

LAB BOOK 1
INFO-8835-23W.
FUNDAMENTAL OF
INFORMATIONSECURITY
NAME: IKEM MERCY OGECHI
STUDENT ID: 8859960
PROFESSOR NAME: PROFESSOR Allen
DUE DATE: FEBRUARY 5TH 2023

[Contents](#)

REMOTE ACCESS POLICY VIA SSH AND SSL.....	2
1.0 Overview	2
2.0 Purpose:	2
3.0 Scope:	2
4.0 Policy:	3
5.0 Definition:.....	3
6.0 Responsibilities:	4
7.0 Penalty:.....	4
8.0 Screenshot.....	4
9.0 Revision History.....	7
PASSWORD POLICY	7
1.0 Overview.....	7
2.0 Purpose:	7
3.0 Scope:	7
4.0 Policy:	7
5.0 Definition:.....	9
6.0 Responsibilities:	9
7.0 Penalty:.....	9

8.0 Screenshot.....	10
9.0 Revision History.....	13
PATCH MANAGEMENTS.....	13
1.0 Overview	13
2.0 Purpose:	13
3.0 Scope:	13
4.0 Policy:	13
5.0 Definition:.....	14
6.0 Responsibilities:	14
7.0 Penalty:.....	15
8.0 Screenshot.....	15
9.0 Revision History	17
10.0 References	18

REMOTE ACCESS POLICY VIA SSH AND SSL

1.0 Overview:

The computer environment of today frequently requires access to information resources outside of the office. The procedure of connecting to internal resources from an external source is referred to as remote access. Productivity is increased by having safe access to corporate resources from a distance.

2.0 Purpose:

This policy specifies the requirements for APEX workers to connect to the APEX network from a distant location. These guidelines are intended to reduce possible risks such as the loss of sensitive information due to unauthorized usage and malicious attacks that might compromise the integrity of APEX data.

3.0 Scope:

All APEX employees who access, configure, maintain, and support remote connections to the APEX network are subject to the terms of this policy.

4.0 Policy:

The company's IT department oversees all remote access security operations. The IT department must receive the needs from other business units for secure remote access for APEX employees and contractors through SSH and SSL. The IT department further declares that it will conduct its business in accordance with the relevant industry standards for the security of remote access.

- ❖ SSH secure remote access must be tightly regulated. Public/private keys will be controlled via one-time password authentication for strong passphrases. See the password policy for details on generating a strong passphrase.
- ❖ A username and password should be assigned to APEX workers and users with remote access privileges through ssh.
- ❖ At no time is it permitted to reconfigure a home user's equipment for the purpose of split-tunneling.
- ❖ The standards for APEX-owned equipment for remote access must be met by any personal equipment used to connect to APEX business networks.
- ❖ Approved access restrictions, such as authentication rules, role-based access, and data encryption, must be supported by remote access security protocols.
- ❖ Remote access security plans and procedures must be reviewed and tested on a regular basis in an appropriate environment to ensure that security is given on all remotely accessible sessions and that APEX management and employees understand how to execute security controls and their roles and responsibilities in safeguarding APEX information resources.

5.0 Definition:

The act of connecting to IT services, applications, or data from a place other than headquarters is known as remote access. This link enables users to remotely access a network or computer through the internet. SSH is used to encrypt internet communication between two computers or systems. It allows users to execute tasks remotely. SSL, on the other hand, is used to encrypt communication between browsers and servers, or between websites and their visitors. Split-tunneling is a technique that

sends organization-specific traffic over the SSL VPN tunnel while sending other traffic through the remote user's default gateway. General Internet access from home is permitted via the APEX network. However, this should not be used for recreational purposes; before accessing such Internet sites, the remote access connection should be disconnected.

6.0 Responsibilities:

The IT department is in charge of overseeing and revising this policy, and everyone with the ability to connect to the APEX business network remotely via SSH and SSL should abide by its guidelines.

7.0 Penalty:

Any employee who is discovered to have disobeyed this policy may face disciplinary action, which might result in termination.

8.0 Screenshot

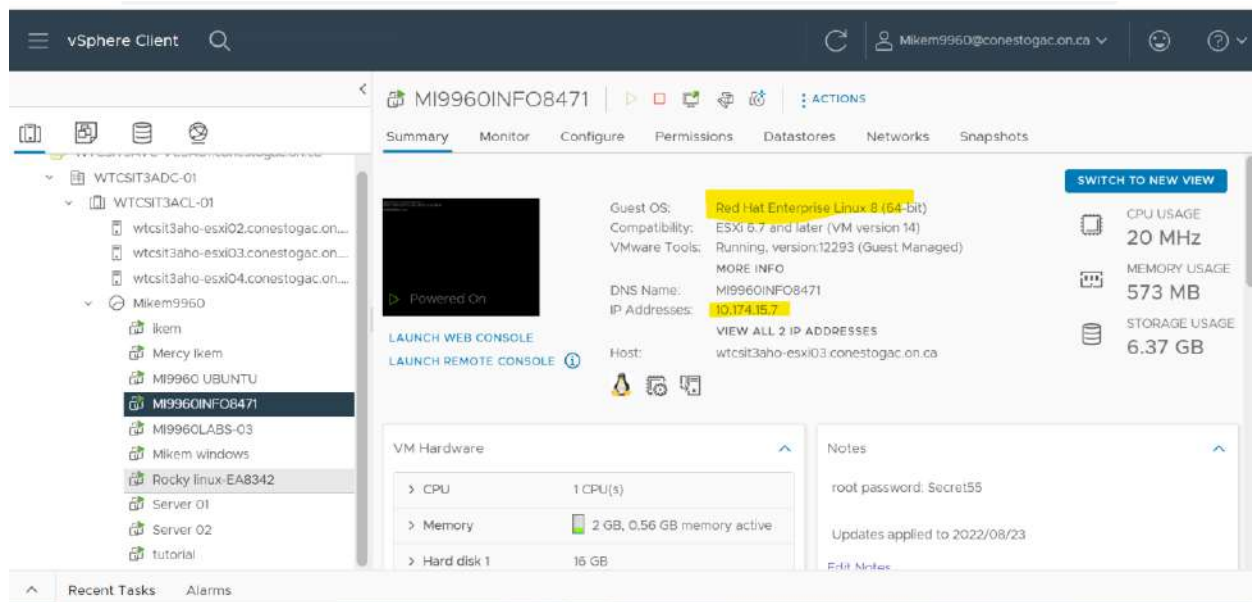


Fig 1 shows the Vn I created to access through ssh

```
root@MI9960INF08471:~  
Microsoft Windows [Version 10.0.19044.2486]  
(c) Microsoft Corporation. All rights reserved.  
  
C:\Users\User>ssh root@10.174.15.7  
root@10.174.15.7's password:  
Last login: Sun Feb 5 11:38:01 2023 from 10.119.71.131  
[root@MI9960INF08471 ~]#
```

