White Team Documentation

Wright State University

Prepared on 2017 March 24

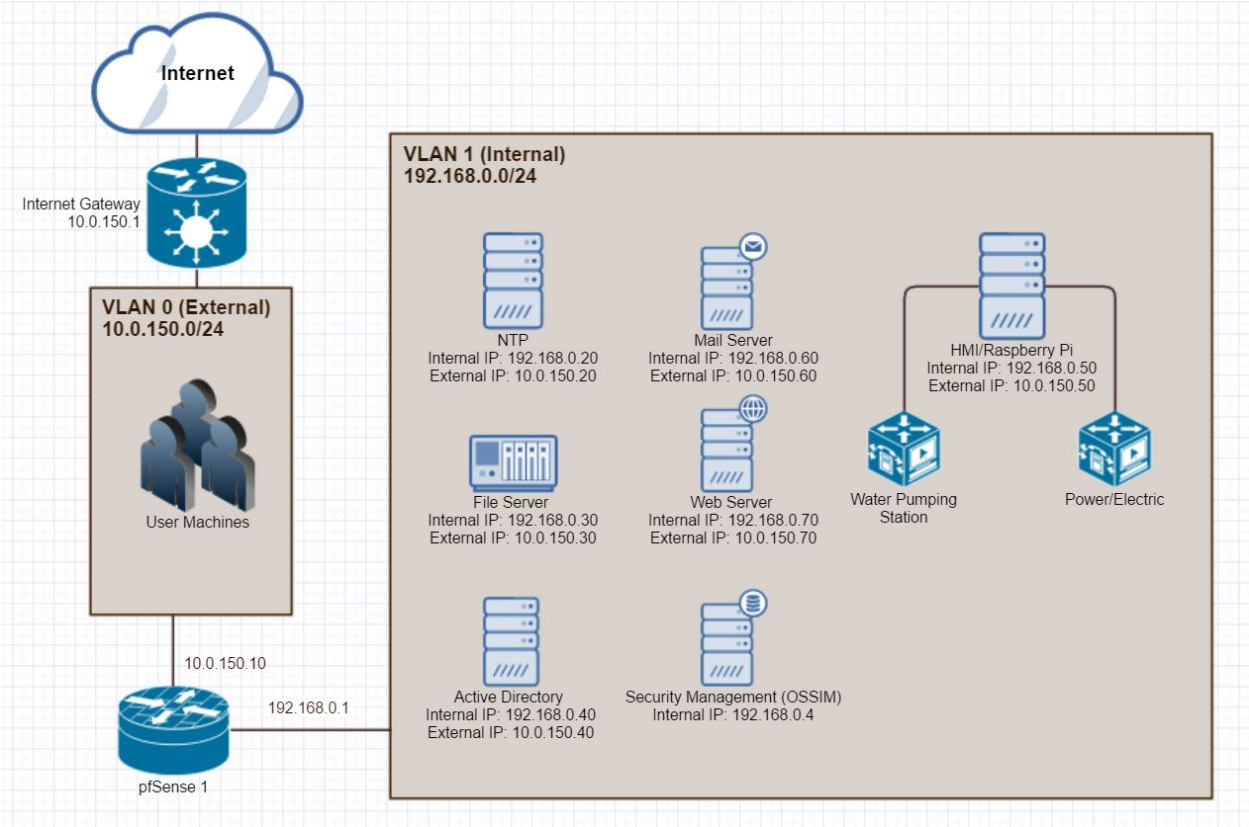
2017 ANL Cyberdefense Competition

Network Topology

Our network utilizes three subnets on one switch using VLANs. VLAN 0 is the external network that is directly connected to the Internet (10.0.150.0/24). VLAN 1 is the internal network that contains most of our machines (192.168.0.0/24).

All of the machines in the internal network are accessible via the external network through pfSense. In the diagram below, the external IP addresses for machines in VLAN 1 are bound through 1:1 NAT on pfSense. pfSense acts as both a router and a firewall, and all external access to our internal machines must pass through it.

