Nasirumbi lornah

Kill chain model

- The focus of the paper is cybersecurity based on intelligence collection. This is understanding and stopping the activity of an intruder, rather than just responding to compromises.

- The work serves to describe the intrusion kill chain model that has 7 stages: reconnaissance, weaponization, delivery, exploitation, installation, command and control (C2), and actions on objectives.

- The model states that disrupting a single phase can halt the entire attack, giving the defenders various exploits to stop adversaries.

- There is mention of indicators (atomic, computed, and behavioral) and their lifecycle in threat intelligence.

- The proposal influenced by the paper is to parallel defensive capabilities with the states of the kill chain. It formulates a course of action matrix.

- There is a critical need for complete analysis and reconstruction of intrusions, including unsuccessful attempts, to security.

- This type of strategy, which is intelligence-driven, disputes the myth that the attackers will still rule over the defenders by nature.

MITRE ATT&CK Framework

The MITRE ATT&CK Framework is a comprehensive knowledge base that describes adversary tactics, techniques, and procedures (TTPs) used in cyberattacks. To understand the framework, it's essential to grasp the concepts of tactics, techniques, and procedures in the context of ATT&CK.

Tactics

In the ATT&CK framework, tactics represent the "why" of an attacker's action. They are high-level categories that describe the adversary's objective or goal at a particular stage of an attack. The Enterprise ATT&CK matrix currently includes 14 tactics, such as Initial Access, Execution, Persistence, and Privilege Escalation.

Example: Lateral Movement is a technique in ATT&CK. It describes how adversaries are working their way through the target environment to reach their objective.

Techniques

Techniques answer the question of "how" the adversary performs the attack. This is the description of how adversaries accomplish their tactical objectives. Each tactic in the ATT&CK matrix contains several techniques, which provide additional detail on how an attacker may go about accomplishing their goal.

Example: Under the "Lateral Movement" tactic, a technique could be "Remote Services" (T1021). This technique involves using valid accounts to log into remote systems using built-in or third-party services.

Procedures
Procedures in ATT&CK are concrete implementations of the techniques observed during an attack. They provide tangible examples of exactly how threat actors or malware have used a particular technique.

Example: A procedure for the "Remote Services" technique might be the use of PsExec, a legitimate Windows administration tool, by the APT29 threat group to move laterally within a network.

Relationship Between Tactics, Techniques, and Procedures

The relationship between these elements can be understood as a hierarchy:

1. Tactics are the highest level, representing overall goals.
2. Techniques are specific methods to achieve those goals.
3. Procedures are real-world implementations of techniques.

How would you compare the Cyber Kill Chain and ATT&CK Enterprise matrix? Who do you think could benefit from these models?

The Cyber Kill Chain and MITRE ATT&CK Enterprise matrix are both important frameworks in cybersecurity, but they differ in their approach, scope, and level of detail. To compare these models and discuss their potential beneficiaries, we need to examine their key characteristics and applications.

Comparison of Cyber Kill Chain and ATT&CK Enterprise Matrix

Structure and Scope
The Cyber Kill Chain, developed by Lockheed Martin, presents a linear, seven-stage model of cyberattacks. These stages are: Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command and Control, and Actions on Objectives

In contrast, the MITRE ATT&CK Enterprise matrix offers a more comprehensive and granular approach, with 14 tactics and numerous techniques and sub-techniques. The ATT&CK framework is not linear and recognizes that attackers may use multiple tactics and techniques in varying orders.

Nasirumbi lornah

Focus and Depth
The Cyber Kill Chain primarily focuses on external attacks and the stages leading up to and including the initial compromise. It provides a high-level overview of the attack process.

In contrast, the ATT&CK Enterprise matrix covers a broader range of adversary behaviors, including post-compromise activities, lateral movement, and evasion techniques. It offers more detailed information about specific tactics and techniques used by attackers.

Flexibility and Adaptability

The Cyber Kill Chain follows a more rigid, sequential model of attacks. This can be beneficial for understanding the general flow of an attack but may not capture the complexity of modern, sophisticated threats.

