Colby Heilner
Professor Torres
10/14
IT 120

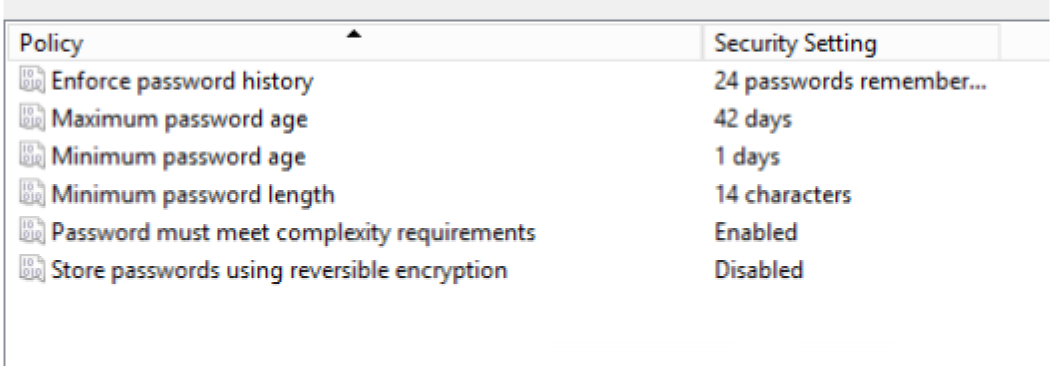
Lab 8

Part A: NetlabLinks to an external site.

Log on to NetlabNDG Security+ v3, Lab 01, Investigating ARP Poisoning, Windows 2012R2, and adjust the security utilizing the Windows Benchmark settings below. Capture a screenshot of the results of each major command. If you cannot enforce any of the policies, state why. Utilizing Windows benchmark, adjust the security policy for the below utilizing CIS benchmarkLinks to an external site.:

1.1 Password Policy:

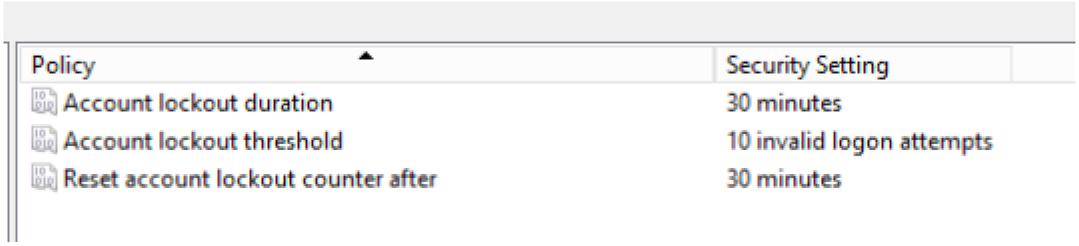
- 1.1.1 (L1) Ensure 'Enforce password history' is set to '24 or more password(s)'
- 1.1.2 (L1) Ensure 'Maximum password age is set to '60 or fewer days, but not 0'
- 1.1.3 (L1) Ensure 'Minimum password age is set to '1 or more day(s)'
- 1.1.4 (L1) Ensure 'Minimum password length is set to '14 or more character(s)'
- 1.1.5 (L1) Ensure 'Password must meet complexity requirements' is set to 'Enabled'



Policy	Security Setting
Enforce password history	24 passwords remember...
Maximum password age	42 days
Minimum password age	1 days
Minimum password length	14 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

1.2 Account Lockout Policy

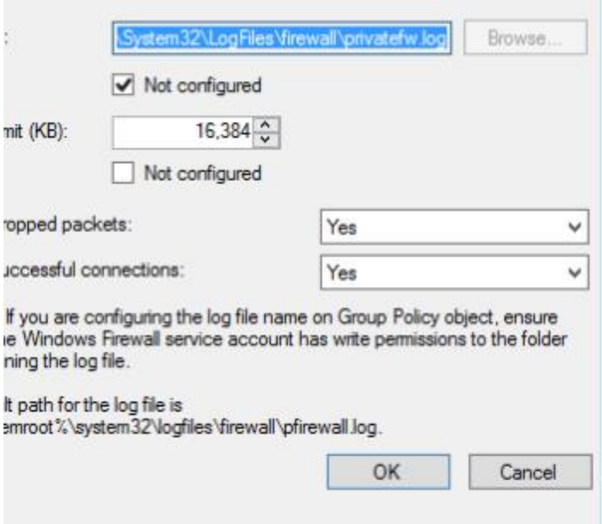
- 1.2.1 (L1) Ensure 'Account lockout duration' is set to '15 or more minute(s)'
- 1.2.2 (L1) Ensure 'Account lockout threshold is set to '10 or fewer invalid logon attempt(s), but not 0'
- 1.2.3 (L1) Ensure 'Reset account lockout counter after' is set to '15 or more minute(s)'



