Alex Arnold

Professor Torres

04-22-25

IT 0115-41197

Lab 12

Part A: [Netlab 3Links to an external site.](https://netlabve3.flc.losrios.edu/), 70-742, Lab01

* Log on to the Windows 2016 box.
  + Access the event viewer logs of the DCB from the DCA Box

A screen shot of a computer

AI-generated content may be incorrect.

A blue rectangular sign with white text

AI-generated content may be incorrect.

Com+ and remote event log management rules enabled to allow for remote administration

A computer screen shot of a computer screen

AI-generated content may be incorrect.

Access to logs on DCB from DCA without joining domain

Access the DCA box. Windows 10 A is already joined to this box. Join DCB to this domain  
A screenshot of a computer

AI-generated content may be incorrect.

DCB joined to DCA domain

* + - Access DCB via PowerShell on the DCA. Using PowerShell:
      * list out the main event viewer areas.

A blue screen with white text

AI-generated content may be incorrect.

* + - * Discuss what type of events are found in the major areas of the Event Viewer logs
* System - OS-level events: driver issues, shutdowns, service failures
* Application - Logs from apps like SQL Server, Exchange, or custom software
* Security - Audit logs: login attempts, policy changes, access violations (if auditing is enabled)
* Directory Services – (Only on Domain Controllers) Changes to directory partitions, domain controller promotion or demotion
* Hardware – CPU or memory faults, disk failures, BIOS or firmware issues
* Powershell – Command execution, script errors
  + - * Save your output to a text file



A screenshot of a computer program

AI-generated content may be incorrect.

Part B: [Netlab 2Links to an external site.](https://netlabve2.flc.losrios.edu/) NISGTC Linux+ Series 1, Lab 02 (pick a system)

* Research and discuss what types of logs are found in the /var/log section on Linux distributions in general

**/var/log/messages** General system messages: boot, hardware, kernel, cron jobs, etc. (on many distros except Debian-based)

**/var/log/syslog**  General system activity logs (Debian/Ubuntu equivalent of /var/log/messages)

**/var/log/auth.log** Authentication logs: sudo use, SSH logins, failed login attempts (Debian/Ubuntu)

**/var/log/secure**  Authentication and security logs (RHEL/CentOS/Fedora equivalent of auth.log)

**/var/log/dmesg** Kernel ring buffer: hardware detection messages from boot

**/var/log/kern.log** Kernel-specific logs (useful for kernel debugging)

**/var/log/boot.log** Boot-related service startup messages

**/var/log/faillog** Failed login attempts (binary format, use faillog command to read)

**/var/log/lastlog** Info about last logins (binary, view with lastlog)

**/var/log/wtmp** Login/logout activity (binary, use who, w, or last to read)

**/var/log/btmp** Failed login attempts (binary, view with lastb)

**/var/log/yum.log** Package installation via YUM (on RHEL/CentOS)

**/var/log/apt/** Logs from apt package manager (Ubuntu/Debian)

**/var/log/httpd/** Apache logs (access\_log, error\_log) for Red Hat-based systems

**/var/log/apache2/** Apache logs on Debian-based systems

**/var/log/mysql/** MySQL/MariaDB logs (general log, error log, slow query log)

**/var/log/cron or cron.log** Logs of scheduled jobs via cron

**/var/log/Xorg.0.log** X server (GUI) startup log

**/var/log/mail.log or maillog** Logs from mail server (Postfix, Sendmail, etc.)

**/var/log/audit/**  Audit framework logs (if auditd is installed and enabled)

**/var/log/ufw.log** UFW (Uncomplicated Firewall) logs (Ubuntu systems)

* Log on to the Ubuntu box. Research how to run the below commands, and run them against any log within /var/log. Discuss what you are trying to do and your findings (your research into these commands will help with this):
  + Sed – used to replace, delete, or change text in a file / input stream



* + Grep – searches for lines that match a pattern in a file



* + Awk - can extract fields, format output, or perform calculations on structured text (like logs).

A screen shot of a computer

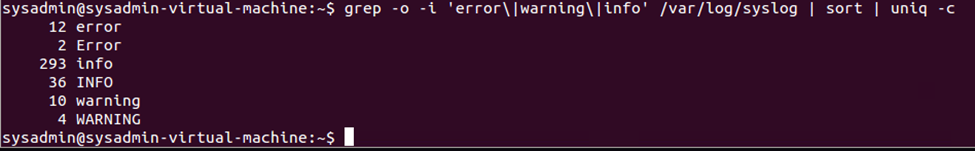
AI-generated content may be incorrect.

* + Uniq - removes duplicate adjacent lines or counts occurrences.

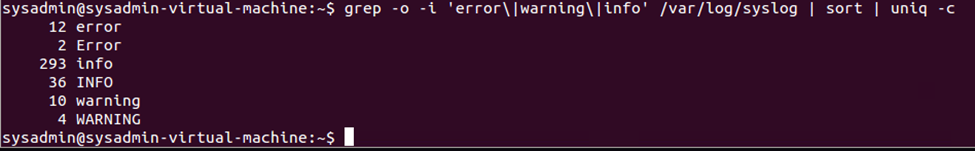
A computer screen shot of a error

AI-generated content may be incorrect.

* + Sort - orders lines alphabetically or numerically.



* Combine two or more of the above commands and run it against any log within /var/log. Discuss what you are trying to do and your findings (your research into these commands will help with this):



This command takes the syslog file and searches for error warning and info log level alerts then sorts them alphabetically using the sort command. After this the uniq command takes all of the duplicate matching words and removes them adding a count for each one. This can give you an overview of the number of each kind of theses alerts that have been generated by the system.

