RIT

جامعة روتشستر الأمريكية للتكنولوجيا في دبي

A Global American University in Dubai

CSEC 202 Reverse Engineering Fundamentals

Module 0x06
Basic Dynamic Analysis
1 / 2

Eng. Emad Abu Khousa

Sections: 600 | 601 | 602

March 18, 2024

Basic Dynamic Analysis

- **Basic dynamic analysis refers to the process of evaluating and analyzing a program or software system by executing it in a controlled environment to observe its behavior.**
- Unlike advanced static analysis, which inspects the program's code without running it, basic dynamic analysis requires the program to be in operation, **without directly examining the code itself.**
- This approach is especially useful in the field of malware analysis, software testing, and debugging, where **understanding the runtime behavior of a program** can provide critical insights that are not apparent through code examination alone.

Basic Dynamic Analysis

- Dynamic analysis is any examination performed after executing malware or monitoring it while running. Dynamic analysis techniques are the second step in the malware analysis process.

- Although dynamic analysis techniques are extremely powerful, they should be performed only after basic static analysis has been completed, because dynamic analysis can put your network and system at risk

Dynamic Malware Analysis

- In dynamic analysis, the malware is executed on a system to understand its behavior after infection
- This type of analysis requires a safe environment such as virtual machines and sandboxes to deter the spreading of malware
- Dynamic analysis consists of two stages: **System Baselining** and **Host Integrity Monitoring**

Dynamic Malware Analysis

System Baselining

- Refers to taking a **snapshot** of the system at the time the malware analysis begins
- The main purpose of system baselining is to **identify significant changes** from the baseline state
- The system baseline includes details of the **file system**, **registry**, **open ports**, **network activity**, etc.

Dynamic Malware Analysis

Host Integrity Monitoring

Host integrity monitoring includes the following:

- Port Monitoring
- Process Monitoring
- Registry Monitoring
- Windows Services Monitoring
- Startup Programs Monitoring
- Event Logs Monitoring/Analysis
- Installation Monitoring
- Files and Folders Monitoring
- Device Drivers Monitoring
- Network Traffic Monitoring/Analysis
- DNS Monitoring/Resolution
- API Calls and System Calls Monitoring

Sandboxing: Malware Analysis in Controlled Environments

- **Controlled Environment:** Analyze malware within a virtual machine (VM) to avoid accidental execution.
- **Isolated VM:** Use a VM not connected to live systems, dedicated to malware analysis.
- **Snapshot Functionality:** Ability to revert to a clean state before analyzing new malware.
- **Monitoring Tools:** Employ both automated and manual tools to analyze malware behavior.
- **File-Sharing Mechanism:** Use safe methods to transfer malware and analysis data, ensuring isolation.

Tools:

1- **P**rocess **M**onitor

2- Process Explorer or Process Hacker

3- API logger and API monitor

4- Regshot: : Highlights changes to the file system and the registry

5- Faking a Network with ApateDNS

6- Monitoring with Netcat

7- Packet Sniffing with Wireshark

8- Using INetSim

9- ProcDOT: Visualizes Process Monitor logs for easier analysis.