Policy	Security Setting
Account lockout duration	30 minutes
Account lockout threshold	10 invalid logon attempts
Reset account lockout counter after	30 minutes

9.2 Private Profile

- 9.2.8 (L1) Ensure 'Windows Firewall: Private: Logging: Name' is set to '%SYSTEMROOT%\System32\logfiles\firewall\privatefw.log' (Scored)
- 9.2.9 (L1) Ensure 'Windows Firewall: Private: Logging: Size limit (KB)' is set to '16,384 KB or greater' (Scored)
- 9.2.10 (L1) Ensure 'Windows Firewall: Private: Logging: Log dropped packets' is set to 'Yes' (Scored)



: System32\LogFiles\Firewall\privatefw.log

☑ Not configured

mit (KB): 16,384

☐ Not configured

ropped packets: Yes

uccessful connections: Yes

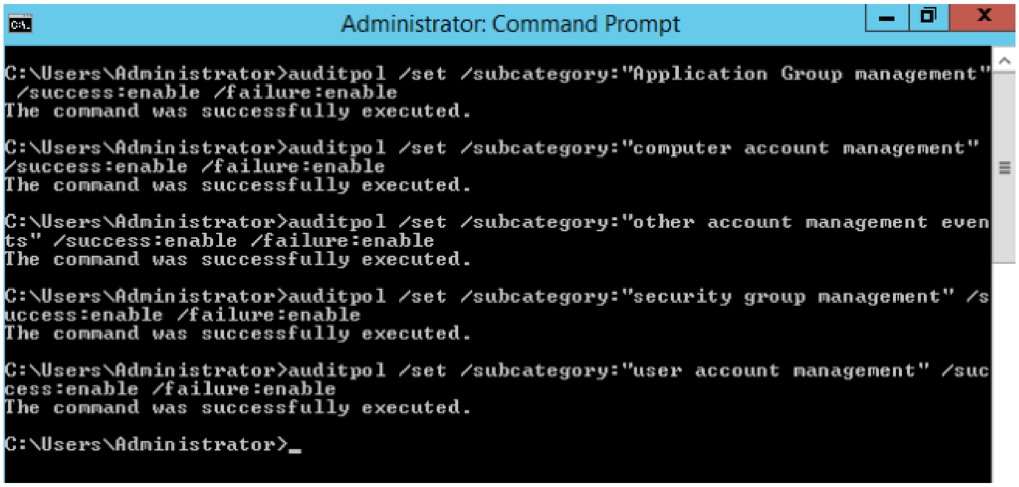
If you are configuring the log file name on Group Policy object, ensure
ie Windows Firewall service account has write permissions to the folder
ning the log file.

lt path for the log file is
emroot%\system32\logfiles\firewall\pfirewall.log.

17.2 Account Management (Tricky one, take your time, it is there. The path is different)

- 17.2.1 (L1) Ensure 'Audit Application Group Management' is set to 'Success and Failure'

- 17.2.2 (L1) Ensure 'Audit Computer Account Management' is set to 'Success and Failure'
- 17.2.3 (L1) Ensure 'Audit Other Account Management Events' is set to 'Success and Failure'
- 17.2.4 (L1) Ensure 'Audit Security Group Management' is set to 'Success and Failure'
- 17.2.5 (L1) Ensure 'Audit User Account Management' is set to 'Success and Failure'



```
C:\Users\Administrator>auditpol /set /subcategory:"Application Group management"
 /success:enable /failure:enable
The command was successfully executed.

C:\Users\Administrator>auditpol /set /subcategory:"computer account management"
/success:enable /failure:enable
The command was successfully executed.

C:\Users\Administrator>auditpol /set /subcategory:"other account management even
ts" /success:enable /failure:enable
The command was successfully executed.

C:\Users\Administrator>auditpol /set /subcategory:"security group management" /s
uccess:enable /failure:enable
The command was successfully executed.

C:\Users\Administrator>auditpol /set /subcategory:"user account management" /suc
cess:enable /failure:enable
The command was successfully executed.

C:\Users\Administrator>_
```