Part C: Windows Security Policy

* Using PowerShell and the benchmark for the Windows 2016 OS
  + Create a script that will enforce five (5) security policies (any policy)

I went a bit overboard as I plan to use this in the security class as well.

function Set-NetAccountPolicy {

param (

[string]$Description,

[string]$Command,

[string]$VerifyMatch

)

try {

Write-Host "`n$Description..." -ForegroundColor Cyan

Invoke-Expression $Command

Start-Sleep -Seconds 1

net accounts | Select-String $VerifyMatch

Write-Host "$Description successfully applied." -ForegroundColor Green

} catch {

Write-Host "Failed to apply: $Description. Error: $\_" -ForegroundColor Red

}

}

function Set-AuditPolicy {

param (

[string]$Subcategory,

[string]$Success = "enable",

[string]$Failure = $null

)

try {

Write-Host "`nConfiguring audit policy: $Subcategory..." -ForegroundColor Cyan

$cmd = "AuditPol /set /subcategory:`"$Subcategory`" /success:$Success"

if ($Failure) {

$cmd += " /failure:$Failure"

}

Invoke-Expression $cmd

Start-Sleep -Seconds 1

AuditPol /get /subcategory:"$Subcategory"

Write-Host "Audit policy '$Subcategory' successfully set." -ForegroundColor Green

} catch {

Write-Host "Failed to set audit policy '$Subcategory'. Error: $\_" -ForegroundColor Red

}

}

# --- Password Policy ---

Set-NetAccountPolicy "Setting password history to 24 passwords" 'net accounts /uniquepw:24' "Password history length"

Set-NetAccountPolicy "Setting maximum password age to 60 days" 'net accounts /maxpwage:60' "Maximum password age"

Set-NetAccountPolicy "Setting minimum password age to 1 day" 'net accounts /minpwage:1' "Minimum password age"

Set-NetAccountPolicy "Setting minimum password length to 14 characters" 'net accounts /minpwlen:14' "Minimum password length"

# --- Audit Policies ---

Set-AuditPolicy "Credential Validation" "enable" "enable"

Set-AuditPolicy "Kerberos Authentication Service" "enable" "enable"

Set-AuditPolicy "Kerberos Service Ticket Operations" "enable" "enable"

Set-AuditPolicy "Application Group Management" "enable" "enable"

Set-AuditPolicy "Computer Account Management" "enable"

Set-AuditPolicy "User Account Management" "enable" "enable"

# --- Account Lockout Policies ---

Set-NetAccountPolicy "Setting account lockout duration to 15 minutes" 'net accounts /lockoutduration:15' "Lockout duration"

Set-NetAccountPolicy "Setting account lockout threshold to 5 attempts" 'net accounts /lockoutthreshold:5' "Lockout threshold"

Set-NetAccountPolicy "Setting reset account lockout counter after 15 minutes" 'net accounts /lockoutwindow:15' "Lockout observation window"

Part D: Linux Security Policy

* Using Bash Scripting or Python and the benchmark for the Ubuntu distro
  + Create a script that will enforce five (5) security policies (any policy)

#!/bin/bash

echo -e "\n--- SSH Grace Time---"

grep "^LoginGraceTime" /etc/ssh/sshd\_config

echo -e "\n--- SSH ACCESS Limited---"

grep "^AllowUsers" /etc/ssh/sshd\_config

grep "^AllowGroups" /etc/ssh/sshd\_config

grep "^DenyUsers" /etc/ssh/sshd\_config

grep "^DenyGroups" /etc/ssh/sshd\_config

echo -e "\n--- Lockout for Failed Password---"

grep "pam\_tally2" /etc/pam.d/common-auth

echo -e "\n--- Password Hash algorithm---"

egrep '^password\s+\S+\s+pam\_unix.so' /etc/pam.d/common-password

echo -e "\n--- Shadow PW Peramiters---"

grep PASS\_MAX\_DAYS /etc/login.defs

grep PASS\_MIN\_DAYS /etc/login.defs

grep PASS\_WARN\_AGE /etc/login.defs

echo -e "\n--- Ensure system accounts are non-login ---"

egrep -v "^\+" /etc/passwd | awk -F: '($1!="root" && $1!="sync" && $1!="shutdown" && $1!="halt" && $3<1000 && $7!="/usr/sbin/nologin" && $7!="/bin/false") {print}'

echo -e "\n--- Ensure access to the su command is restricted ---"

grep pam\_wheel.so /etc/pam.d/su

grep wheel /etc/group

echo -e "\n--- verify file permissions ---"

stat /etc/passwd

stat /etc/shadow

stat /etc/group

echo -e "\n--- Ensure core dumps are restricted ---"

grep "hard core" /etc/security/limits.conf /etc/security/limits.d/\*

sysctl fs.suid\_dumpable

grep "fs\.suid\_dumpable" /etc/sysctl.conf /etc/sysctl.d/\*

echo -e "\n--- Ensure DHCP Server is not enabled ---"

initctl show-config isc-dhcp-server

initctl show-config isc-dhcp-server6

echo -e "\n--- Ensure LDAP server is not enabled ---"

ls /etc/rc\*.d/S\*slapd

echo -e "\n--- Ensure DNS Server is not enabled ---"

ls /etc/rc\*.d/S\*bind9

echo -e "\n--- Ensure FTP Server is not enabled ---"

initctl show-config vsftpd

echo -e "\n--- Ensure HTTP server is not enabled ---"

ls /etc/rc\*.d/S\*apache2

echo -e "\n--- Ensure IMAP and POP3 server is not enabled ---"

initctl show-config dovecot

echo -e "\n--- Ensure Samba is not enabled ---"

initctl show-config smbd

echo -e "\n--- Ensure SNMP Server is not enabled ---"

ls /etc/rc\*.d/S\*snmpd

echo -e "\n--- Ensure telnet client is not installed ---"

dpkg -s telnet