In contrast, the ATT&CK framework is more flexible and adaptable, allowing for a more nuanced understanding of diverse attack patterns and evolving threat landscapes.

Potential Beneficiaries

Both models offer valuable insights for various stakeholders in the cybersecurity ecosystem:

Cyber Kill Chain Beneficiaries

- ***Security Teams***: The Cyber Kill Chain can help security professionals develop a high-level understanding of attack stages and create defensive strategies accordingly.
- ***Executives and Decision-makers***: The model's simplicity makes it useful for communicating cybersecurity concepts to non-technical stakeholders.
- ***Incident Response Teams***: The framework can guide teams in identifying the current stage of an ongoing attack and prioritizing response efforts.

ATT&CK Enterprise Matrix Beneficiaries

- ➔ ***Threat Hunters and Analysts***: The detailed tactics and techniques in ATT&CK can inform advanced threat hunting and analysis activities.
- ➔ ***Security Architects***: The comprehensive nature of ATT&CK can help in designing robust security architectures that address a wide range of potential attack vectors.
- ➔ ***Red Teams and Penetration Testers***: ATT&CK provides a framework for simulating real-world adversary behaviors in security assessments.
- ➔ ***Security Product Developers***: The detailed techniques in ATT&CK can guide the development of more effective security tools and solutions.
- ➔ ***Cybersecurity Researchers***: The framework serves as a common language for describing and categorizing adversary behaviors, facilitating research and knowledge sharing.

Nasirumbi lornah

While both the Cyber Kill Chain and MITRE ATT&CK Enterprise matrix have their strengths, the ATT&CK framework generally offers a more comprehensive and flexible approach to understanding and addressing modern cyber threats. However, the Cyber Kill Chain's simplicity can still be valuable for high-level strategic planning and communication.
Organizations may benefit from using both models in complementary ways: the Cyber Kill Chain for broad strategic planning and the ATT&CK matrix for detailed tactical and operational cybersecurity activities.

Pick a security incident and learn about it. Write briefly about it. Point out the concepts of threat actor, exploit, vulnerability, and (business) impact. (You can find writeups about security incidents from Darknet Diaries and Krebs)

The incident I have chosen is EP 148: Dubsnatch

The Dubsnatch incident involves a teenage music enthusiast, known as Professor Dubstep, who exploited vulnerabilities in online systems to access unreleased music tracks and insider information from the electronic dance music (EDM) industry.

Threat Actor
The primary threat actor in this case was Professor Dubstep, a 13-year-old fan of electronic music who initially had no malicious intent but gradually became involved in more questionable activities.

Exploits and Vulnerabilities
Professor Dubstep exploited several vulnerabilities:

- ***Bitly URL Shortener Flaw***: By adding a '+' to the end of shortened links, users could access the public profile of the account that created the link, revealing all their shortened URLs.
- ***Weak Access Controls***: Management accounts often shared internal documents using the same Bitly accounts used for public promotions, inadvertently exposing sensitive information.
- Social Engineering: Professor Dubstep manipulated other collectors by creating fake "unreleased" tracks to trade for genuine unreleased music.

Business Impact
The incident had several potential impacts on the music industry:

- ***Premature Exposure***: Unreleased tracks and promotional plans were accessed before their intended release dates.
- ***Loss of Competitive Advantage***: Internal memos and promotion plans being exposed could give competitors insight into marketing strategies.
- ***Reduced Track Value***: As noted by Professor Dubstep, when an unreleased track leaks online, "it's over for that track forever," potentially damaging an artist's or label's revenue prospects.

While the full extent of the damage is not detailed in the provided information, the incident highlights the need for improved security practices in the music industry, especially regarding the handling of unreleased material and internal communications.

c) Install Debian on Virtualbox. Report your work, including the environment (including host OS, the real physical computer used), the steps you took, and their results.