10 – Cuckoo Sandbox

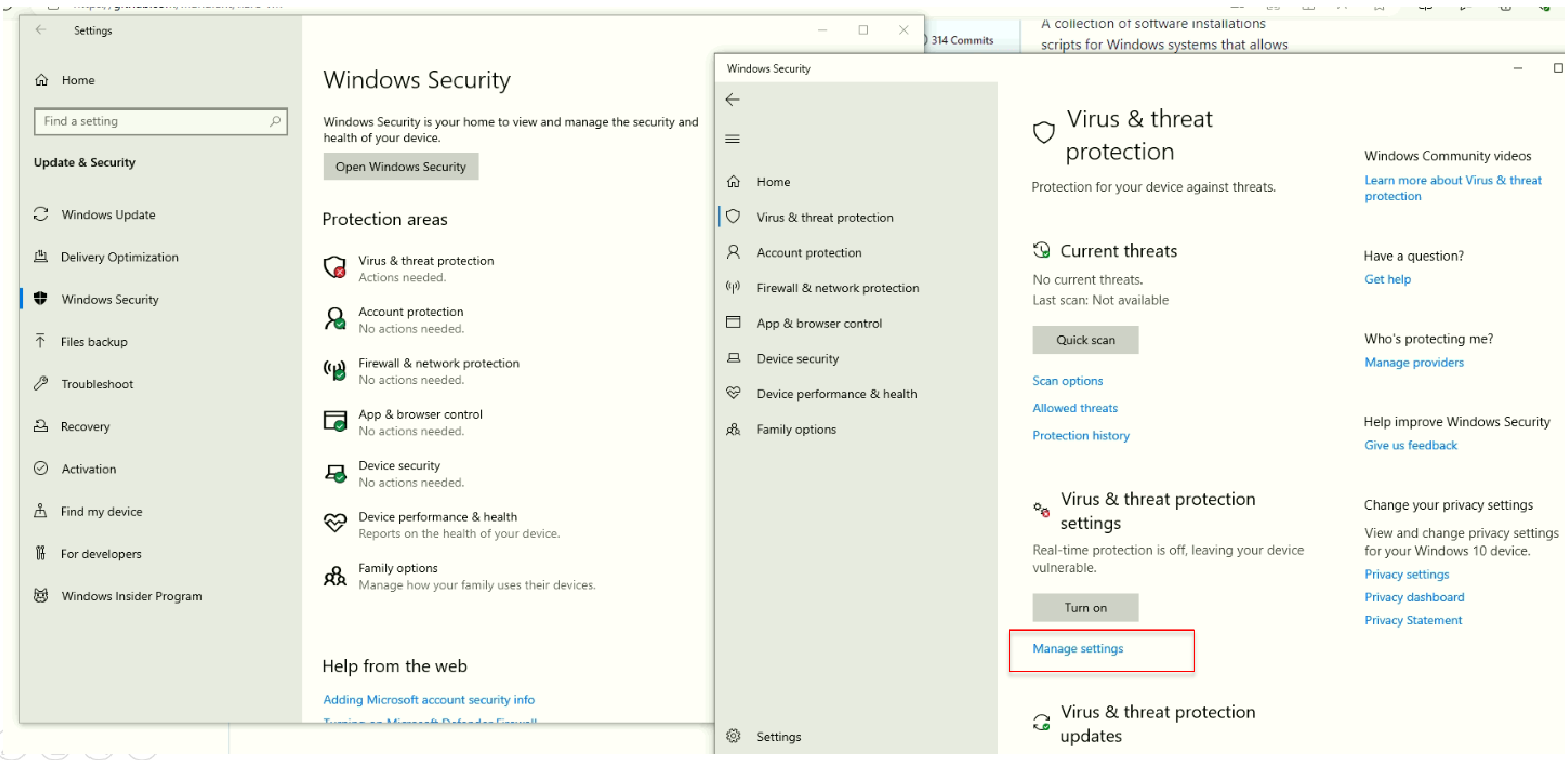
Build Your Lab

Building The Lab VM and Disabling Security Features

- **Install windows 10 vm. https://www.microsoft.com/en-us/software-download/windows10**
- **Disable Microsoft Defender Antivirus.**
  - Microsoft Defender Antivirus is a pre-installed security program that shields your computer from harm. However, there may be occasions where you'll need to briefly disable it.
- **Disable Tamper protection**
- **Install Flare VM from:**

https://github.com/mandiant/flare-vm

Building The Lab VM and Disabling Security Features



314 Commits

A collection of software installations scripts for Windows systems that allows

Settings

Home

Find a setting

Update & Security

- Windows Update
- Delivery Optimization
- Windows Security
- Files backup
- Troubleshoot
- Recovery
- Activation
- Find my device
- For developers
- Windows Insider Program

Windows Security

Windows Security is your home to view and manage the security and health of your device.

Open Windows Security

Protection areas

Virus & threat protection
Actions needed.

Account protection
No actions needed.

Firewall & network protection
No actions needed.

App & browser control
No actions needed.

Device security
No actions needed.

Device performance & health
Reports on the health of your device.

Family options
Manage how your family uses their devices.