Fig 2 shows that I can access my linux through ssh

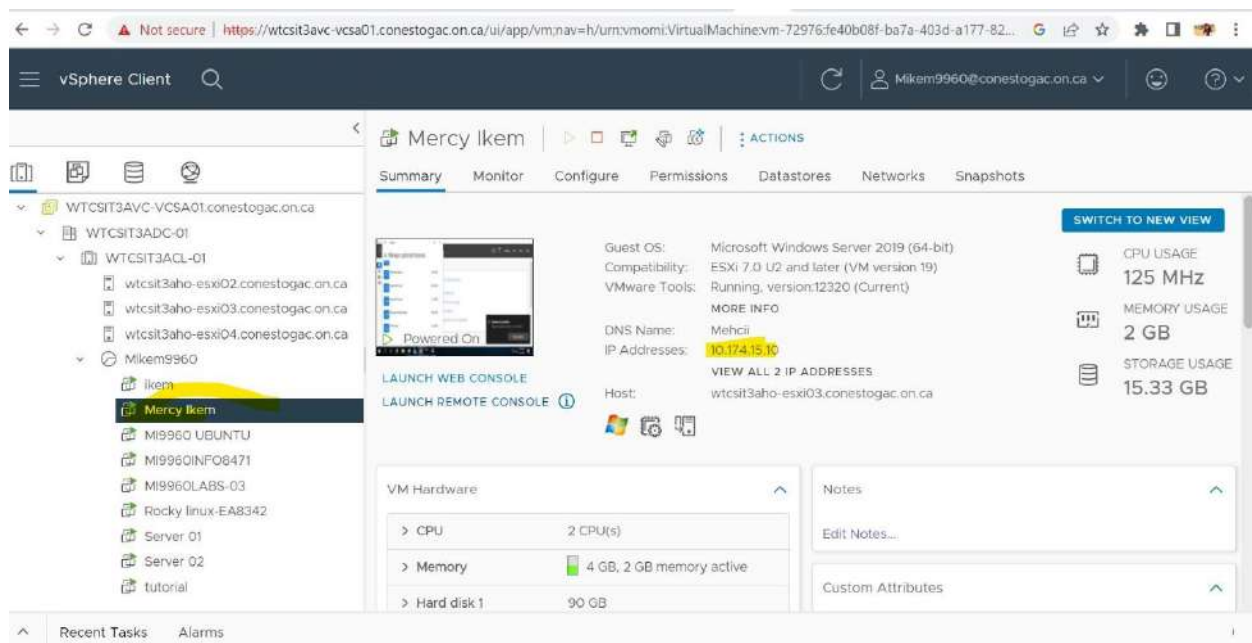
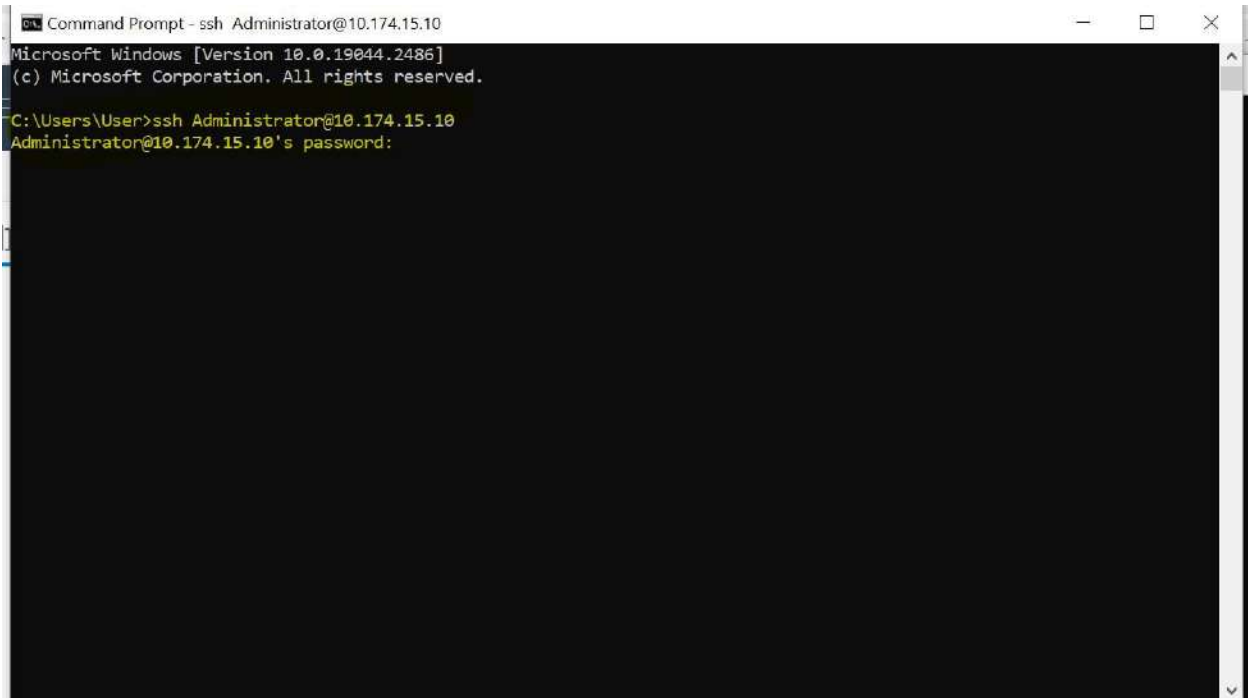