The OSSIM server running on 192.168.0.4 is the only device that is not externally accessible, and must be accessed through a VPN running on pfSense.



DNS is provided to external clients through the Active Directory server at 10.0.150.40, and the server will resolve external IP addresses for the pangea.local domain. Internal machines only use DNS to talk to the outside world (they do not use the Active Directory DNS), and all of the machines have an identical hosts file to resolve internal addresses.

Security Measures

Remote Administrative Access

All of the servers hosting SSH have been configured to disallow remote login to the root account with password authentication. The administrators have access to the servers using public key authentication, and if somebody needs to restore or gain access, they can do so through the console of the machine itself.

The Active Directory domain controller server can only be accessed via the console and has no remote administration features enabled.

The NTP server can also only be accessed via the console. Considering the simplicity of NTP and the fact that the server is not running anything but the NTP daemon, it is unlikely that frequent access will be needed.

As an additional security measure will be randomly banner swapping/removing between servers

Local Administrative Access

The administrative accounts and passwords of each machine are listed below:

Machine	**Username**	**Password**
pfSense	`admin`	`q3832iHS6RNCcu`
ntp.pangea.local	`root`	`tvJXFLi9kTgrJpQ8`
files.pangea.local	`root`	`Loxs7aRgxQiNTzDG`
dc.pangea.local	`Administrator`	`sincehelicalflatulationentersintelthroughtheamd`
hmi.pangea.local	`root`	`rk4voNAwWhK4sTpw`
mail.pangea.local	`root`	`f7PuXVaATNmYRWAz`
www.pangea.local	`root`	`RX9sbjiDAgKrLpB6`

System Configuration

Web Server

Hostname:	www.pangea.local
IP:	10.0.150.70, 192.168.0.70
OS:	Debian 7 ("wheezy")
Software:	Apache 2.2.22
	MySQL 5.5.54
	PHP 5.4.45
	Drupal 7.54

The web server is running on top of a standard LAMP (Linux, Apache, MySQL, PHP) stack with Drupal installed to provide a framework for the website. Drupal is bound to LDAP on the Active Directory domain controller and can use it to authenticate users logging in to the website.

The MySQL backend for the website has had its password changed from the default and Drupal now accesses its database with its own account. The password for the `root` account for MySQL on the web server is: `MHdaRwN76DBgZWeyJ8FYWcP4oXaKF9vNgCVTKdv7G9gJBADaGgWSziANBt9SZYd6`. It is likely that an administrator will be able to use SSH to remotely access the web server and paste the password in to avoid typing the entirety of it.

Security Management (OSSIM)

Hostname:	n/a
IP:	192.168.0.4
OS:	Alienvault OSSIM
Software:	PRADS
	OpenVAS
	Snort
	Suricata
	Tcptrack
	Nagios
	OSSEC
	Munin
	NFSen/NFDump
	FProbe

This system will be a central system for analyzing and reporting network and host related security events. This system will be forwarded all of the network traffic through NAT firewall rules on pfSense.

Active Directory Domain Controller

Hostname:	dc.pangea.local
IP:	10.0.150.40, 192.168.0.40
OS:	Windows Server 2008 R2
Software:	Primary Domain Controller role
	DNS role

Windows Server has been configured to act as a domain controller and DNS server for the pangea.local domain.

NTP Server

Hostname:	ntp.pangea.local
IP:	10.0.150.20, 192.168.0.20
OS:	Debian 8 ("jessie")
Software:	NTPsec 0.9.7

The NTP server is running the latest build of NTPsec, which is a fork of the standard NTPd software with reduced complexity, which should lead to a reduced attack surface.

pfSense

Hostname:	pf.pangea.local
IP:	10.0.150.10, 192.168.0.10
OS:	pfSense 2.3.3
Software:	Snort 3.2.9.2
	Unbound (DNS resolver for internal network)

pfSense 1 is configured as a firewall and router between the external (10.0.150.0/24) and internal (192.168.0.0/24) networks. All traffic from the external network needs to pass through pfSense to access the machines on the internal network, which are bound to their external ports using 1:1 NAT in pfSense. The firewall is configured to whitelist any necessary ports on the internal network.