Help from the web

Adding Microsoft account security info

Turning on Microsoft Defender Firewall

Windows Security

- Home
- Virus & threat protection
- Account protection
- Firewall & network protection
- App & browser control
- Device security
- Device performance & health
- Family options
- Settings

Virus & threat protection

Protection for your device against threats.

Current threats

No current threats.
Last scan: Not available

Quick scan

Scan options

Allowed threats

Protection history

Virus & threat protection settings

Real-time protection is off, leaving your device vulnerable.

Turn on

Manage settings

Virus & threat protection updates

Windows Community videos
Learn more about Virus & threat protection

Have a question?
Get help

Who's protecting me?
Manage providers

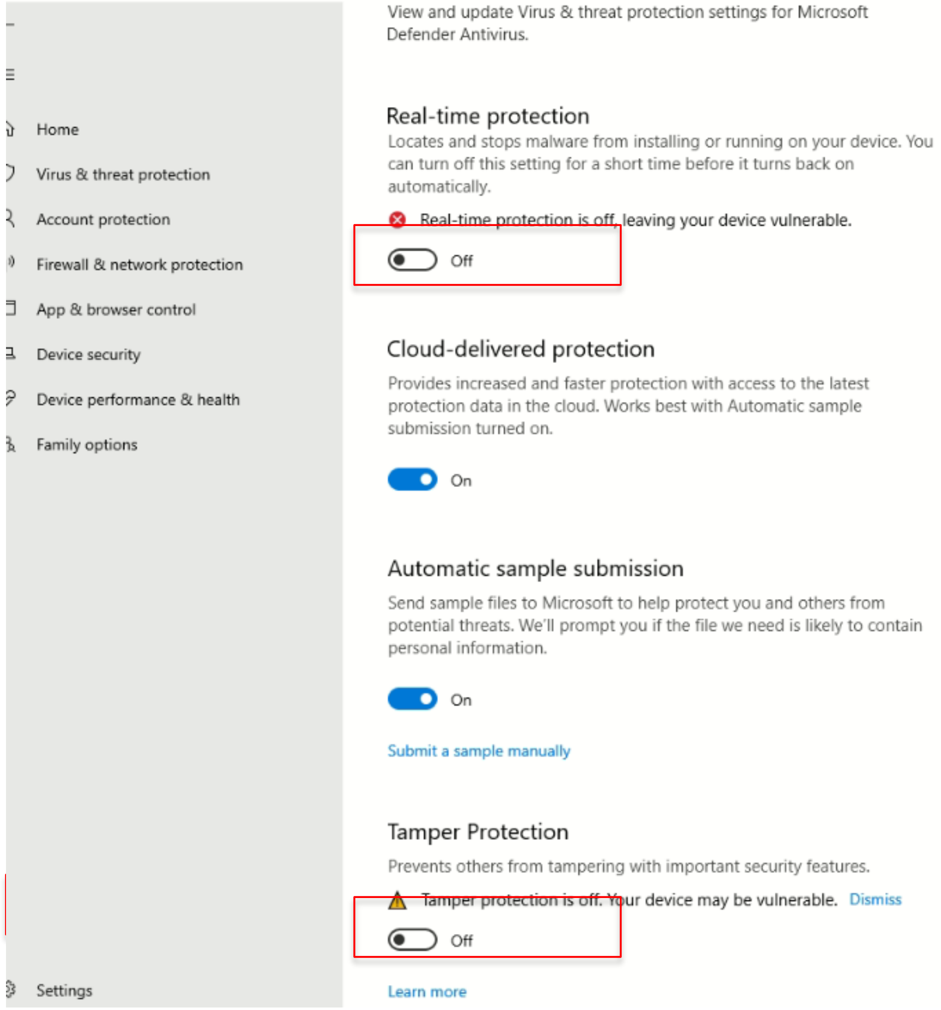
Help improve Windows Security
Give us feedback

Change your privacy settings
View and change privacy settings for your Windows 10 device.
Privacy settings
Privacy dashboard
Privacy Statement

Building The Lab VM and Disabling Security Features

Here's a helpful guide to help you disable Microsoft Defender Antivirus:

1. Step One: Open the Settings app in the Start Menu.
2. Step Two: Select "Update & Security" in the Settings app.
3. Step Three: Choose "Windows Security" from the left sidebar.
4. Step Four: Tap "Virus & threat protection" under Windows Security.
5. Step Five: Hit "Manage settings" under Virus & threat protection settings.
6. Step Six: Turn off Real-time protection by moving the switch to the off position
7. Step Seven: Turn off Tamper Protection


Home
Virus & threat protection
Account protection
Firewall & network protection
App & browser control
Device security
Device performance & health
Family options
Settings

View and update Virus & threat protection settings for Microsoft Defender Antivirus.

