Common Settings

General Information	
System Administrator	Josh Cannons
Contact	Josh.cannons@privata.com.au
Commissioned Purpose	Instructional
Operating System	Ubuntu Linux 12.04.5 LTS Server
Kernel	ubuntu 3.13.0-32-generic
Date Commissioned	Sunday May 24th, 2015
System	
Asset/Service Tag	-
Serial Number	-
Model	-
CPU	1 CPU/Core, 2.40Ghz Xeon E5645
RAM	256Mb
Main Hard drive	2GB SCSI
Secondary Hard drive	-
Additional Hard drives	-
Network	
Network Address	192.168.33.0/24
Domain	-
Configured Gateway	192.168.2.1
Configured DNS	192.168.2.1
Search Domains	-

Date	**Update History**
24/05/2015	System update

Configured Logical Volumes	**Size**		**Network Volumes**	**Location**
/dev/mapper/VG_01-root	291		SMB Export	/home/<*user*>
/dev/mapper/VG_01-usr	567		NFS file1 file server	/file1
/dev/mapper/VG_01-var	484			
/dev/mapper/VG_01-tmp	27			
/dev/mapper/VG_01-home	240			

Date	**Software Installed**
24/05/2015	System install
24/05/2015	man-db
24/05/2015	openssh-server
24/05/2015	traceroute
24/05/2015	byobu
24/05/2015	vim
24/05/2015	eLinks

Date	Software Installed
24/05/2015	samba smbfs
24/05/2015	exim4-daemon-light mailutils
24/05/2015	nmap
24/05/2015	tcpdump
24/05/2015	ossec 2.7.1

Date	Services Configured	Ports
24/05/2015	Install and network connectivity	
24/05/2015	openssh-server	22
24/05/2015	smbd nmbd	137-139, 445
24/05/2015	smtp	25
24/05/2015	ossec	*

Samba Configuration

```
[global]
   workgroup = WORKGROUP
   server string = ubuntu
   dns proxy = no
   log file = /var/log/samba/log.%m
   max log size = 1000
   syslog = 0
   panic action = /usr/share/samba/panic-action %d
   security = user
   username map = /etc/samba/smbusers
   encrypt passwords = true
   passdb backend = tdbsam
   obey pam restrictions = yes
   unix password sync = yes
   passwd program = /usr/bin/passwd %u
   passwd chat = *Enter\snew\s*\spassword:* %n\n *Retype\snew\s*\spassword:* %n\n *password\supdated\ssuccessfully* .
   pam password change = yes
   map to guest = bad user
   usershare allow guests = yes
[homes]
   comment = Home Directories
   browseable = yes
   read only = no
   valid users = %S
```

No.	Date	Major System Commands Run	Purpose
1	24/05/2015	`sudo apt-get update`	Update package lists
2	24/05/2015	`sudo apt-get upgrade`	Perform upgrade
3	24/05/2015	`sudo rm /var/lib/apt/lists/*`	Repair apt cache errors
4	24/05/2015	`sudo apt-get install -f`	Fix previous install errors
5	24/05/2015	`sudo apt-get install man-db`	Install man pages
6	24/05/2015	`sudo apt-get install openssh-server`	Install openssh-server
7	24/05/2015	`sudo apt-get install traceroute`	Install traceroute
8	24/05/2015	`sudo apt-get install byobu`	Install byobu client
9	24/05/2015	`sudo apt-get install vim`	Install VI iMproved
10	24/05/2015	`vi .vimrc`	Edit local vim config file