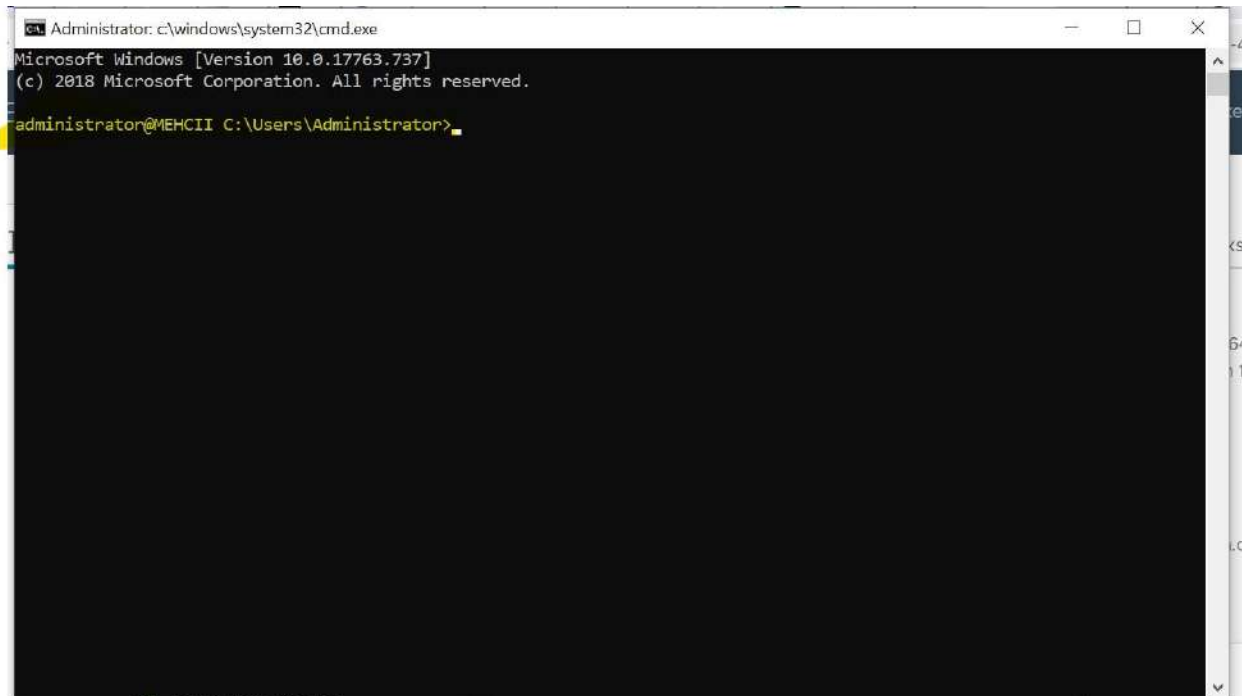
Fig 3 shows the Vm that I created for windows.



```
Command Prompt - ssh Administrator@10.174.15.10
Microsoft Windows [Version 10.0.19044.2486]
(c) Microsoft Corporation. All rights reserved.

C:\Users\User>ssh Administrator@10.174.15.10
Administrator@10.174.15.10's password:
```

Fig 4 shows that I can access my windows using command prompt



```
Administrator: c:\windows\system32\cmd.exe
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

administrator@MEHCII C:\Users\Administrator>
```

Fig 5 shows that I am inside my windows via ssh.

9.0 Revision History.

To make sure that the policy is followed and changed

PASSWORD POLICY

1.0 Overview:

Passwords are very essential in computer security; they help to protect authorized users from having access to confidential information. So, Apex employees are responsible for taking the appropriate steps as outlined below in order to protect company information.

2.0 Purpose:

Information and Network are very vital and important, so we must find a way to protect them(confidentiality) and make sure they are not modified(integrity) and are available when needed(availability). So, the purpose of this policy is to outline the steps required to protect the information and Network in your organization, how to protect the password and the creation of strong passwords.

3.0 Scope:

This policy applies to all staff, contractors of Apex who owned a workstation used to connect to Apex network.

4.0 Policy:

Policy statements

- ❖ All passwords must be changed after 90days

- ❖ All users must ensure that their password is not shared by anyone.
- ❖ Staff in Apex must not store their password or write down their password.
- ❖ Password must be of a minimum length of 8 characters and have mix of alphabets, numbers and characters.
- ❖ The remember password feature shall not be used.
- ❖ Administrator should enforce changing of password by user in first login.
- ❖ Users should never talk about their password to anyone.
- ❖ One-time password authentication should be implemented to verify users.
- ❖ Password must not be communicated through emails.
- ❖ Users must not use the same password for different applications.
- ❖ If user disclosed his/her password to anyone, that password must be changed.
- ❖ For password change, the old password is required to be given.
- ❖ Users should never reveal a password over the phone to ANYONE.
- ❖ Users should never hint on a password.
- ❖ They should be a warning to users to change their password after 70 days.
- ❖ All users' passwords must conform to the following requirements and guidelines below.

❖ **General Password Creation Guidelines**

When creating your own password in Apex, avoid the use of weak passwords for your email accounts, voicemail, screen saver protection, web account etc.

- ❖ Poor, weak passwords include the following characteristics.
 - If the password is found in a dictionary
 - If the password has a minimum of seven characters
 - Your password should not be created based on:
 - Name of a pet, friends, co-worker etc.
 - Birthdays
 - Children or spouse names
 - Company name
 - Weather condition
- ❖ Strong passwords have the following characteristics.

- It must contain upper and lowercase characters.
- Must have special symbols/characters.
- At least eight character long.
- Password must not be word in any language, slang etc.
- The password can be a phrase for example
“MynameisMercylkem9960”.

5.0 Definition:

Authentication is the verification of someone identity. A Password is a secret word or phrase that is used to gain access to an information or an association.