Real-time protection

Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.

Real-time protection is off, leaving your device vulnerable.

Off

Cloud-delivered protection

Provides increased and faster protection with access to the latest protection data in the cloud. Works best with Automatic sample submission turned on.

On

Automatic sample submission

Send sample files to Microsoft to help protect you and others from potential threats. We'll prompt you if the file we need is likely to contain personal information.

On

Submit a sample manually

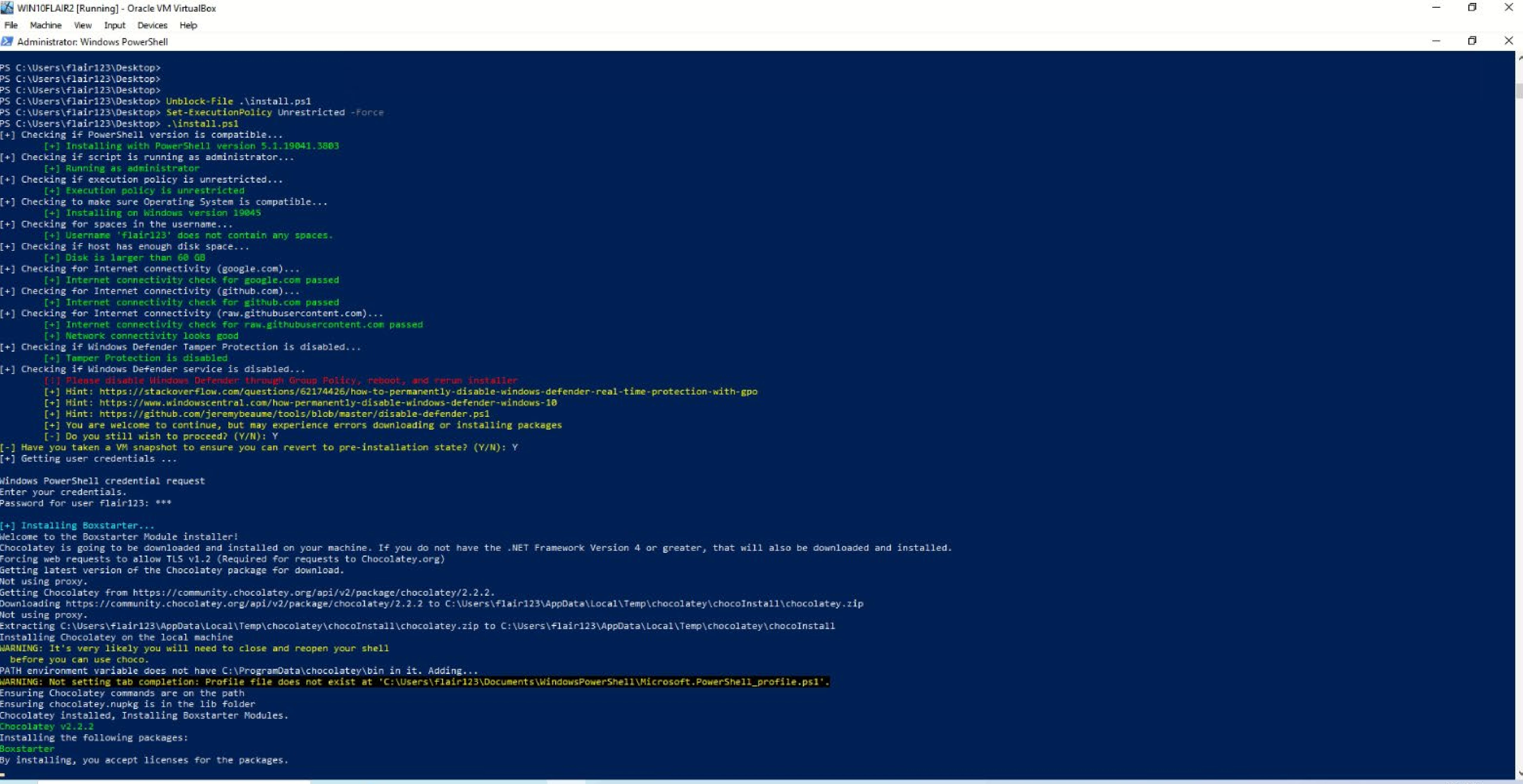
Tamper Protection

Prevents others from tampering with important security features.

