerad sen tidigare och ställs endast in för att samla loggar från PfSensen. För att kunna verifiera funktion och om någon gör otillåtna förändringar.

9.1 Konfiguration[?]

1. User och grupp för syslog-ng servern:
Namn: syslog-admin
password: xxxxxxxxx
Grupp: syslog-grp

Användare och grupp skapas för att kunna skapa filerna för de olika loggarna som tas emot och så dessa inte utgör en säkerhets risk.

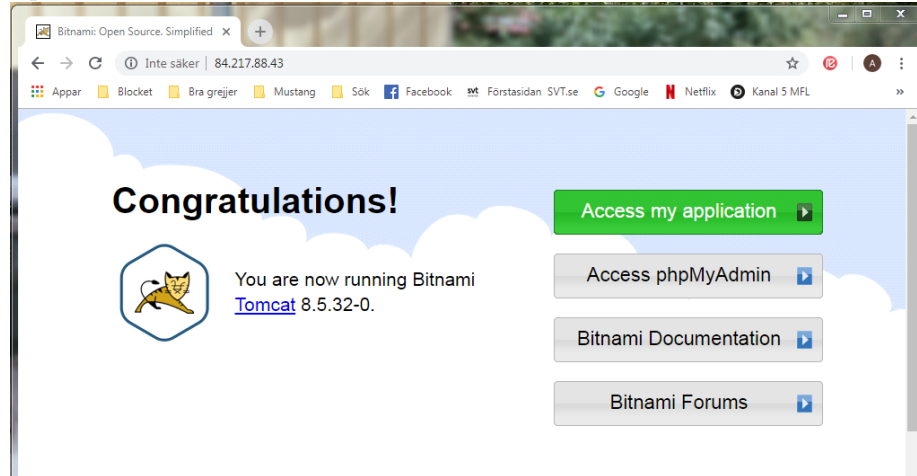
2. Network konfiguration:
Default-gateway: 10.200.200.2/24
IP-address: 10.200.200.1/24
DNS-server: 1.1.1.1
3. NTP server:
Sät NTP servern till 172.26.0.1 som är fysiska brandväggen för korrelerade loggar.

4. Syslog-ng.conf filens konfiguration:
Logg filerna lagras i /var/log/syslog-ng/hostname/year/month/ i formatet hostname.year.month.day
Konfigurations filen ligger /etc/syslog-ng/conf.d/ och skapa en syslog-ng konfigurations fil som heter syslog_ ng_ log_ collector.conf och innehåller:

```
options {  
    create_ dirs(yes);  
    owner(syslog-admin);  
    group(syslog-group);  
    perm(0640);  
    dir_ owner(syslog-admin);  
    dir_ group(syslog-group);  
    dir_ perm(0750);  
};  
source s_ net {  
    tcp(ip(0.0.0.0) port(514));  
    udp(ip(0.0.0.0) port(514));  
};  
  
destination d_ host-specific {  
    file("/var/log/syslog-ng/$HOST/$YEAR/$MONTH/$HOST-$YEAR-$MONTH-$DAY.log");  
};  
  
log {  
    source(s_ net);  
    destination(d_ host-specific);  
};
```

10 Testing

- t-pot access test:



- syslog-ng access test:

```
root@ubuntu-syslog-ng:/etc/syslog-ng/conf.d# netstat -tulnp | grep 514
tcp        0      0 0.0.0.0:514          0.0.0.0:*           LISTEN      1829/syslog-ng
udp        0      0 0.0.0.0:514          0.0.0.0:*           1829/syslog-ng
root@ubuntu-syslog-ng:/etc/syslog-ng/conf.d# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eno1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:23:24:77:c1:0a brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.187/24 brd 192.168.1.255 scope global eno1
        valid_lft forever preferred_lft forever
    inet6 fe80::23:24:77:c1:0a/64 scope link
        valid_lft forever preferred_lft forever
root@ubuntu-syslog-ng:/etc/syslog-ng/conf.d# ls -la /var/log/syslog-ng/
total 12
-rw-r--r-- 3 syslog-admin syslog-group 4096 Feb 26 17:21 .
-rw-r--r-- 9 root          syslog      4096 Feb 26 17:21 ..
-rw-r--r-- 3 syslog-admin syslog-group 4096 Feb 26 17:21 192.168.1.181
root@ubuntu-syslog-ng:/etc/syslog-ng/conf.d# cd /var/log/syslog-ng/192.168.1.181/2019/02/
root@ubuntu-syslog-ng:/var/log/syslog-ng/192.168.1.181/2019/02# ls -la
total 12
-rw-r--r-- 2 syslog-admin syslog-group 4096 Feb 26 17:21 .
-rw-r--r-- 3 syslog-admin syslog-group 4096 Feb 26 17:21 ..
-rw-r--r-- 1 syslog-admin syslog-group 145 Feb 26 17:21 192.168.1.181-2019-02-26.log
root@ubuntu-syslog-ng:/var/log/syslog-ng/192.168.1.181/2019/02# cat 192.168.1.181-2019-02-26.log
Feb 26 17:21:41 192.168.1.181 1 2019-02-26T17:21:41.712119+01:00 lux root - - [timeQuality tzKnown="1" isSynced="1" syncAccuracy="730000"] hello
root@ubuntu-syslog-ng:/var/log/syslog-ng/192.168.1.181/2019/02# tail -f 192.168.1.181-2019-02-26.log
Feb 26 17:21:41 192.168.1.181 1 2019-02-26T17:21:41.712119+01:00 lux root - - [timeQuality tzKnown="1" isSynced="1" syncAccuracy="730000"] hello
Feb 26 17:23:03 192.168.1.181 1 2019-02-26T17:23:03.649065+01:00 lux root - - [timeQuality tzKnown="1" isSynced="1" syncAccuracy="771000"] apa
Feb 26 17:23:08 192.168.1.181 1 2019-02-26T17:23:08.242243+01:00 lux root - - [timeQuality tzKnown="1" isSynced="1" syncAccuracy="773500"] hej san
Feb 26 17:23:13 192.168.1.181 1 2019-02-26T17:23:13.476258+01:00 lux root - - [timeQuality tzKnown="1" isSynced="1" syncAccuracy="776000"] vad gör du?
```

11 Resultat

Resultatet av detta jobb blev att en fungerande ESXi, pfsense, tspot blev installerad, konfigurerad och härdad. Dessa har nätverks access och är segmenterade på olika delar av nätverket. Dessa har blivit segmenterade via VLAN och olika web interface i brandväggen. Sedan har ett administrations nät blivit installerat med övervakning via en syslog-ng server för att se om någon ansluter ditt och förändrar något under körningen. Administrations nätverket används för att få tillgång till loggar på t-poten för att kunna ladda ner dessa var 29 dag för lagring.

Det som inte blev levererat var själva testningen med nessus och kali. Denna gick tyvärr inte att genomföra på grund av att tiden inte räckte till och denna kan utföras under 1 vecka på önskad tid om företaget önskar detta. Min rekommendation är dock att testa denna konfiguration ur ett penetrations testing perspektiv för att säkerställa att denna inte påverkar företagets andra resurser.

12 References

- [1] “Vmware esxi installation and setup,” 2018. [Online]. Available: <https://docs.vmware.com/en/VMware-vSphere/6.7/vsphere-esxi-67-installation-setup-guide.pdf>
- [2] “Vsphere security,” 2017. [Online]. Available: <https://docs.vmware.com/en/VMware-vSphere/6.7/vsphere-esxi-vcenter-server-67-security-guide.pdf>
- [3] “The pfsense book,” 2019. [Online]. Available: <https://www.netgate.com/docs/manuals/the-pfsense-book.pdf>
- [4] “T-pot,” 2019. [Online]. Available: <https://github.com/dtag-dev-sec/tpotce>
- [5] “T-pot: A multi-honeypot platform,” 2019. [Online]. Available: <http://dtag-dev-sec.github.io/mediator/feature/2015/03/17/concept.html>
- [6] “Us-cert,” 2018. [Online]. Available: <https://www.us-cert.gov/>
- [7] “Nessus,” 2019. [Online]. Available: <https://www.tenable.com/products/nessus/nessus-professional>
- [8] “Kali linux,” 2019. [Online]. Available: <https://www.kali.org/>
- [9] “Nessus,” 2019. [Online]. Available: <https://docs.tenable.com/nessus/7.1/Content/Resources/PDF/Nessus.7.1.pdf>