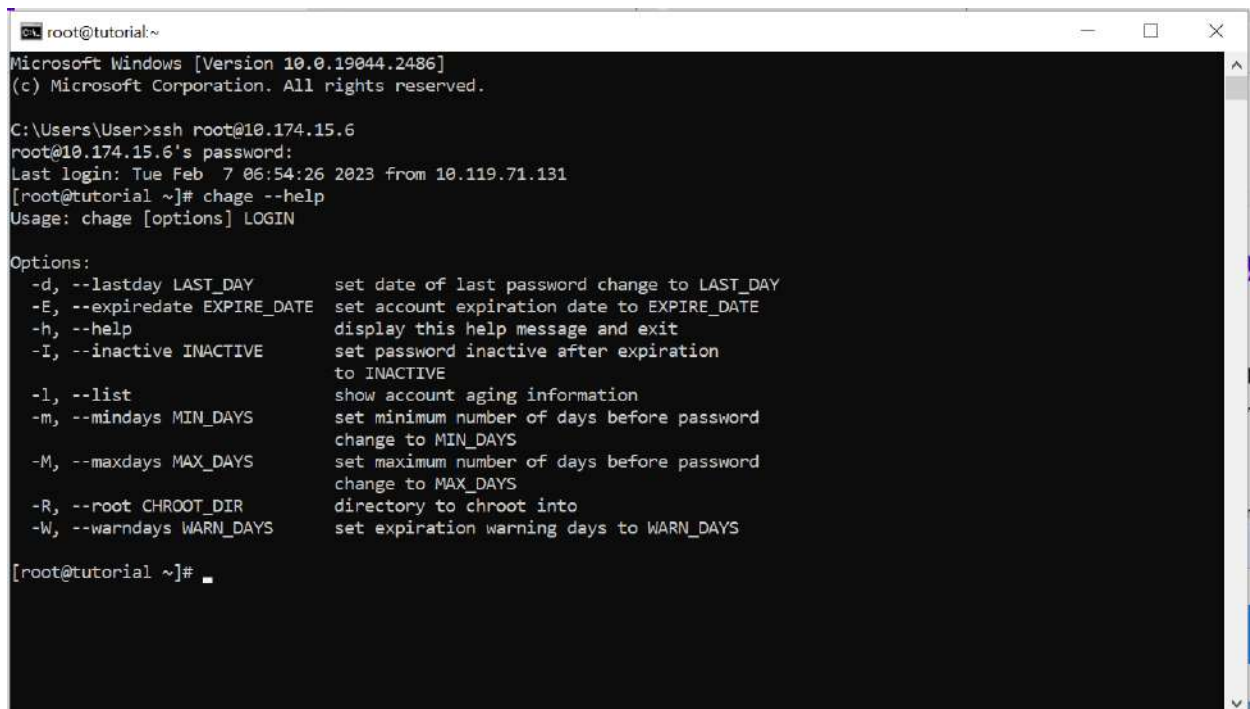
6.0 Responsibilities:

The implementation of this policy is the responsibility of all staff, partner, contractors and all workers of Apex who have access to Apex Computer. It is very important that all workers in Apex takes the seriously the use, protection and integrity of their own password or any system password.

7.0 Penalty:

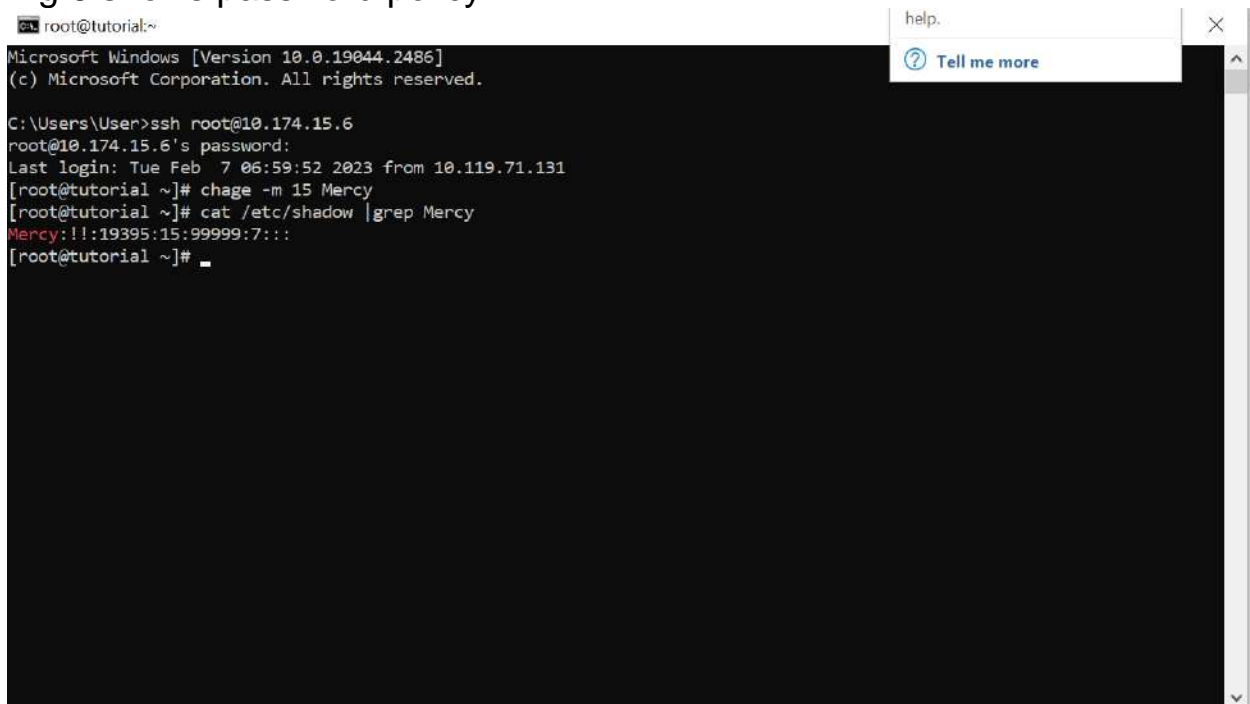
Any employee in Apex found to have violated any policy will be deprived access to the network, maybe subject to disciplinary action and penalized.

8.0 Screenshot



```
root@tutorial:~  
Microsoft Windows [Version 10.0.19044.2486]  
(c) Microsoft Corporation. All rights reserved.  
  
C:\Users\User>ssh root@10.174.15.6  
root@10.174.15.6's password:  
Last login: Tue Feb  7 06:54:26 2023 from 10.119.71.131  
[root@tutorial ~]# chage --help  
Usage: chage [options] LOGIN  
  
Options:  
-d, --lastday LAST_DAY      set date of last password change to LAST_DAY  
-E, --expiredate EXPIRE_DATE set account expiration date to EXPIRE_DATE  
-h, --help                  display this help message and exit  
-I, --inactive INACTIVE     set password inactive after expiration  
                           to INACTIVE  
-l, --list                  show account aging information  
-m, --mindays MIN_DAYS      set minimum number of days before password  
                           change to MIN_DAYS  
-M, --maxdays MAX_DAYS     set maximum number of days before password  
                           change to MAX_DAYS  
-R, --root CHROOT_DIR       directory to chroot into  
-W, --warndays WARN_DAYS    set expiration warning days to WARN_DAYS  
  
[root@tutorial ~]#
```