18.9.26.1 Application

- 18.9.26.1.1 (L1) Ensure 'Application: Control Event Log behavior when the log file reaches its maximum size is set to 'Disabled' (Scored)
- 18.9.26.1.2 (L1) Ensure 'Application: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater (Scored)

18.9.26.2 Security

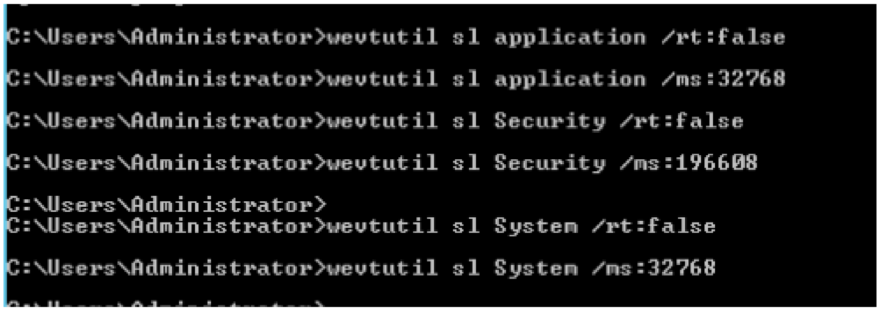
- 18.9.26.2.1 (L1) Ensure 'Security: Control Event Log behavior when the log file reaches its maximum size is set to 'Disabled' (Scored)

- 18.9.26.2.2 (L1) Ensure 'Security: Specify the maximum log file size (KB)' is set to 'Enabled: 196,608 or greater' (Scored)

18.9.26.4 System

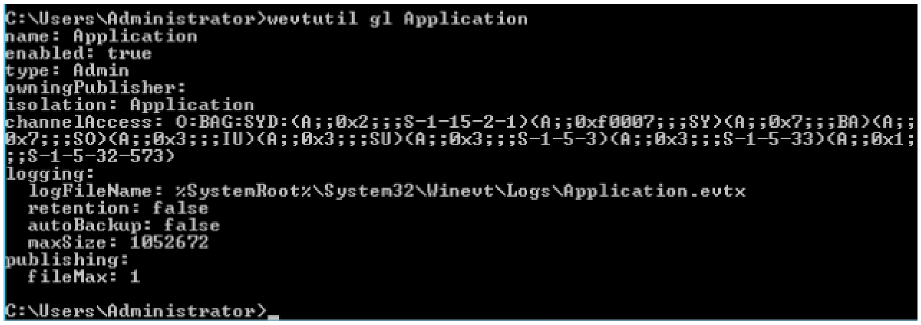
- 18.9.26.4.1 (L1) Ensure 'System: Control Event Log behavior when the log file reaches its maximum size is set to 'Disabled' (Scored)
- 18.9.26.4.2 (L1) Ensure 'System: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater (Scored)

  All above here



```
C:\Users\Administrator>wevtutil sl application /rt:false

C:\Users\Administrator>wevtutil sl application /ms:32768

C:\Users\Administrator>wevtutil sl Security /rt:false

C:\Users\Administrator>wevtutil sl Security /ms:196608

C:\Users\Administrator>
C:\Users\Administrator>wevtutil sl System /rt:false

C:\Users\Administrator>wevtutil sl System /ms:32768
```

How to verify



```
C:\Users\Administrator>wevtutil gl Application
name: Application
enabled: true
type: Admin
owningPublisher:
isolation: Application
channelAccess: O:BAG:SYD:(A;;0x2;;;S-1-15-2-1)(A;;0xf0007;;;SY)(A;;0x7;;;BA)(A;;
0x7;;;SO)(A;;0x3;;;IU)(A;;0x3;;;SU)(A;;0x3;;;S-1-5-3)(A;;0x3;;;S-1-5-33)(A;;0x1;
;;S-1-5-32-573)
logging:
  logFileName: %SystemRoot%\System32\Winevt\Logs\Application.evtx
  retention: false
  autoBackup: false
  maxSize: 1052672
publishing:
  fileMax: 1

C:\Users\Administrator>_
```

Part B:

For this part, review the videos below and give your opinion. For best results, try running all of the commands on your Linux system or in Netlab

- Intro to LinuxLinks to an external site.
- Linux DistributionsLinks to an external site.
- Linux CommandsLinks to an external site.
- Linux LogsLinks to an external site.