Tamper protection is off. Your device may be vulnerable. Dismiss

Off

Learn more



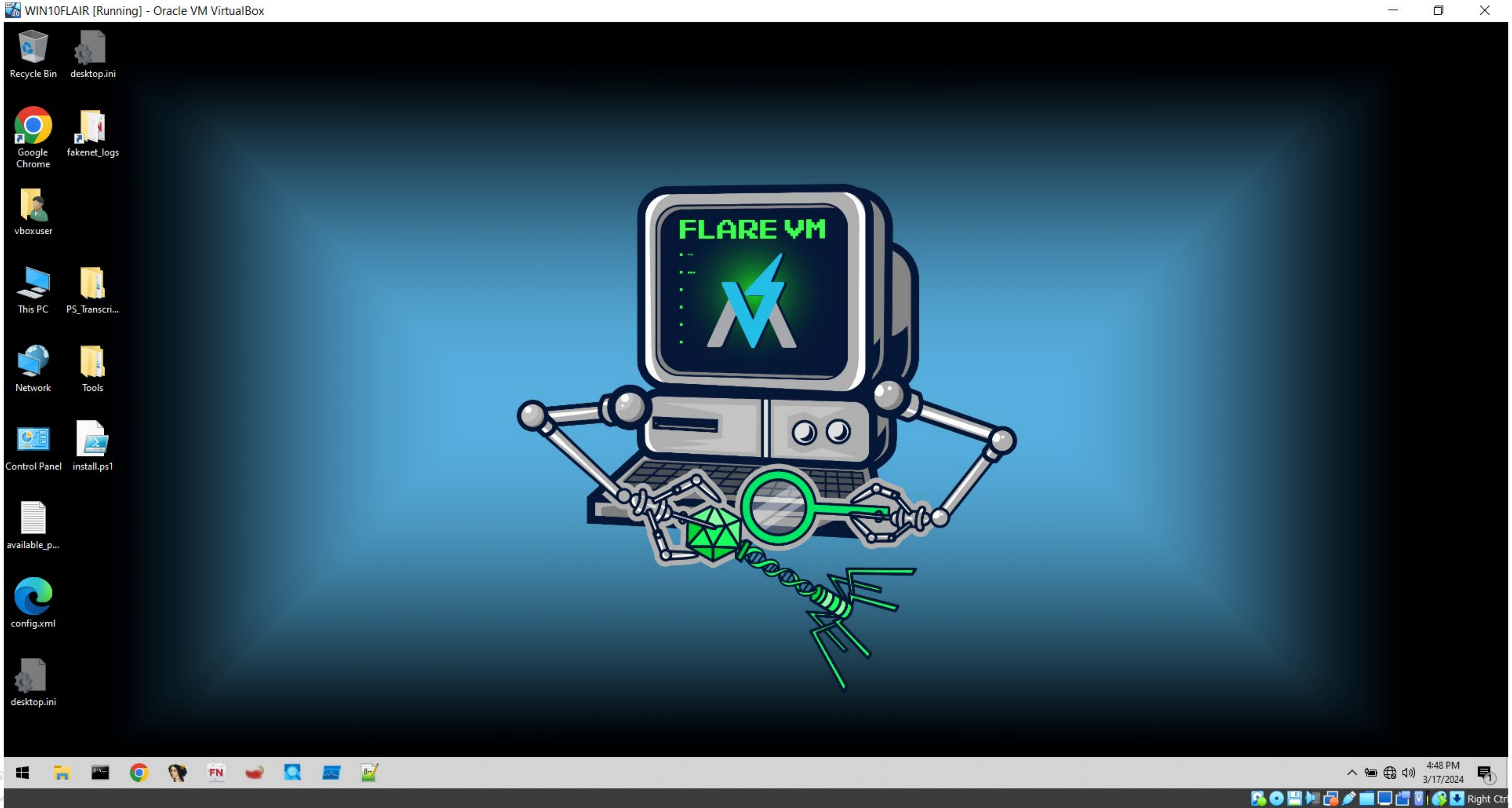
WIN10FLAIR2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Administrator: Windows PowerShell

```
PS C:\Users\flair123\Desktop>
PS C:\Users\flair123\Desktop>
PS C:\Users\flair123\Desktop>
PS C:\Users\flair123\Desktop> Unblock-File .\install.ps1
PS C:\Users\flair123\Desktop> Set-ExecutionPolicy Unrestricted -Force
PS C:\Users\flair123\Desktop> .\install.ps1
[+] Checking if PowerShell version is compatible...
        [+] Installing with PowerShell version 5.1.19041.3803
[+] Checking if script is running as administrator...
        [+] Running as administrator
[+] Checking if execution policy is unrestricted...
        [+] Execution policy is unrestricted
[+] Checking to make sure Operating System is compatible...
        [+] Installing on Windows version 19045
[+] Checking for spaces in the username...
        [+] Username 'flair123' does not contain any spaces.
[+] Checking if host has enough disk space...
        [+] Disk is larger than 60 GB
[+] Checking for Internet connectivity (google.com)...
        [+] Internet connectivity check for google.com passed
[+] Checking for Internet connectivity (github.com)...
        [+] Internet connectivity check for github.com passed
[+] Checking for Internet connectivity (raw.githubusercontent.com)...
        [+] Internet connectivity check for raw.githubusercontent.com passed
        [+] Network connectivity looks good
[+] Checking if Windows Defender Tamper Protection is disabled...
        [+] Tamper Protection is disabled
[+] Checking if Windows Defender service is disabled...
        [!] Please disable Windows Defender through Group Policy, reboot, and rerun installer
        [+] Hint: https://stackoverflow.com/questions/62174426/how-to-permanently-disable-windows-defender-real-time-protection-with-gpo
        [+] Hint: https://www.windowscentral.com/how-permanently-disable-windows-defender-windows-10
