**IEC Chapter 1 Assignment**

**By Ahmed\_Pinger**

**The Configuration:**

**Configuring Rsyslog Server:**

**Step 1.**  Setup 3 machines in any virtualization software such as VMware of Virtual Box

1. Linux Client
2. Linus Based Rsyslog Server
3. Window client

**Step 2.** Move forward to your Rsyslog Server and configure it, I can’t mention every single configuration command because it will become very lengthy

So after configuring server use the following Command to Complete IP tables requirement:

1. iptables -I INPUT -p tcp -s [Your Client IP Address] --dport 514 -j ACCEPT
2. iptables -I INPUT -p udp -s [Your Client IP Address] --dport 514 -j ACCEPT
3. iptables -I INPUT -p tcp -s 0.0.0.0/0 --dport 514 -j DROP
4. service iptables save

the first command will be allowing traffic from TCP and port 514 and second command same purpose for UDP and the third command to block any other traffic on this port and the final Command will be used to save your configuration.

**Configuring Linux Client:**

**Step 1.** The first step should be installing ftp, auditd, and rsyslog so can be further,  
 so after installing do enable FTP service and setup FTP service, then do some basic configuration of auditd like enabling and starting etc, and do them for rsyslog as well, then after doing basic things set some rules for auditing which are listed below with the standard source:

1. -w /var/log/auth.log -p arwx -k Auth.log\_Perm\_CH
2. -w /var/log/messages -p arwx -k Messages\_Perm\_CH
3. -w /etc/shadow -p arwx -k Shadow\_Perm\_CH
4. -w /usr/sbin/adduser -p x -k user\_modification
5. -w /etc/passwd -p wa -k passwd\_Mod

***Source Link:*** [*https://github.com/alphagov/puppet-auditd/pull/1*](https://github.com/alphagov/puppet-auditd/pull/1)

These logs will do some auditing,

1. It logs when auth.log will be access or the permission of this file will change
2. It logs when messages will be access or the permission of this file will change
3. It logs when shadow will be access or the permission of this file will change
4. It logs when any new user will be added in system
5. It logs when any password related work happens in system

**Step 2.** After adding these rules save them and add the log entry in rsyslog.conf file with following steps:

1. #audit log
2. $ModLoad imfile
3. $InputFileName /var/log/audit/audit.log
4. $InputFileTag tag\_audit\_log:
5. $InputFileStateFile audit\_log
6. $InputFileSeverity info
7. $InputFileFacility local6
8. $InputRunFileMonitor

Add the whole conde in this file this code will add audit faculty in rsyslog file

Then add the following at the end of file

1. local6.\* @**[Your Rsyslog server Ip Address]**:514 # Use @ for UDP protocol
2. local6.\* @@**[Your Rsyslog server Ip Address]**:514 # Use @@ for TCP protocol
3. ftp.\* @**[Your Rsyslog server Ip Address]**:514 # Use @ for UDP protocol
4. ftp.\* @@**[Your Rsyslog server Ip Address]**:514 # Use @@ for TCP protocol

This will only send your FTP and audit logs to Rsyslog server as per requirement.

**Step 3.** And that’s it now you can view you logs in rsyslog server from the following command.

1. **tail -f /var/log/messages**

this command will show you live logs from you client.

**Configuring Windows Client:**

**Step 1.** First of install your rsyslog Agent and configure it to send filtered logs to Rsyslog Server

**Step 2.** Then configure the following commands in CMD

logman create trace -n usbtrace -o %SystemRoot%\Tracing\usbtrace.etl -nb 128 640 -bs 128

logman update trace -n usbtrace -p Microsoft-Windows-USB-USBXHCI (Default,PartialDataBusTrace)

logman update trace -n usbtrace -p Microsoft-Windows-USB-UCX (Default,PartialDataBusTrace)

logman update trace -n usbtrace -p Microsoft-Windows-USB-USBHUB3 (Default,PartialDataBusTrace)

logman update trace -n usbtrace -p Microsoft-Windows-USB-USBPORT

logman update trace -n usbtrace -p Microsoft-Windows-USB-USBHUB

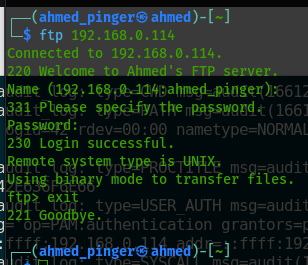
logman update trace -n usbtrace -p Microsoft-Windows-Kernel-IoTrace 0 2

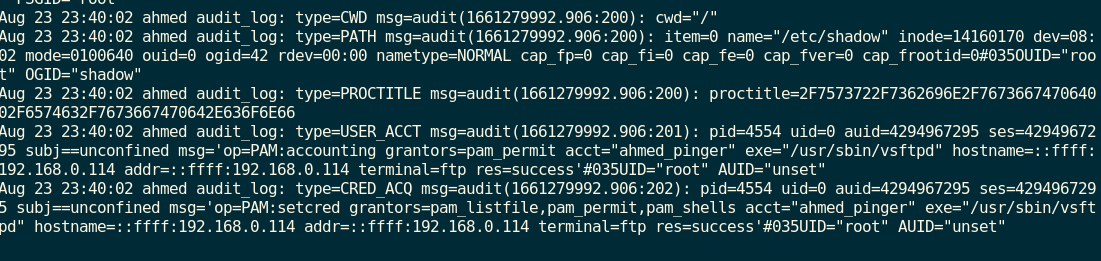
logman start -n usbtrace

this configuration can be done in CMD and AD DS as well, this configuration will be generating a file called usbtrace.etl which include all of the USB Activity and can be easily open in event viewer.

|--------------------------------------------------------------X---------------------------------------------------------------

**Q.1.** Yes, I was able to Aggregate logs from Linux client but I was not able to configure Rsyslog Agent In windows client.