- Linux NetworkingLinks to an external site.

I watched the video on logs and got some good knowledge. He was trying to view ssh logs but they were in binary. So he said that we should specify sudo for priv access and lastb
For last “bad” attempt to login. Looking something like this
Sudo lastb -adF
Where -adF is helping with the formatting of the logs entries.

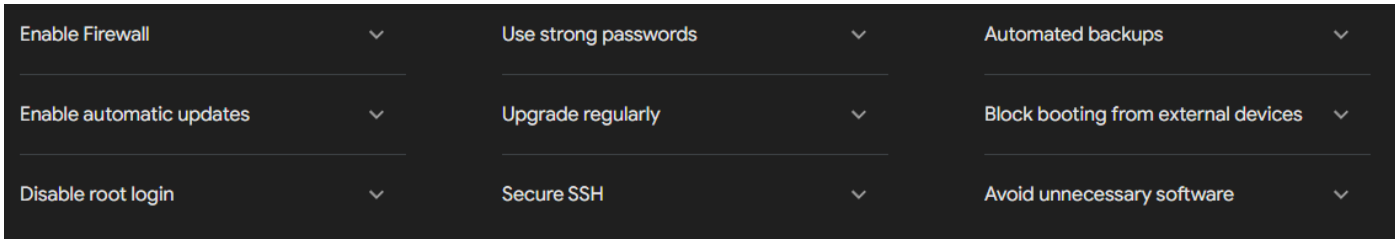
I also learned some good things about different Linux distros. Its best to think what you use your computer and get a distro to fit you best.

Part C:

- Search the internet for "Best Practices" on Linux systems:
  - List 10 best practices for Linux
  - Perform 5 of the best practices on NetlabNDG Security+ v3, Lab 01 -The Ubuntu system

I found a PDF of a bunch of good practices, here is some on SSH and keys
Best Practice Recommendations:
● Eliminate static SSH Keys in favor of one-time client certificates minted on-demand.
● Reduce Public Key Infrastructure (PKI) management complexity by abstracting through a SaaS layer
● Restrict non-certificate access to certain groups, eliminate authorized_keys for individual users and only keep a single admin “break glass” key stored in a vault for emergency situations.
The way I understand this is, Require both key systems for ssh login as well as a password username. That way you don't have to worry about brute force for passwords but it's not as Big of a risk of private keys getting leaked. (still is)

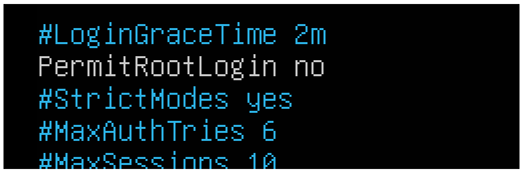
These quick tabs in linux also are good to see. Most of them are self explanitory but the disable root login is one I have not thought of.



- Enable Firewall
- Enable automatic updates
- Disable root login
- Use strong passwords
- Upgrade regularly
- Secure SSH
- Automated backups
- Block booting from external devices
- Avoid unnecessary software

Another thing I was curious about then I saw this was, where is the setting “block booting from external devices” is held.

Here is me changing my permit root login for ssh



```
#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
```

I tried to go into my vms and for some reason my pfsense firewall would not boot. So no internet access for now. But I attempted to install ufw onto my ubuntu server and configure it. Also while my pfsense firewall VM was working, I was doing the CIS benchmark for it. I changed **the allow any lan to any** rule to disabled. And then I added things that my employees may need to access on the internet (http https dns dnstls). I am also able to deny access to my DMZ to make sure it stays separate. I also gave my admin pc ‘192.168.1.3” more permissions to allow me to configure and setup more from it.

Overall the CIS controls have been really interesting for me so far. It's cool to walk thought and see all the “best” settings for security on different apps and operating systems.

Extra Credit: 5 points

Implement 5 Windows controls via the command line or PowerShell

See above.