11	24/05/2015	***sudo apt-get install samba smbfs***	Install samba server
12	24/05/2015	***sudo vi /etc/samba/smb.conf***	Edit smb configuration to allow ~ sharing
13	24/05/2015	***sudo smbpasswd -a ubuntu***	Create smb password for user ubuntu
14	24/05/2015	***sudo vi /etc/samba/smbusers***	Add users to smbusers file
15	24/05/2015	***sudo testparm***	Check samba configuration
16	24/05/2015	***grep -i NETBIOS /etc/services***	Check new open ports
17	24/05/2015	***grep -i CIFS /etc/services***	Check new open ports
18	24/05/2015	***netstat -lnptu***	Verify ports are open
19	24/05/2015	***sudo apt-get install exim-daemon-light mailutils***	Install exim MTA
20	24/05/2015	***sudo dpkg-reconfigure exim4-config***	Configure exim for smarthost mail transfer using gmail
21	24/05/2015	***sudo vi /usr/bin/backup.sh***	Create backup script
22	24/05/2015	***sudo /usr/bin/backup.sh daily***	Run initial daily backup
23	24/05/2015	***sudo vi /etc/crontab***	Add backup jobs to system crontab
24	24/05/2015	***sudo apt-get install build-essential***	Install build tools
25	24/05/2015	***mkdir ossec***	Make ossec directory
26	24/05/2015	***cd ossec***	Change to issec directory
27	24/05/2015	***wget http://www.ossec.net/files/ossec-hids-2.7.tar.gz***	Download latest ossec binaries
28	24/05/2015	***tar -xvf ossec-hids-2.7.tar.gz***	Untar ossec binaries
29	24/05/2015	***cd ossec-hids-****	Change to ossec directory
30	24/05/2015	***sudo ./install.sh***	Make ossec
31	24/05/2015	***sudo apt-get purge build-essential***	Purge build-essential files
32	24/05/2015	***sudo apt-get autoremove***	Remove purged install files
33	24/05/2015	***sudo /var/ossec/bin/ossec-control start***	Start ossec
34	24/05/2015	***sudo groupadd -g 1002 support***	Add group “support”
35	24/05/2015	***sudo usermod -a -G support ubuntu***	Add Ubuntu to support group
36	24/05/2015	***sudo usermod -a -G backup ubuntu***	Add Ubuntu to backup group
37	24/05/2015	***sudo adduser support1***	Add User support1 with adduser script
38	24/05/2015	***sudo usermod -a -G support support1***	Add support1 to support group
39	24/05/2015	***sudo usermod -a -G backup ubuntu***	Add support1 to backup group
40	24/05/2015	***sudo vi /etc/login.defs***	Change password aging policy
41	24/05/2015	***sudo vi /etc/default/userad***	Change password aging policiy

42	24/05/2015	***sudo change –M 60 ubuntu***	Change password aging policy for ubuntu
43	24/05/2015	***sudo visudo***	Edit Visudo file
44	24/05/2015	***sudo smbpasswd –a support1***	Create smb password for user support1
45	24/05/2015	***echo "alias restorefiles='tar –xpjvf'" >> ~/.bash_aliases***	Add alias for simple file restore operation
6	24/05/2015	***sudo fdisk /dev/sdb***	Create partition on new hardrive
47	24/05/2015	***sudo mkfs –t ext4 /dev/sdb1***	Create filesystem on new harddrive
48	24/05/2015	***sudo vi fstab***	Edit fstab to mount new harddrive on /TommyToe/backup
49	24/05/2015	***sudo mount –a***	Remount fstab

Gateway/Firewall - Perimeter1 Settings

Information	
Host Name	perimeter1
Purpose	Network Gateway and Firewall
IP Address	LAN : 192.168.33.254 WAN : 192.168.2.254
Domain	-
Configured Gateway	192.168.2.254
Configured DNS	192.168.2.254
Search Domains	-
MAC Address	LAN : 08:00:27:48:8d:06 WAN: 08:00:27:7d:a8:3f

User	Groups	Shell	Uid	Full Name	Contact
ubuntu	ubuntu,support	/bin/bash	1000	Josh Cannons	admin@server.com
support1	support1,support	/bin/bash	1004	Support	support1@server.com

Group	Guid	Users	Purpose
ubuntu	1000	ubuntu	Admin
support	1002	support1,ubuntu	Support Users
backup	34	ubuntu, support1	Backup users

No.	Date	Major System Commands Run	Purpose
1	24/05/2015	***sudo apt-get install iptables***	Install iptables
2	24/05/2015	***sudo vi /etc/sysctl.conf***	Change kernel routing settings
3	24/05/2015	***sudo vi /etc/firewallrules.sh***	Create firewall rules script
4	24/05/2015	***sudo chmod +x /etc/firewallrules.sh***	Change file to executable
5	24/05/2015	***sudo chown root:root /etc/fierwallrules.sh***	Change ownership to root
6	24/05/2015	***sudo /etc/firewallrules.sh***	Load firewall rules
7	24/05/2015	***sudo apt-get install isc-dhcp-server***	Install ISC DHCP server
8	24/05/2015	***sudo vi /etc/default/isc-dhcp-server***	Set interface
9	24/05/2015	***sudo vi /etc/dhcp/dhcpd.conf***	Set static DHCP address scheme
10	24/05/2015	***sudo service isc-dhcp-server restart***	Restart DHCP server
11	24/05/2015	***sudo netstat -uap***	Confirm DHCP server is running
12	24/05/2015	***sudo service isc-dhcp-server stop***	Stop DHCP server

Date	Software Installed
24/05/2015	Iptables isc-dhcp-server

Date	Services Configured	Ports
24/05/2015	firewall	See below
24/05/2015	Packet forwarding	All
24/05/2015	isc-dhcp-server	43