As traffic passes through, it is inspected by the Snort Intrusion Detection System (IDS). Because all traffic must pass through this central point, we can easily monitor for malicious network activity.

HMI

Hostname:	n/a
IP:	10.0.150.50, 192.168.0.50
OS:	Raspbian 8 ("jessie")
Software:	Python 2.7.9 with Flask 0.12
	Apache 2.4.10

The HMI is a Raspberry Pi computer running Raspbian, a version of Debian GNU/Linux for the Raspberry Pi. It is running a web application using Python 2.7 and Flask that is used to interface with the water and power systems.

Flask is available via uWSGI on localhost:2421 and is configured to be accessible externally through an Apache reverse proxy. When accessing the /water, /power, or /killswitch paths, Apache will ask for credentials for a member of the Technicians group in LDAP before allowing access.

File Server

Hostname:	file.pangea.local
IP:	10.0.150.30, 192.168.0.30
OS:	Ubuntu 14.04 LTS
Software:	Samba 4.3.11
	vsFTPd 3.0.2

The file server provides FTP access to a share for LDAP users, as well as access to Samba shares.

Mail Server

Hostname:	mail.pangea.local
IP:	10.0.150.60, 192.168.0.60
OS:	CentOS 6
Software:	Postfix 2.6.6
	Dovecot 2.0.9
	Squirrelmail 1.4.22
	Apache 2.2.15
	PHP 5.3.3

The mail server handles all mail for the cdc.pan domain. It provides a webmail interface through Squirrelmail running on Apache and PHP as well as secure SMTP and IMAP access through Postfix and Dovecot.

Ports and Protocols

All of the open ports and protocols for each machine are listed below. All of the firewalls in place are implemented as whitelists, so ports must be explicitly opened if they are to be used.

Machine	**Outbound Ports**	**Inbound Ports**
Web Server	UDP/123 (NTP) to NTP server TCP/UDP/389 (LDAP) to AD DC TCP/636 (LDAPS) to AD DC	TCP/22 (SSH) from everywhere TCP/80 (HTTP) from everywhere TCP/443 (HTTPS) from everywhere
Security Management		UDP/514 (Syslog Forwarding) from 192.168.0.1/24 TCP/80 (HTTP) from 192.168.0.1/24 TCP/433 (HTTPS) from everywhere
AD Domain Controller	UDP/53 (DNS) to pfSense 1 UDP/123 (NTP) to NTP server	UDP/53 (DNS) from everywhere TCP/UDP/88 (Kerberos) from File and Mail TCP/UDP/389 (LDAP) from everywhere TCP/636 (LDAPS) from everywhere
NTP Server	UDP/53 (DNS) to pfSense	TCP/22 (SSH) from everywhere UDP/123 (NTP) from everywhere
pfSense	UDP/53 (DNS) to everywhere UDP/123 (NTP) to NTP server	UDP/53 (DNS) from 192.168.0.0/24 TCP/80 (HTTP) from everywhere TCP/443 (HTTPS) from everywhere
HMI	TCP/2421 to localhost (uWSGI)	TCP/80 (HTTP) from everywhere TCP/443 (HTTP) from everywhere TCP/2421 from localhost (uWSGI backend)
File Server	UDP/53 (DNS) to AD DC UDP/123 (NTP) to NTP server Anything to AD DC	TCP/21 (FTP) from everywhere TCP/22 (SSH) from everywhere Anything from AD DC
Mail Server	UDP/53 (DNS) to AD DC UDP/123 (NTP) to NTP server Anything to AD DC	TCP/22 (SSH) from everywhere TCP/80 (HTTP) from everywhere TCP/443 (HTTPS) from everywhere Anything from AD DC