**Q.1.1.** As mentioned previously I was not able to log from windows client.

**Q.2.** Yes, we can write rule in the following files:

**#/etc/pam.d/system-auth  
#/etc/pam.d/password-auth**

Rules should be:

**auth required pam\_faillock.so preauth silent audit deny=3 unlock\_time=600  
auth [default=die] pam\_faillock.so authfail audit deny=3 unlock\_time=600**

**Explanation:**

These rules will block user account for 600 Seconds if user failed to login for 3 times

**Q.3.** The Advantage are that we can obtain only required logs and does not get all of the logs e.g. service start logs, login log, like every single log.

**Q.4.** Yes, while using syslog program we can aggregate only Authentication events by adding auditing rule which is listed below:

**-w /var/log/auth.log -p arwx -k Auth.log\_Perm\_CH**

**Q.5.** The device control is one of the most important control because if anyone among of employees of out siders insert malicious USB In any system it can easily bypass all of your Preventative Controls e.g. IPS, Firewall etc. So it should be very strict rule that not to insert any USB in any system.

**Some of my configuration is listed below:**

logman create trace -n usbtrace -o %SystemRoot%\Tracing\usbtrace.etl -nb 128 640 -bs 128

logman update trace -n usbtrace -p Microsoft-Windows-USB-USBXHCI (Default,PartialDataBusTrace)

logman update trace -n usbtrace -p Microsoft-Windows-USB-UCX (Default,PartialDataBusTrace)

logman update trace -n usbtrace -p Microsoft-Windows-USB-USBHUB3 (Default,PartialDataBusTrace)

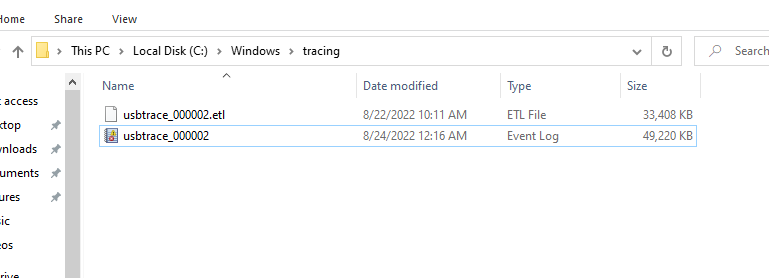
logman update trace -n usbtrace -p Microsoft-Windows-USB-USBPORT

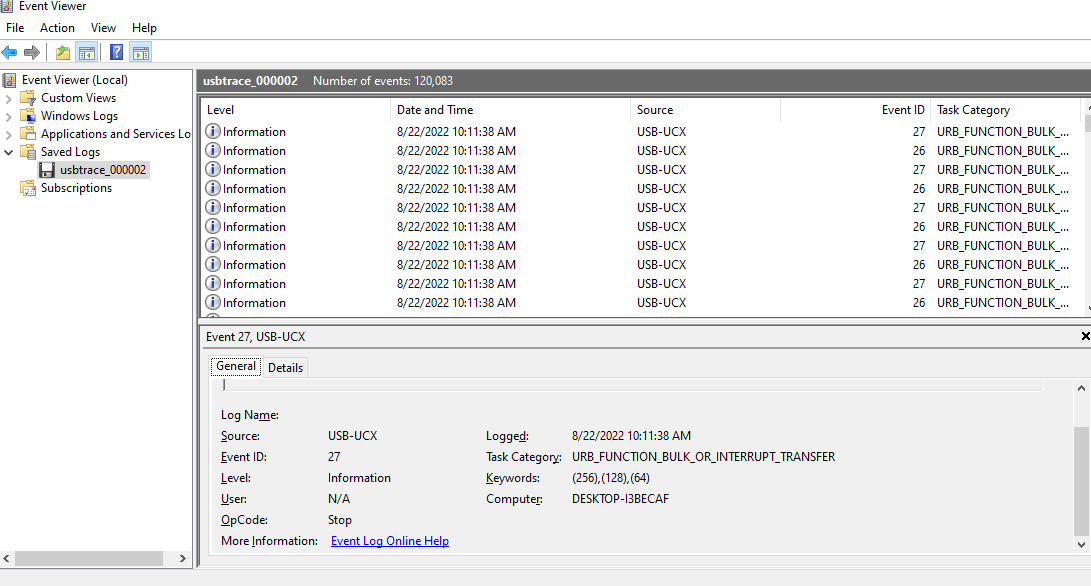
logman update trace -n usbtrace -p Microsoft-Windows-USB-USBHUB

logman update trace -n usbtrace -p Microsoft-Windows-Kernel-IoTrace 0 2

logman start -n usbtrace

this configuration can be done in CMD and AD DS as well, this configuration will be generating a file called usbtrace.etl which include all of the USB Activity and can be easily open in event viewer.





**Topology Diagram:**