Fig 6 shows password policy



```
root@tutorial:~  
Microsoft Windows [Version 10.0.19044.2486]  
(c) Microsoft Corporation. All rights reserved.  
  
C:\Users\User>ssh root@10.174.15.6  
root@10.174.15.6's password:  
Last login: Tue Feb  7 06:59:52 2023 from 10.119.71.131  
[root@tutorial ~]# chage -m 15 Mercy  
[root@tutorial ~]# cat /etc/shadow |grep Mercy  
Mercy:!!:19395:15:99999:7:::  
[root@tutorial ~]#
```

Fig 7 shows that the minimum days to change password

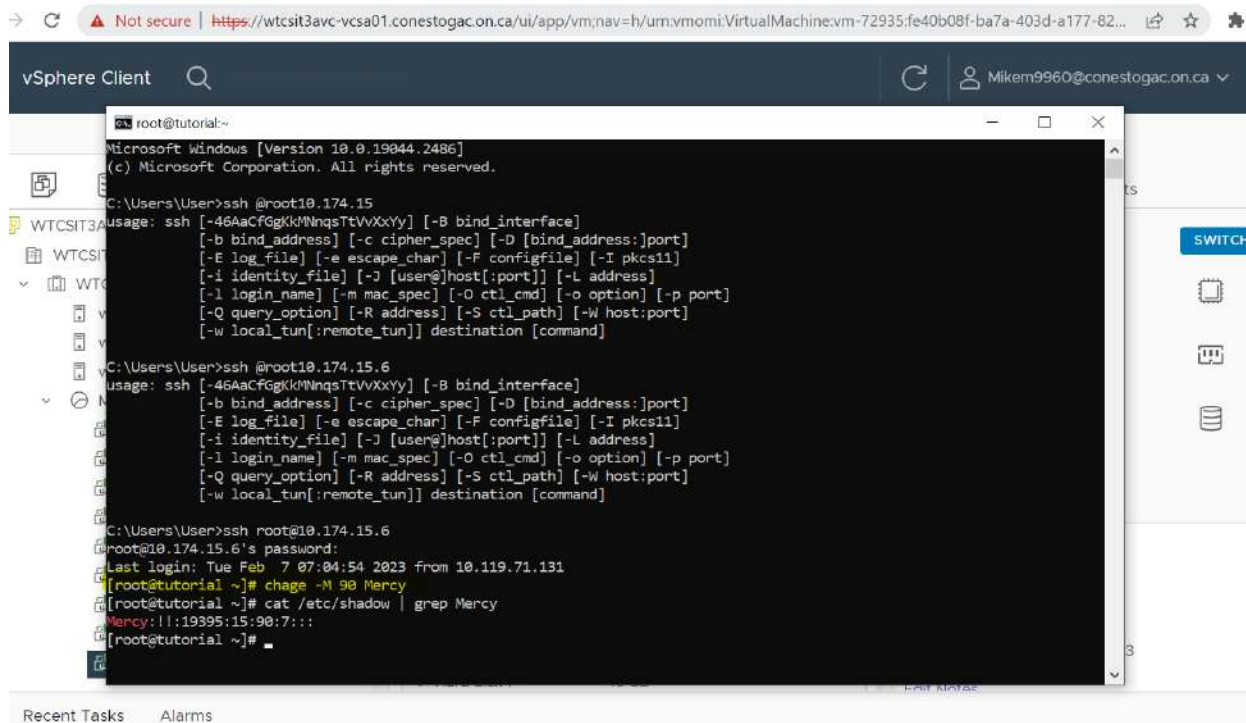


Fig 8 shows the the maximum days for user to change password

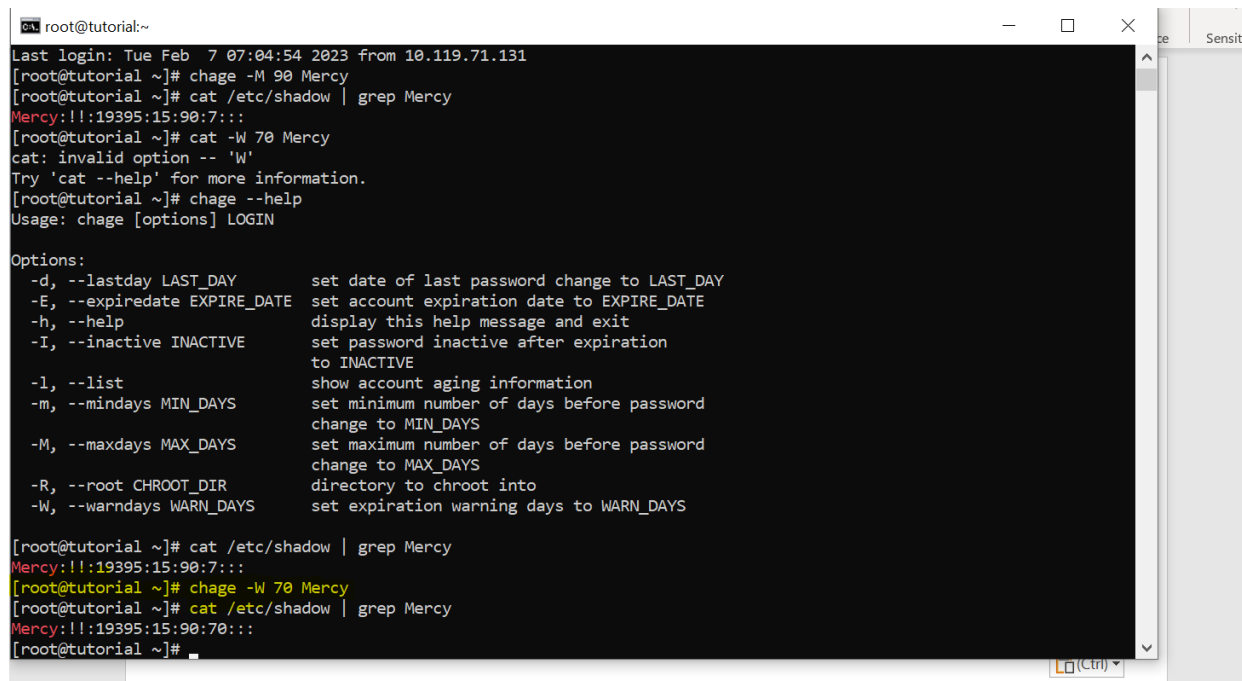


Fig 9 shows the warning days.

```
root@tutorial:~  
# Configuration for systemwide password quality limits  
# Defaults:  
#  
# Number of characters in the new password that must not be present in the  
# old password.  
# difok = 1  
#  
# Minimum acceptable size for the new password (plus one if  
# credits are not disabled which is the default). (See pam_cracklib manual.)  
# Cannot be set to lower value than 6.  
# minlen = 8  
#  
# The maximum credit for having digits in the new password. If less than 0  
# it is the minimum number of digits in the new password.  
# dcredit = 0  
#  
# The maximum credit for having uppercase characters in the new password.  
# If less than 0 it is the minimum number of uppercase characters in the new  
# password.  
# ucredit = 0  
#  
# The maximum credit for having lowercase characters in the new password.  
# If less than 0 it is the minimum number of lowercase characters in the new  
# password.  
# lcredit = 0  
#  
# The maximum credit for having other characters in the new password.  
# If less than 0 it is the minimum number of other characters in the new
```

Fig 10 shows the min length of password.