        [+] Hint: https://github.com/jeremybeaume/tools/blob/master/disable-defender.ps1
        [+] You are welcome to continue, but may experience errors downloading or installing packages
        [-] Do you still wish to proceed? (Y/N): Y
[-] Have you taken a VM snapshot to ensure you can revert to pre-installation state? (Y/N): Y
[+] Getting user credentials ...

Windows PowerShell credential request
Enter your credentials.
Password for user flair123: ***

[+] Installing Boxstarter...
Welcome to the Boxstarter Module installer!
Chocolatey is going to be downloaded and installed on your machine. If you do not have the .NET Framework Version 4 or greater, that will also be downloaded and installed.
Forcing web requests to allow TLS v1.2 (Required for requests to Chocolatey.org)
Getting latest version of the Chocolatey package for download.
Not using proxy.
Getting Chocolatey from https://community.chocolatey.org/api/v2/package/chocolatey/2.2.2.
Downloading https://community.chocolatey.org/api/v2/package/chocolatey/2.2.2 to C:\Users\flair123\AppData\Local\Temp\chocolatey\chocoInstall\chocolatey.zip
Not using proxy.
Extracting C:\Users\flair123\AppData\Local\Temp\chocolatey\chocoInstall\chocolatey.zip to C:\Users\flair123\AppData\Local\Temp\chocolatey\chocoInstall
Installing Chocolatey on the local machine
WARNING: It's very likely you will need to close and reopen your shell
  before you can use choco.
PATH environment variable does not have C:\ProgramData\chocolatey\bin in it. Adding...
WARNING: Not setting tab completion: Profile file does not exist at 'C:\Users\flair123\Documents\WindowsPowerShell\Microsoft.PowerShell_profile.ps1'.
Ensuring Chocolatey commands are on the path
Ensuring chocolatey.nupkg is in the lib folder
Chocolatey installed, Installing Boxstarter Modules.
Chocolatey v2.2.2
Installing the following packages:
Boxstarter
By installing, you accept licenses for the packages.
```