Environment
Host OS: Windows 10 Home
Physical Computer: LAPTOP-8OIJK58N
Processor: AMD Ryzen 3 3200U with Radeon Vega Mobile Gfx (2.60 GHz)
RAM: 4 GB (3.42 GB usable)
System Type: 64-bit operating system, x64-based processor

Installation Steps and Results

1. Download Debian ISO

I downloaded the latest Debian 12 AMD64 Netinst ISO from the official Debian website (debian.org). The Netinst version is ideal for my setup as it requires an internet connection during installation but results in a smaller initial download.

Note: The Debian ISO file I downloaded is not meant to be installed directly on my Windows system. It's designed to be used as a virtual disk image within VirtualBox to install Debian in a virtual environment. So after downloading the Debian ISO, my next step is to download and install VirtualBox on my Windows 10 system. Once VirtualBox is installed, I will create a new virtual machine and use the Debian ISO during the setup process of that virtual machine.

2. Install VirtualBox

I downloaded and installed VirtualBox 7.1.4 from (virtualbox.org), selecting the Windows host version.

Note: After a successful download I got an error while trying to install the virtual box installer.

VirtualBox cannot be installed because you do not have Microsoft Visual C++ 2019 Redistributable Package. Please download it before installing VirtualBox.

I downloaded and installed both x86 and x64 versions of the multi-installer Visual C++ 2015, 2017, 2019, and 2022 redistributable. Restarted my PC after the installation and I was able to install it properly. Note: Don't install the ARM64
https://learn.microsoft.com/en-US/cpp/windows/l…