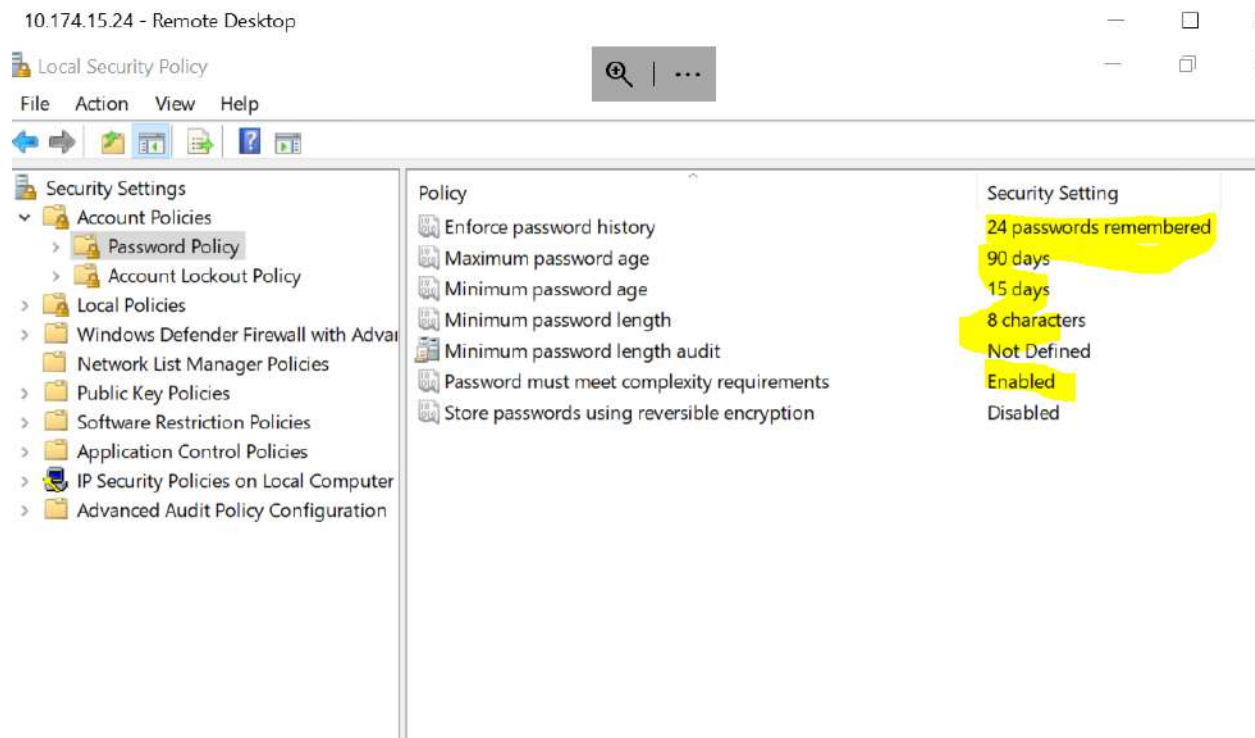


Fig 11 shows the password policy in windows

9.0 Revision History.

To make sure that this policy is in line with the policy password and should be changed periodically.

PATCH MANAGERMENTS

1.0 Overview:

Patch management is necessary at APEX Company to reduce risk to personal data and the integrity of APEX Company systems. It is an effective technique for protecting against vulnerabilities, a procedure that must be done on a regular basis and should be as comprehensive as possible to be most successful. Apex company must prioritize its assets and safeguard the most vital ones first; yet all machines must be patched.

2.0 Purpose:

It is a preventative measure meant to keep known vulnerabilities in an organization's IT infrastructure from being exploited. Apex clients and users rely on software to deliver services. This policy serves as the foundation for a continuing and consistent system update that emphasizes regular security upgrades and OS patches.

3.0 Scope:

This policy is applicable to all servers, computers, and software that APEX Company owns and maintains.

4.0 Policy:

Most operating systems for computers have software packages that might have security holes. If hackers figure out these weaknesses, they could breach the computer and get access to sensitive corporate data and information, endangering the security of the APEX network and the

computers connected to it. Therefore, security-related patches ought to be implemented.

- ❖ If a critical or security patch cannot be centrally distributed by IT teams, it must be installed as soon as possible with the greatest resources available.
- ❖ All APEX systems and devices must be patched on a regular basis. Patching must incorporate all operating system upgrades.
- ❖ All APEX IT systems must be properly licensed, supported by the manufacturer, and run current and patched operating system and application software.
- ❖ Before APEX systems would accept third-party supply, they must offer confirmation of current patching.
- ❖ To restrict the introduction of new risks, new systems must be patched to the existing agreed-upon baseline before going live.
- ❖ All changes must be checked before complete implementation because patches might cause unexpected problems.
- ❖ APEX IT should strive for 100% compliance for patching the OS under their supervision.
- ❖ A reporting metric that summarizes the results of each patching cycle must be compiled and kept up to date by those in charge of patching. The reports will be used to assess the current degree of risk and the patching levels for all systems.
- ❖ APEX's IT staff will supervise the patching of servers in accordance with a set routine.

5.0 Definition:

Patch management is the process of delivering and installing software updates. It is the process of locating and applying software updates or patches to various endpoints such as PCs, mobile devices, and servers. A patch is a particular modification or series of updates made available by software developers to address identified security flaws.