DHCP Configuration

```
ddns-update-style none;
log-facility local7;
authoritative;

subnet 192.168.33.0 netmask 255.255.255.0 {
   range 192.168.33.1 192.168.33.253;
   option domain-name-servers 192.168.2.1;
   option routers 192.168.33.254;
   option broadcast-address 192.168.33.255;
   default-lease-time 600;
   max-lease-time 7200;
}

host ids1 {
  hardware ethernet 08:00:27:24:fc:70;
  fixed-address 192.168.33.250;
}

host web1 {
  hardware ethernet 08:00:27:ac:4a:61;
  fixed-address 192.168.33.251;
}

host file1 {
  hardware ethernet  08:00:27:00:cc:77;
  fixed-address 192.168.33.252;
}
```

Firewall	iptables
Ports Allowed	IN: 80,443,22 OUT: All
Ports Denied	IN: ALL OUT: None

Firewall Configuration

```
# User variables
GATEWAY_IP=192.168.2.254
LAN_IP=192.168.33.254
WEB=192.168.33.251
DHCP=192.168.33.253
FILE=192.168.33.252
IDS=192.168.33.250
LAN_INT=eth1
WAN_INT=eth0

# Flush all iptables rules and reset policies
iptables -t filter -F
iptables -t nat -F
iptables -t mangle -F
iptables -t raw -F
iptables -P INPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -P OUTPUT ACCEPT

# Drop all packets IN to gateway
iptables -P INPUT DROP
iptables -P FORWARD DROP

# Enable logging
iptables -A INPUT -i ${WAN_INT} -j LOG
iptables -A FORWARD -i ${WAN_INT} -j LOG

# Allow all internal connections OUT and allow stateful IN
iptables -I FORWARD -i ${LAN_INT} -p ALL -j ACCEPT
iptables -I FORWARD -i ${LAN_INT} -p ALL -j ACCEPT
iptables -I FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT

# Enable NAT on outgoing interface
iptables -t nat -A POSTROUTING -o ${WAN_INT} -j MASQUERADE
#iptables -t nat -A POSTROUTING -o ${WAN_INT} -j SNAT --to ${GATEWAY_IP}

# Allow ssh and http(s) IN to servers as required
iptables -I FORWARD -d 192.168.33.0/24 -p ICMP -j ACCEPT
iptables -I FORWARD -d ${FILE} -p tcp --dport 22 -j ACCEPT
iptables -I FORWARD -d ${LAN_IP} -p tcp --dport 22 -j ACCEPT
iptables -I FORWARD -d ${IDS} -p tcp --dport 22 -j ACCEPT
iptables -I FORWARD -d ${DHCP} -p tcp --dport 22 -j ACCEPT
iptables -I FORWARD -d ${WEB} -p tcp --dport 22 -j ACCEPT
iptables -A FORWARD -d ${WEB} -p tcp --dport 80 -j ACCEPT

# Allow NAT prerouting
iptables -t nat -A PREROUTING -p tcp -d ${GATEWAY_IP} --dport 80 -j DNAT --to ${WEB}:80

# Allow ssh TO gateway from the internal network
iptables -I INPUT -i ${LAN_INT} -d ${LAN_IP} -p tcp --dport 22 -j ACCEPT

```

```
52 # Allow loopback
53 iptables -I INPUT -i lo -d 127.0.0.1 -p ALL -j ACCEPT
54
55 # Allow ICMP TO gateway
56 iptables -I INPUT -i ${LAN_INT} -p icmp -j ACCEPT
57 iptables -I INPUT -i ${WAN_INT} -p icmp -j ACCEPT
58
59 # Allow SSH To gateway for TESTING
60 iptables -A INPUT -i ${WAN_INT} -d ${GATEWAY_IP} -p tcp --dport 22 -j ACCEPT
```

DHCP Server DHCP1 Settings

Network	
Host Name	dhcp1
Purpose	DHCP Server
IP Address	192.168.33.253
Domain	-
Configured Gateway	192.168.33.254
Configured DNS	192.168.33.254
Search Domains	-
MAC Address	LAN : 08:00:27:a5:78:38

No.	Date	Major System Commands Run	Purpose
1	24/05/2015	`sudo apt-get install isc-dhcp-server`	Install ISC DHCP server
2	24/05/2015	`sudo vi /etc/default/isc-dhcp-server`	Set interface
3	24/05/2015	`sudo vi /etc/dhcp/dhcpd.conf`	Set static DHCP address scheme
4	24/05/2015	`sudo service isc-dhcp-server restart`	Restart DHCP server
5	24/05/2015	`sudo netstat -uap`	Confirm DHCP server is running