Nasirumbi lornah

I used the Microsoft community to get this advice which worked

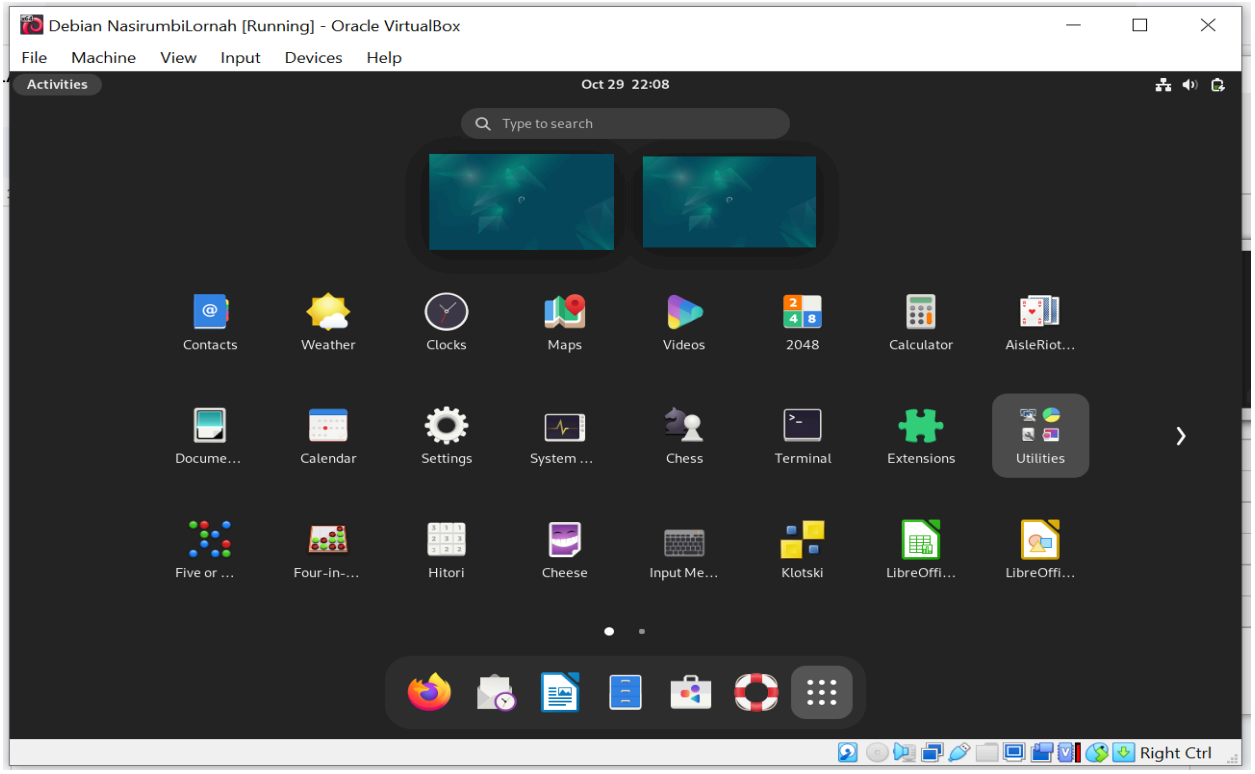
3. Create a New Virtual Machine

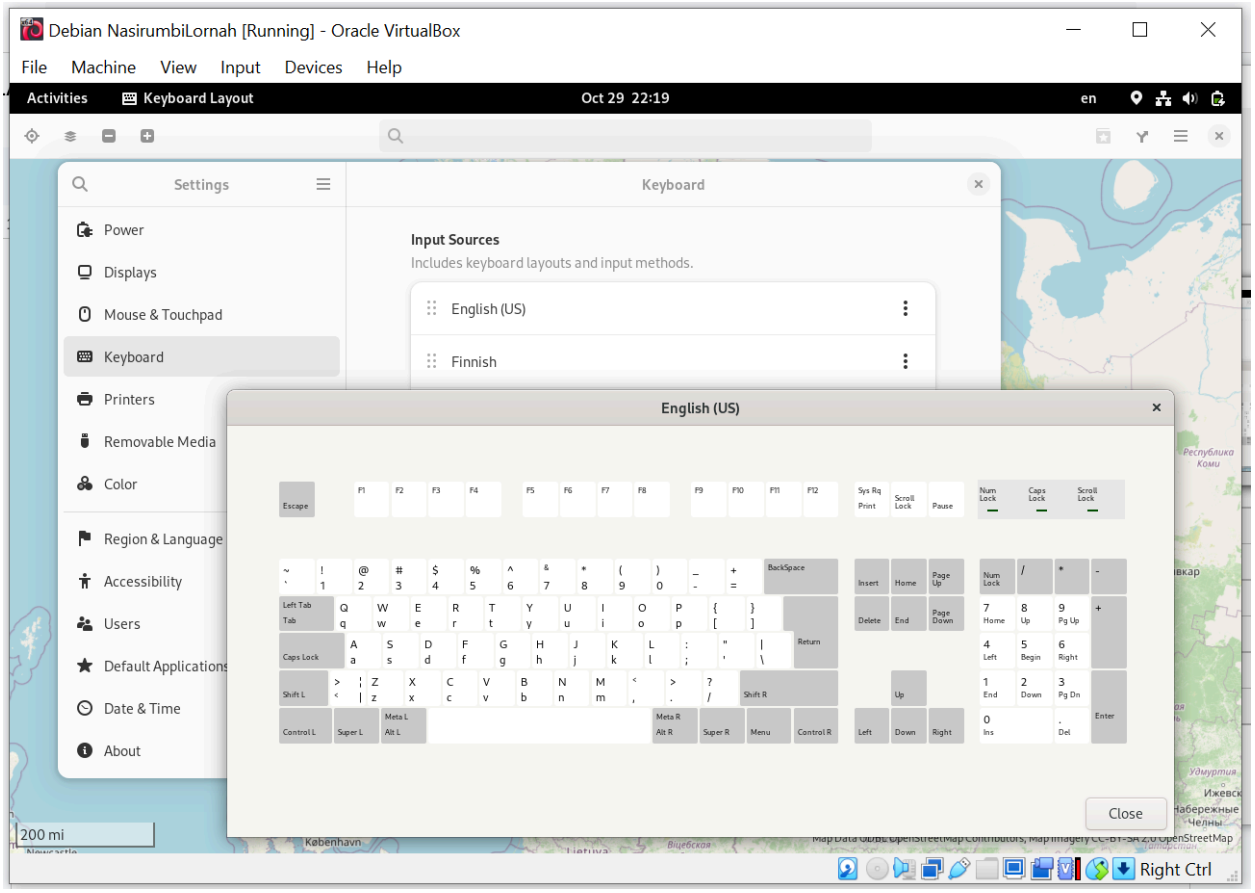
I launched VirtualBox selected expert mode and created a new virtual machine with the following settings:
- Name: Debian Nasirumbilornah
- Type: Linux
- Version: Debian (64-bit)
- Memory: 2024 MB (considering the host system has 4 GB RAM)
- Hard disk: Created a virtual hard disk, dynamically allocated, 20 GB in size