6.0 Responsibilities:

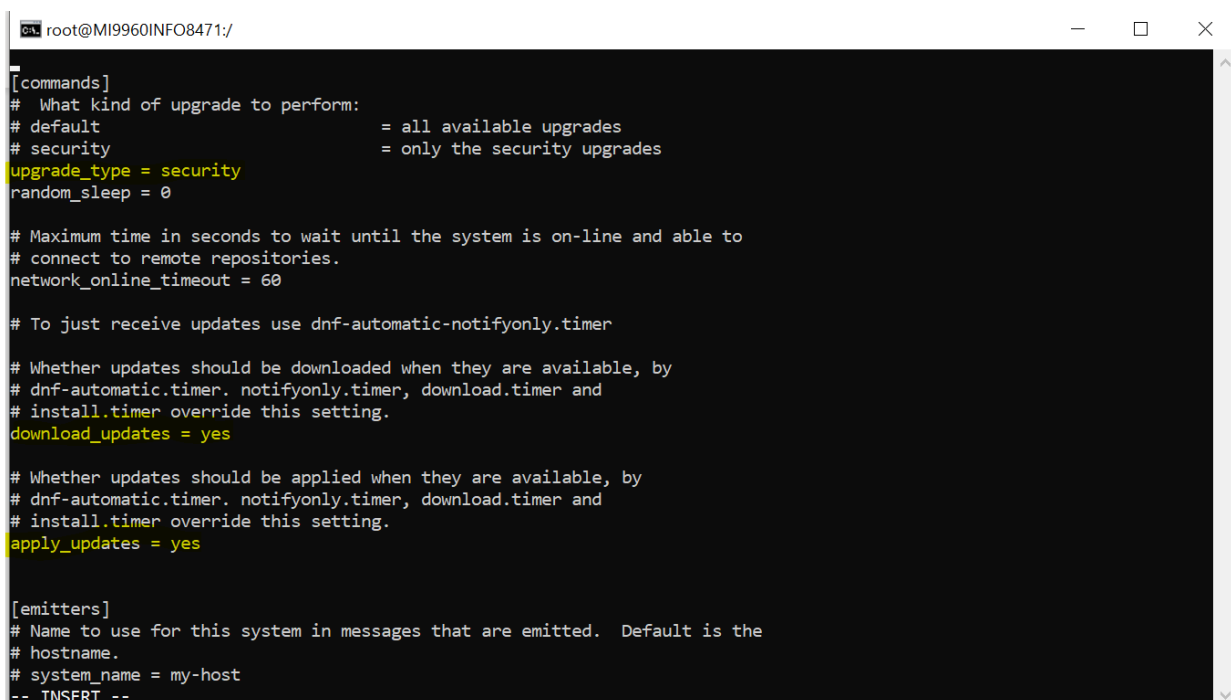
- ❖ For the APEX firm, a secure network environment is provided by the IT department. All computers linked to the APEX network must

- have the most recent OS, security, and application patches installed as per APEX business policy.
- ❖ Every user is responsible for ensuring that computer and network resources are used prudently and responsibly.
 - ❖ IT is responsible for putting in place all known and reasonable measures to mitigate network vulnerabilities while keeping the network operational.

7.0 Penalty:

- ❖ Employees who commit intentional policy violations may face disciplinary action, including termination.
- ❖ The IT department may face disciplinary action if it consistently fails to comply with the terms of this Patch Management policy.
- ❖ Resources on the network should not be accessed by devices with OS software that do not adhere to patching rules.

8.0 Screenshot



```
root@MI9960INFO8471:/  
[commands]  
# What kind of upgrade to perform:  
# default                = all available upgrades  
# security                = only the security upgrades  
upgrade_type = security  
random_sleep = 0  
  
# Maximum time in seconds to wait until the system is on-line and able to  
# connect to remote repositories.  
network_online_timeout = 60  
  
# To just receive updates use dnf-automatic-notifyonly.timer  
  
# Whether updates should be downloaded when they are available, by  
# dnf-automatic.timer, notifyonly.timer, download.timer and  
# install.timer override this setting.  
download_updates = yes  
  
# Whether updates should be applied when they are available, by  
# dnf-automatic.timer, notifyonly.timer, download.timer and  
# install.timer override this setting.  
apply_updates = yes  
  
[emitters]  
# Name to use for this system in messages that are emitted. Default is the  
# hostname.  
# system_name = my-host  
-- INSERT --
```

Fig 12 shows the update in windows(linux)

```

grub2-tools.x86_64 1:2.02-123.el8_6.8.rocky.0.1 @baseos
grub2-tools-efi.x86_64 1:2.02-142.el8_7.1.rocky.0.2 baseos
grub2-tools.x86_64 1:2.02-123.el8_6.8.rocky.0.1 @baseos
grub2-tools-extra.x86_64 1:2.02-142.el8_rocky.0.2 baseos
grub2-tools.x86_64 1:2.02-123.el8_6.8.rocky.0.1 @baseos
grub2-tools-extra.x86_64 1:2.02-142.el8_7.1.rocky.0.2 baseos
grub2-tools.x86_64 1:2.02-123.el8_6.8.rocky.0.1 @baseos
grub2-tools-minimal.x86_64 1:2.02-142.el8_rocky.0.2 baseos
grub2-tools.x86_64 1:2.02-123.el8_6.8.rocky.0.1 @baseos
grub2-tools-minimal.x86_64 1:2.02-142.el8_7.1.rocky.0.2 baseos
grub2-tools.x86_64 1:2.02-123.el8_6.8.rocky.0.1 @baseos

```

[root@M19960INFO8471 ~]# dnf update
Last metadata expiration check: 0:21:46 ago on Tue 07 Feb 2023 06:59:18 PM EST.
Dependencies resolved.

