

WINDOWS FUNDAMENTALS 3: SECURITY AND SYSTEM PROTECTION

EXP.NO: 1(c)

AIM:

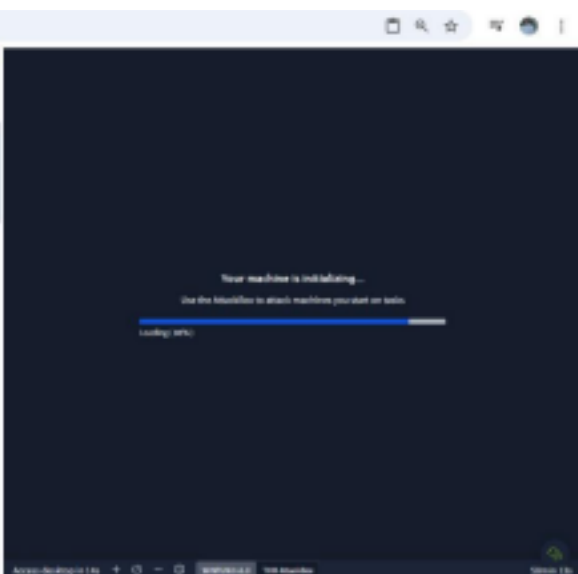
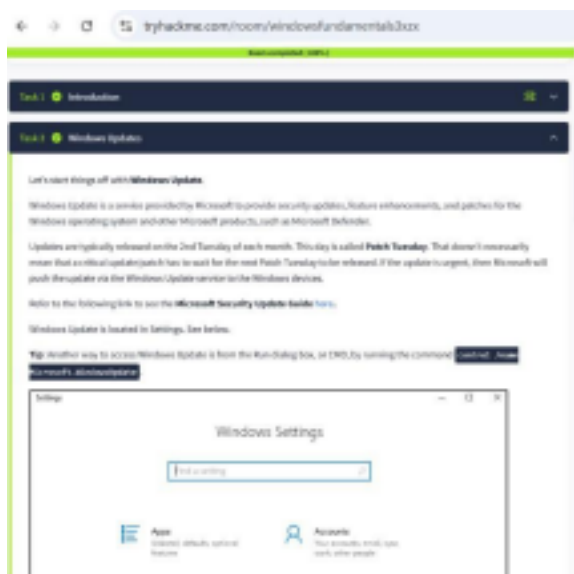
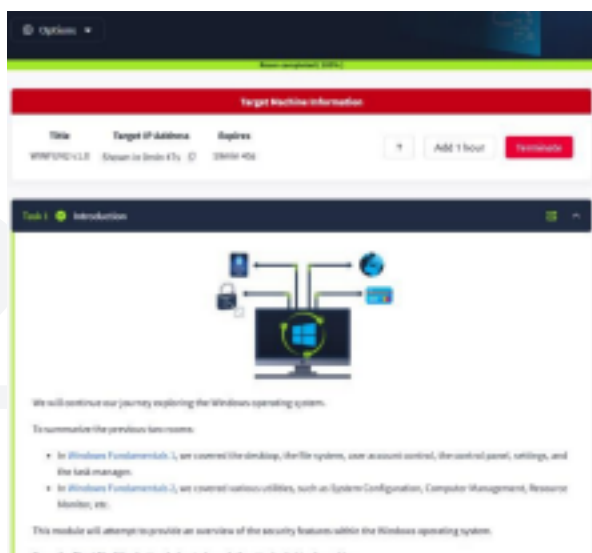
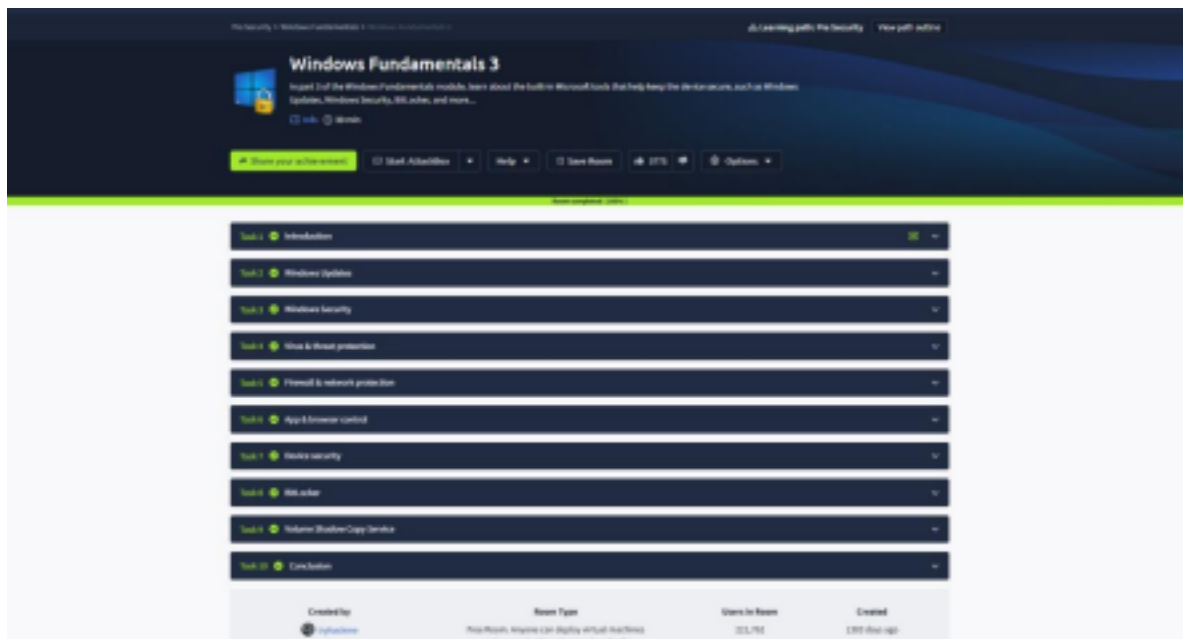
To understand and explore key security features in Windows, including Windows Defender, Firewalls, User Account Control (UAC), BitLocker, and Windows Updates.