Note: Configurations of the Virtual Machine Settings are already done. I had to check and confirm the following before starting VM.
- System > Processor: Allocated 1 CPU core
- Storage: Attached the downloaded Debian ISO to the virtual optical drive
- Network: Enabled NAT for internet connectivity

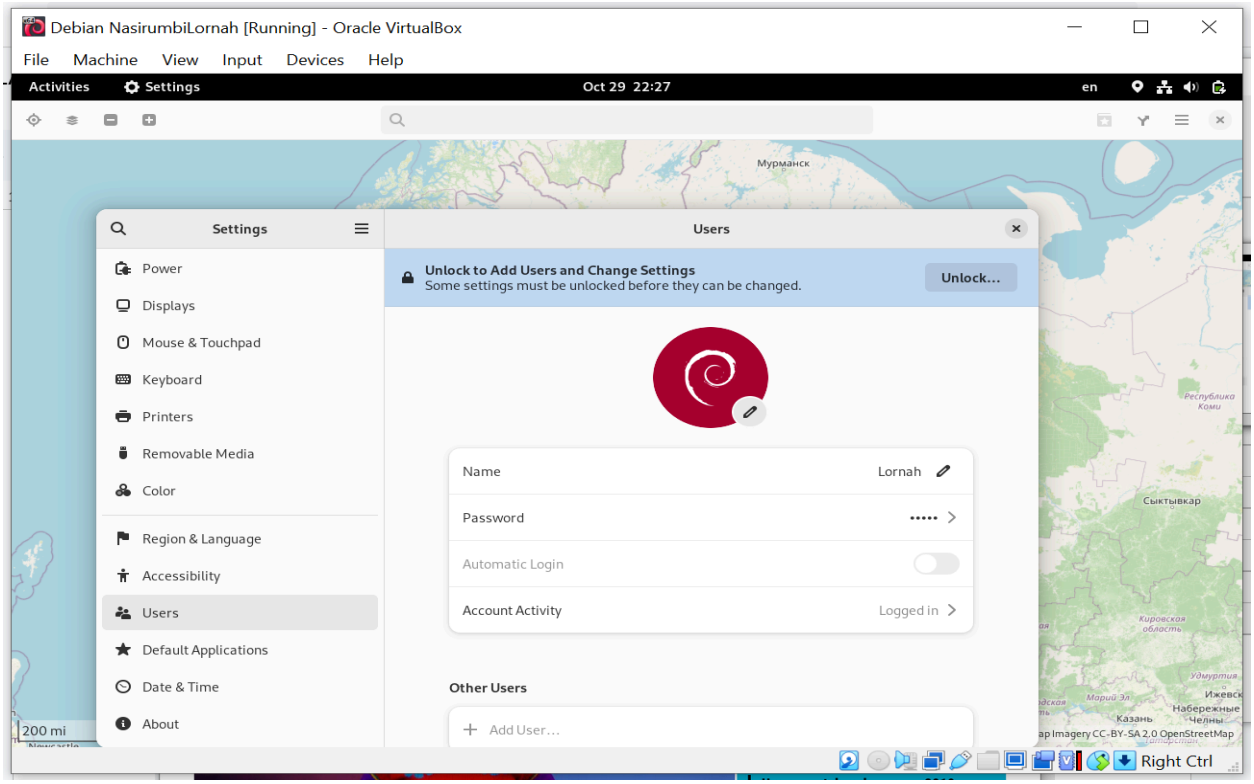
4. Start Installation
I started the virtual machine and began the Debian installation process:
I selected to install from the boot menu
Choose the language(English), location, and keyboard layout.
Created a user name (Lornah123)
Created login name (Lornah)and password.
Note: At this point, I am able to access my VM