User	Groups	Shell	Uid	Full Name	Contact
ubuntu	ubuntu,support	/bin/bash	1000	Josh Cannons	admin@server.com
support1	support1,support	/bin/bash	1004	Support	support1@server.com

Group	Guid	Users	Purpose
ubuntu	1000	ubuntu	Admin
support	1002	support1,ubuntu	Support Users
backup	34	ubuntu, support1	Backup users

Date	Software Installed
24/05/2015	Isc-dhcp-server

Date	Services Configured	Ports
24/05/2015	Isc-dhcp-server	43

DHCP Configuration

```
 1 ddns-update-style none;
 2 log-facility local7;
 3 authoritative;
 4
 5 subnet 192.168.33.0 netmask 255.255.255.0 {
 6    range 192.168.33.1 192.168.33.253;
 7    option domain-name-servers 192.168.2.1;
 8    option routers 192.168.33.254;
 9    option broadcast-address 192.168.33.255;
10    default-lease-time 600;
11    max-lease-time 7200;
```

```
12 }
13
14 host ids1 {
15   hardware ethernet 08:00:27:24:fc:70;
16   fixed-address 192.168.33.250;
17 }
18
19 host web1 {
20   hardware ethernet 08:00:27:ac:4a:61;
21   fixed-address 192.168.33.251;
22 }
23
24 host file1 {
25   hardware ethernet  08:00:27:00:cc:77;
26   fixed-address 192.168.33.252;
27 }
```

Intrusion Detection Server IDS1 Settings

Network	
Host Name	ids1
Purpose	IDS Security
IP Address	Static DHCP 192.168.33.250
Domain	-
Configured Gateway	192.168.33.254
Configured DNS	192.168.33.254
Search Domains	-
MAC Address	LAN : 08:00:27:24:fc:70

User	Groups	Shell	Uid	Full Name	Contact
ubuntu	ubuntu,support	/bin/bash	1000	Josh Cannons	admin@server.com
support1	support1,support	/bin/bash	1004	Support	support1@server.com

Group	Guid	Users	Purpose
ubuntu	1000	ubuntu	Admin
support	1002	support1,ubuntu	Support Users
backup	34	ubuntu, support1	Backup users

No.	Date	Major System Commands Run	Purpose
1	24/05/2015	`sudo apt-get install snort`	Install snort
2	24/05/2015	`sudo cp /etc/snort/snort.conf /etc/snort/snort.conf.orig`	Backup snort original file
3	24/05/2015	`sudo vi /etc/snort/snort.conf`	Configure snort for local interface
4	24/05/2015	`sudo service snort start`	Start snort
5	24/05/2015	`sudo ps ax|grep snort`	Validate snort running

Date	Software Installed
24/05/2015	snort

Date	Services Configured	Ports
24/05/2015	snort	All

Snort Configuration (all other lines default)

```
1 # Setup the network addresses you are protecting
2 ipvar HOME_NET 192.168.33.0/24
```

Web Server Web1 Settings

Network	
Host Name	web1
Purpose	Web Server
IP Address	Static DHCP 192.168.33.251
Domain	-
Configured Gateway	192.168.33.254
Configured DNS	192.168.33.254
Search Domains	-
MAC Address	LAN : 08:00:27:ac:4a:61

User	Groups	Shell	Uid	Full Name	Contact
developer1	devloper1,developer	/bin/bash	1004	Web Developer	developer1@server.com
ubuntu	ubuntu,support	/bin/bash	1000	Josh Cannons	admin@server.com
support1	support1,support	/bin/bash	1005	Support	support1@server.com

Group	Guid	Users	Purpose
webdev	1003	developer1	Web Development
ubuntu	1000	ubuntu	Admin
support	1002	support1,ubuntu	Support Users
backup	34	ubuntu, support1	Backup users

No.	Date	Major System Commands Run	Purpose
1	24/05/2015	***sudo apt-get install lighttpd php5-cgi apache2-utils***	Install lighttpd web server with php and apache additions
2	24/05/2015	***sudo lighty-enable-mod fastcgi***	Enable fastcgi
3	24/05/2015	***sudo lighty-enable-mod fastcgi-php***	Enable php
4	24/05/2015	***sudo service lighttpd force-reload***	Reload lighttpd service
5	24/05/2015	***echo "<?php phpinfo(); ?>" | sudo tee /var/www/index.php***	Create index.php information page

Date	Software Installed
24/05/2015	lighttpd php5-cgi apache2-utils

Date	Services Configured	Ports
24/05/2015	lighttpd	80,443