Package	Architecture	Version	Repository	Size
Installing:				
kernel	x86_64	4.18.0-425.10.1.el8_7	baseos	8.8 M
Upgrading:				
NetworkManager	x86_64	1:1.40.0-5.el8_7	baseos	2.3 M
NetworkManager-initscripts-updown	noarch	1:1.40.0-5.el8_7	baseos	140 k
NetworkManager-libnm	x86_64	1:1.40.0-5.el8_7	baseos	1.9 M
NetworkManager-team	x86_64	1:1.40.0-5.el8_7	baseos	157 k
NetworkManager-tui	x86_64	1:1.40.0-5.el8_7	baseos	351 k
audit	x86_64	3.0.7-4.el8	baseos	262 k
audit-libs	x86_64	3.0.7-4.el8	baseos	122 k
authselect	x86_64	1.2.5-2.el8_7	baseos	145 k
authselect-libs	x86_64	1.2.5-2.el8_7	baseos	228 k
ca-certificates	noarch	2022.2.54-80.2.el8_6	baseos	919 k
coreutils	x86_64	8.30-13.el8	baseos	1.2 M
coreutils-common	x86_64	8.30-13.el8	baseos	2.0 M
cronie	x86_64	1.5.2-8.el8	baseos	118 k
cronie-anacron	x86_64	1.5.2-8.el8	baseos	41 k
curl	x86_64	7.61.1-25.el8_7.1	baseos	351 k
dbus	x86_64	1:1.12.8-23.el8_7.1	baseos	41 k
dbus-common	noarch	1:1.12.8-23.el8_7.1	baseos	46 k
dbus-daemon	x86_64	1:1.12.8-23.el8_7.1	baseos	240 k
dbus-libs	x86_64	1:1.12.8-23.el8_7.1	baseos	184 k
dbus-tools	x86_64	1:1.12.8-23.el8_7.1	baseos	85 k
device-mapper	x86_64	8:1.02.181-6.el8	baseos	376 k

Fig 13 shows some update in linux

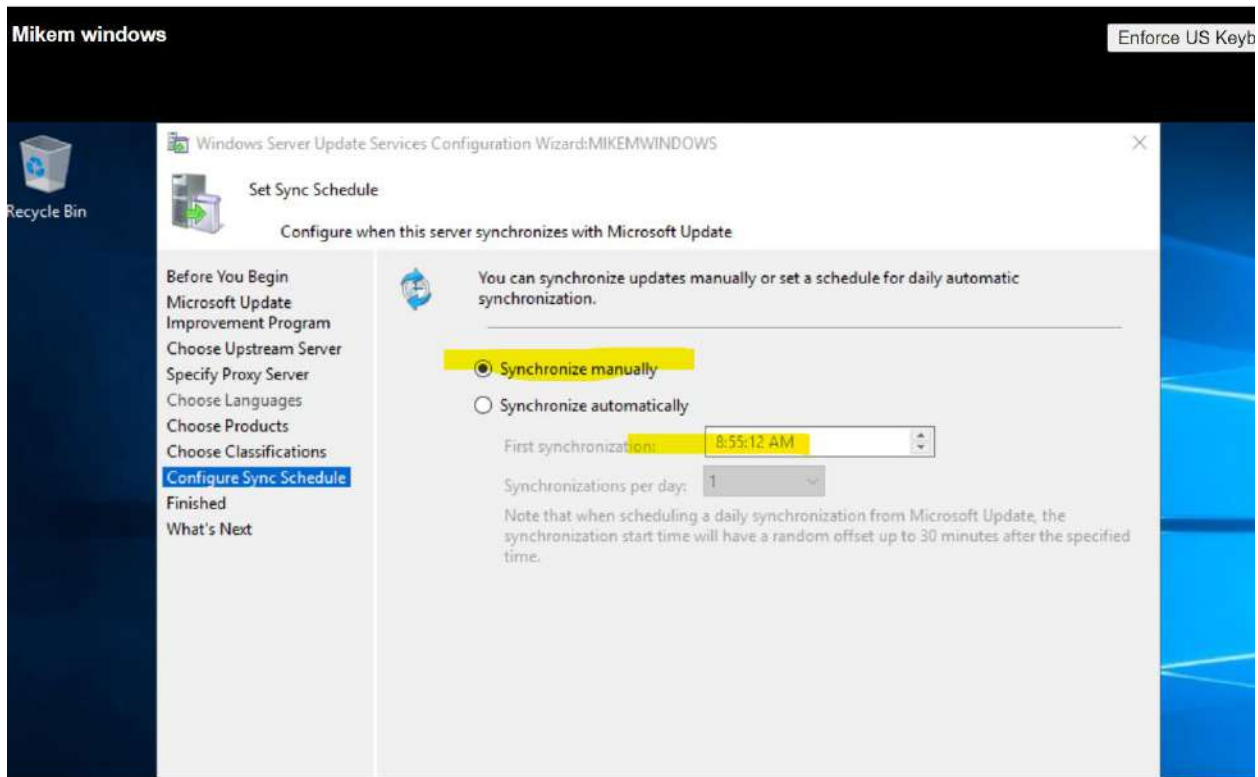


Fig 14 shows the updates.

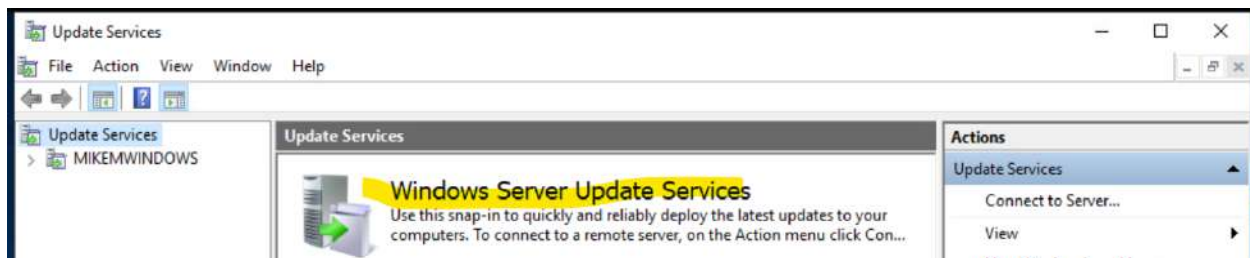


Fig 15 shows that the windows has been updated

9.0 Revision History

This policy will be modified periodically, and it should be taken seriously.

10.0 References

PurpleSec. (2023, February 2). *Sample Patch Management Policy Template*.

<https://purplesec.us/resources/cyber-security-policy-templates/patch-management/>

Team, A. (n.d.). *Free Remote Access Policy Template*. <https://blog.focal-point.com/remote-access-policy-template>

What is VPN Split Tunneling? (n.d.-b). Fortinet.

<https://www.fortinet.com/resources/cyberglossary/vpn-split-tunneling>

Roehampton University. <https://www.roehampton.ac.uk/globalassets/documents/corporate-information/policies/cyber-security-policies/patch-management-policy>.

Team, A. (n.d.-b). *Free Remote Access Policy Template*. <https://blog.focal-point.com/remote-access-policy-template>

What is Patch Management? Benefits & Best Practices. (n.d.). Rapid7.

<https://www.rapid7.com/fundamentals/patch-management/>