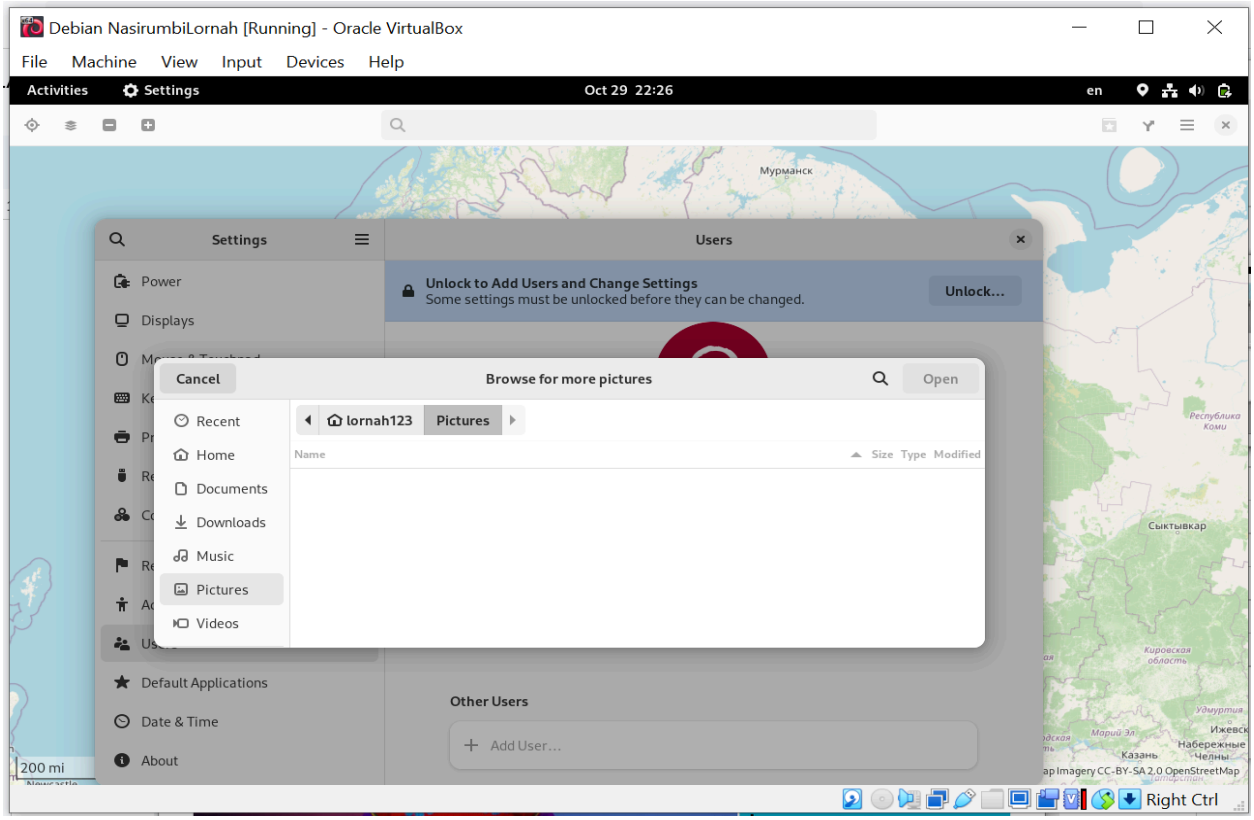
Nasirumbi lornah





Nasirumbi lornah





Nasirumbi lornah

References:

1. MITRE. (2024). MITRE ATT&CK®. Retrieved October 28, 2024, from https://attack.mitre.org/

2. Strom, B. E., Applebaum, A., Miller, D. P., Nickels, K. C., Pennington, A. G., & Thomas, C. B. (2018). MITRE ATT&CK™: Design and Philosophy. The MITRE Corporation.

3. Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. Leading Issues in Information Warfare & Security Research, 1(1), 80.

4. https://darknetdiaries.com/episode/148/