FLARE Virtual Machine



Behavioral Analysis Essentials

From Tigers, For Tigers Presentations

From Tigers, For Tigers Presentations
Online sessions: April 1 to April 4, 2024

Lecture 1 (Monday, Tuesday)	Lecture 2 (Wednesday, Thursday)
Process Monitor	API Logger and API monitor
Process Explorer or Process Hacker	Monitoring with Netcat
Regshot	Using INetSim
Faking a Network with ApateDNS	Cuckoo Sandbox
ProcDOT	
Packet Sniffing with Wireshark	

From Tigers, For Tigers Presentations

TOOLS	TEAM MEMBERS (CSEC202.600)
Process Monitor	Omar Helal
Process Explorer or Process Hacker	Adi Alghfli
API Logger and API monitor	Kawin Yogam
Regshot: : Highlights changes to the file system and the registry	Yara Abdallah
Faking a Network with ApateDNS	Sara Zako
Monitoring with Netcat	Shreenidhi Bikkavill
Packet Sniffing with Wireshark	Goudy Elimam, Shane Saldanha
Using INetSim	Mohammed Haji, Khalifa Almheiri
ProcDOT: Visualizes Process Monitor logs for easier analysis.	Seifeldin Awaad, Amr Atalla
Cuckoo Sandbox	Farkh Leka Hashimy

From Tigers, For Tigers Presentations

TOOLS	TEAM MEMBERS (CSEC202.601)
Process Monitor	Fatima Mansur, Rania Kanaan, Suhaila Alfalasi
Process Explorer or Process Hacker	Rachel Serena, Simran Bhagchandani, Youssef Elgayar
API Logger and API monitor	Ayush Gowda, Nikita Astionov, Syed Shayan Ali
Regshot: : Highlights changes to the file system and the registry	Mohammed Fahmi, Sufyan Alsayeh, Khalifa Alfalasi
Faking a Network with ApateDNS	Omar Morsy, Majd Katerji, Abdullah Kair
Monitoring with Netcat	Faiza Fatima, Esha Roxy, Aaina Shifas
Packet Sniffing with Wireshark	Krunal Thumar, Anes Zerouati, Ayham Swad
Using INetSim	Ahmad Amer, Karim Al-Karmy, Yousif Naji
ProcDOT: Visualizes Process Monitor logs for easier analysis.	Tayyab Sajid, Ethan Nagooroo, Suva Parvin Srithe
Cuckoo Sandbox	Omar Ahmed, Mohammed Faisal Al Marri, Rashid Faisal Almarri

From Tigers, For Tigers Presentations

TOOLS	TEAM MEMBERS (CSEC202.602)
Process Monitor	Husain Murtaza Ariwala
Process Explorer or Process Hacker	Leen Malkawi, Khalid Alshekhhossin
API Logger and API monitor	Viha Agrawal
Regshot: : Highlights changes to the file system and the registry	Ayman Al Jayyosi
Faking a Network with ApateDNS	Zaman Kakkadath, Muhammad Fahd Khan
Monitoring with Netcat	Omar Jammoul, Moaz ElSayed
Packet Sniffing with Wireshark	Mina Farag, Ahmad Daqruq
Using INetSim	Nay Lin Aung, Muhammad Umer
ProcDOT: Visualizes Process Monitor logs for easier analysis.	Joseph Cremeno
Cuckoo Sandbox	Prisha Modi, Pranav Prasath

Course Overview

- **Title: “CSEC 202 - Reverse Engineering Fundamentals”**

Instructor	Office	Phone	Email	Semester-Year
Emad Abu Khousa	D003		eakcad@rit.edu	Spring-2024
Office Hours:	M: 12:00-01:00 TR: 11:00-12:00			

- **600: TR 12:00-01:20, Room B-107**
- **601: MW 01:05-02:25, Room C-109**
- **602: TR 01:30-02:50, Room D-207**

Thank You and Q&A