ALGORITHM:

1. Access the lab in TryHackMe platform using the link below
<https://tryhackme.com/r/room/windowsfundamentalsxxz>
2. Click Start a Machine and AttackBox to run the instance of Kali Windows distribution.
3. Solve the task questions start with Windows Update – Patch Tuesday – Windows Setting – Update & Security (or in command prompt type control / name Microsoft.WindowsUpdate .
4. Explore Windows Security → Protection areas, Virus & threat protection, Firewall & network protection, App & browser control, Device security.
5. Learn in Firewall & network protection – Domain network , Private network and Public network – Windows Defender Firewall (WF.msc)
6. Understand the Microsoft Defender SmartScreen – Exploit Protection – System Settings - Program Settings.
7. Explore about Device Security → Core isolation → Memory Integrity , Security Processor → Trusted Platform Module (TPM).
8. Understand about BitLocker – Practical Application – BitLocker and TPM – System Requirements – Device Encryption – TPM versions.
9. Explore Volume Shadow copy Service (VSS) – Advanced System Settings – Create a restore point – Perform system restore – Configure restore settings – Delete restore points.

CS19642 Cryptography and Network Security

OUTPUT:



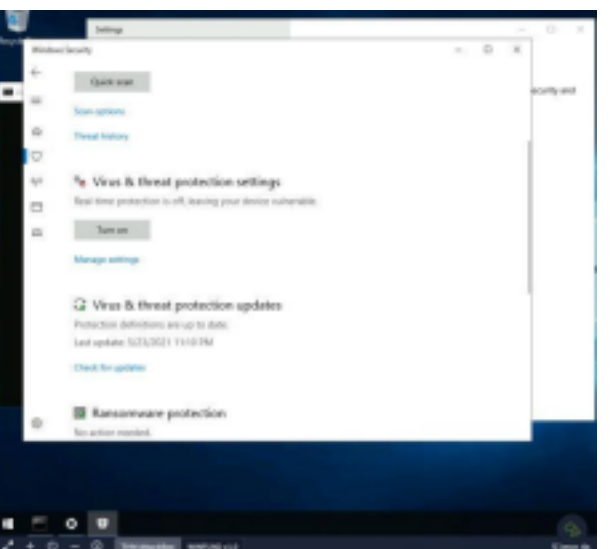
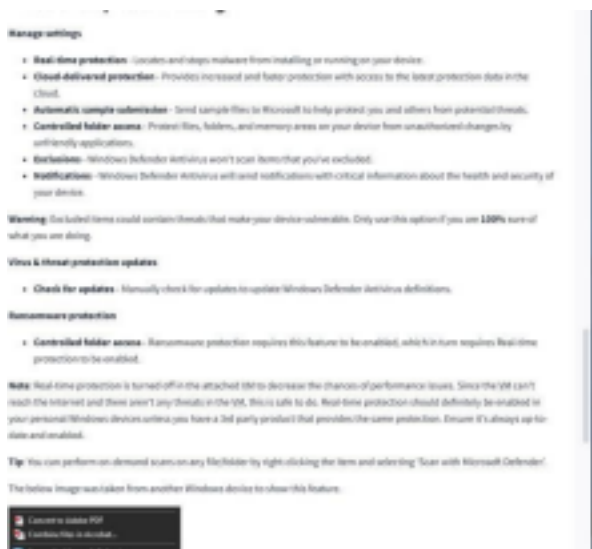
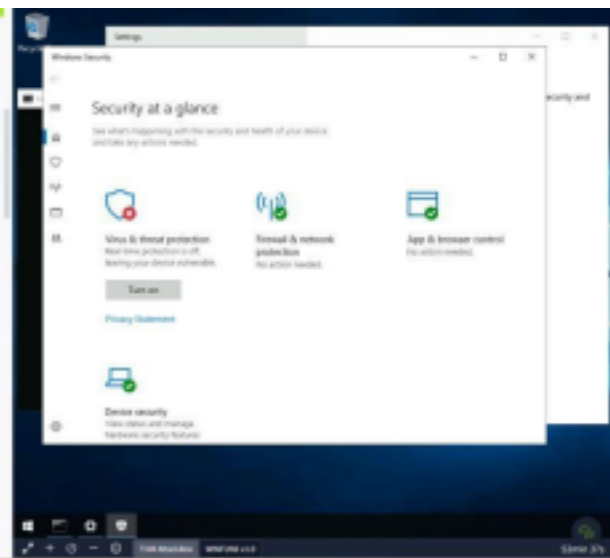
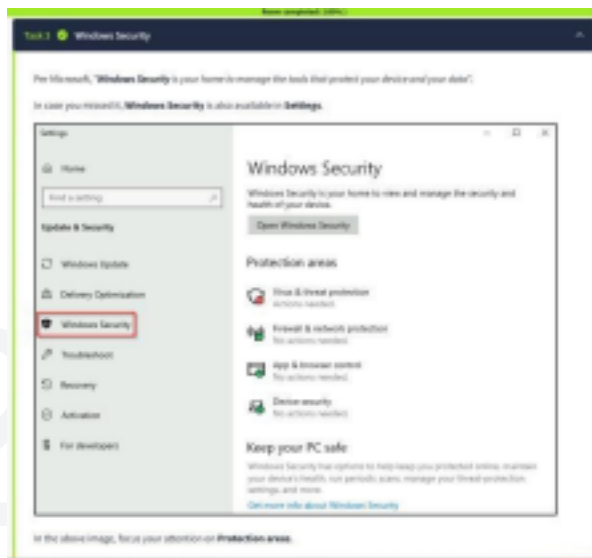
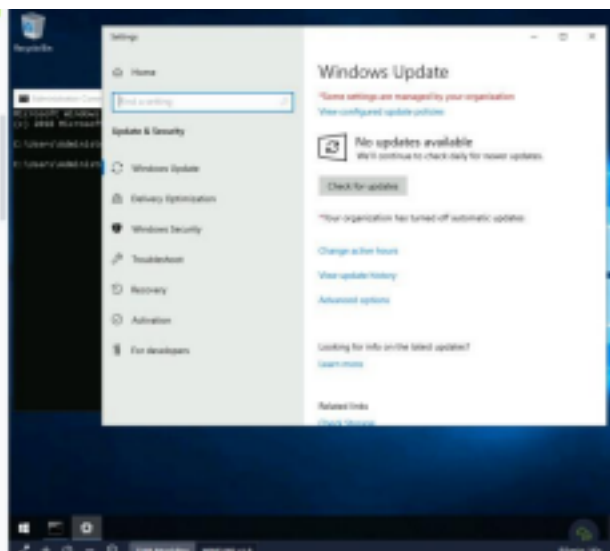
CS19642

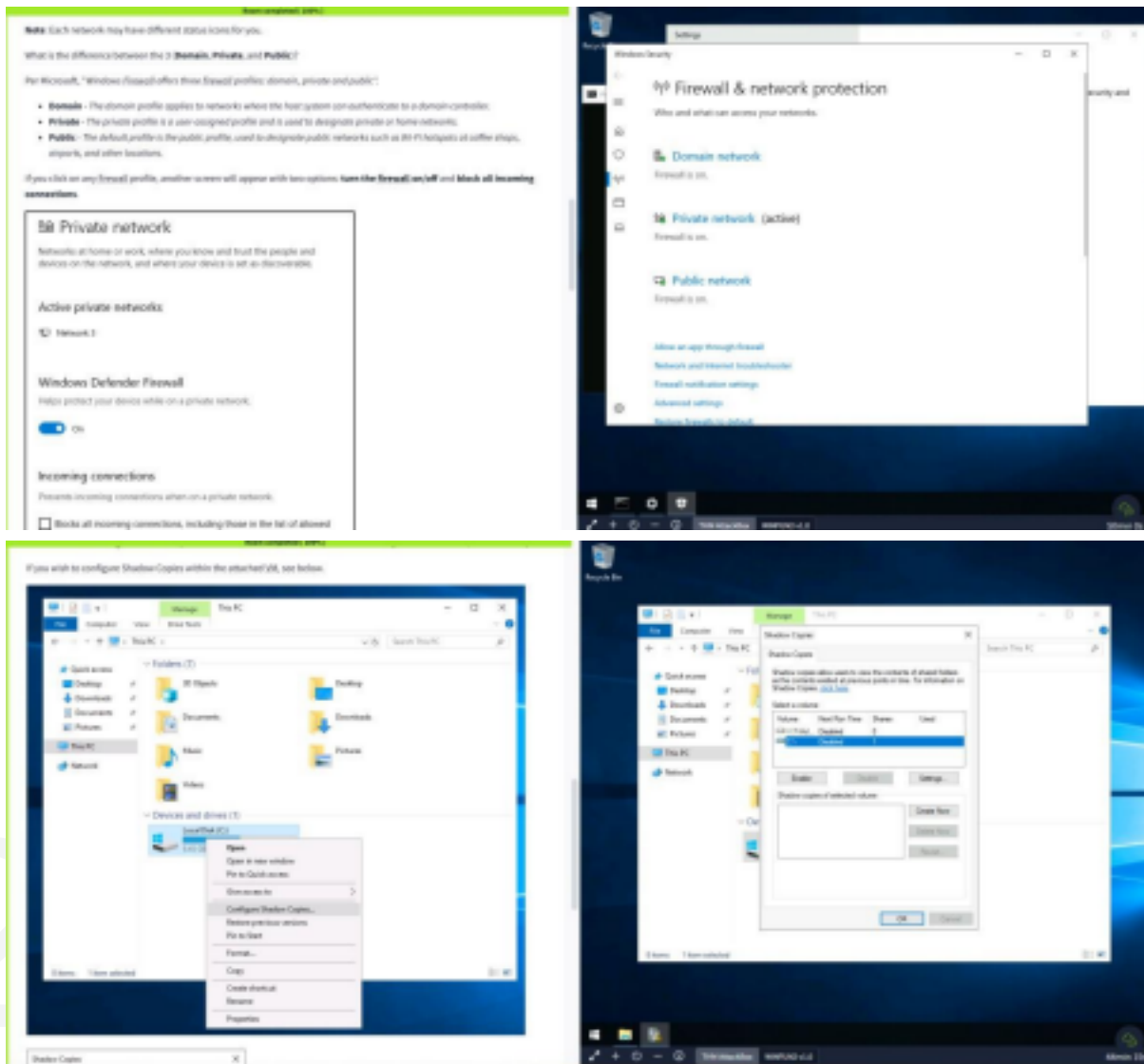
Cryptography

and

Network

Security





1. Windows Defender

- Learn about Microsoft's built-in antivirus solution.
- Understand real-time protection, malware scanning, and threat detection.
- Explore different scanning options and how Defender integrates with Windows Security.

2. Windows Firewall

- Understand how firewalls protect against unauthorized network traffic.
- Learn how to configure firewall rules for applications and ports.
- Explore inbound and outbound connection management

CS19642 Cryptography and Network Security

3. User Account Control (UAC)

- Understand the role of UAC in preventing unauthorized changes.
- Learn how UAC helps restrict administrative privileges to prevent malware execution.
- Explore different UAC settings and their impact on security.

4. BitLocker Encryption

- Learn how BitLocker encrypts drives to prevent data theft.
- Explore encryption key management and recovery options.
- Understand the importance of encrypting removable storage devices.

5. Windows Updates

- Understand the significance of keeping Windows up to date.
- Learn how updates provide security patches and feature enhancements.
- Explore how to configure update settings and troubleshoot update issues.

Answer the questions below

There were two definition updates installed in the attached VM. On what date were these updates installed?

5/3/2021

✓ Correct Answer

Checking the Security section on your VM, which area needs immediate attention?

Virus & threat protection

✓ Correct Answer

If you were connected to airport Wi-Fi, what most likely will be the active firewall profile?

Public network

✓ Correct Answer

🔍 Hint

Specifically, what is turned off that Windows is notifying you to turn on?

Real-time protection

✓ Correct Answer

CS19642 Cryptography and Network Security

What is the TPM?

Trusted Platform Module

✓ Correct Answer

What is VSS?

Volume Shadow Copy Service

✓ Correct Answer

RESULT:

This experiment provides an understanding of Windows security best practices and hands-on experience configuring and managing security settings, which is essential for protecting systems from cyber threats.