Cyber Warriors: A Comprehensive Introduction to Cybersecurity Tools and Techniques

June 24-28, 2024

Murtuza Jadliwala

murtuza.jadliwala@utsa.edu

SPrITE LAB

UTSA

NSF

Introductions to Kali Linux and Security Toolkit

Penetration Testing/Red Teaming

- **Penetration Testing (or Pen-Testing)**: process of safely exploiting vulnerabilities without impacting the actual information system, network or business operations.

- Scope of penetration testing:
  - **General (Open)**: Can any known vulnerability be exploited on the target system or network to compromise it?
  - **Focused (Goal-based)**: Can a target system or network be compromised to accomplish certain goals/objectives by exploiting one or more known vulnerabilities.

- **Red Teaming**: process of evaluating the effectiveness of an organization to defend against cyber threats and improve its security by any possible means.
  - Typically, Red Teaming involves significant amount of penetration testing.

Difference between Hacking and Pen-Testing

Hacking	**Pen-Testing**
• Vulnerabilities are exploited for nefarious goal/objective.	• Vulnerabilities are exploited for a benevolent goal/objective
• Involves employing new, as well as zero-day vulnerabilities.	• Testing does not typically attempt to uncover zero-day vulnerabilities.
• Exploitation process generally not very structured.	• Exploitation process typically follows a well-defined attack kill chain

Testing Methodology – Attack Kill Chain

- Most Pen-Testing activities earlier on were generally executed in an unstructured fashion
  - Pen-Testers felt that structure hindered their creativity!
  - Also, malicious hackers typically don't follow any structure, and pen-testers wanted to replicate that mindset!
- In 2009, Mike Cloppert of Lockhead Martin introduced the notion of Attack Kill Chain.
- An Attacker's kill chain typically consists of four sequential processes
  1. Reconnaissance
  2. Delivery
  3. Exploitation
  4. Post-Exploitation

Phase I – Reconnaissance

- Process of learning about of the target system, its users and the exploitable resources on that system.
- Most important phase of the attack kill chain.
  - Reconnaissance is important to determine the scope of the attack, attack surface and post-exploitable actions.
- Two types of reconnaissance activities:
  - **Passive**: Does not directly interact with the target system. Could employ publicly-available or open-source intelligence (OS-INT). For example, web scraping.
  - **Active**: collects intelligence by interacting (often in a valid fashion) with the target system. For example, port scanning.
  - Passive reconnaissance is undetectable, while active reconnaissance can be detected by the target!
  - Reconnaissance phase is required for vulnerability assessment (or for determining the attack surface)!

Phase II – Delivery

- This phase involves selection and development of the weapon (including the payload) that will be used to complete the exploit during the attack.
  - This "weapon" is typically made up of a set of actions (that needs to be carried out by an attacker) or an attack script (that needs to be executed on the target system or interface).
  - The exact "weapon" will depend on the type and goal (objective) of the attack.
- Another important aspect of the Delivery phase is the **Delivery Route** or the path taken to deploy the attack weapon to its target.
  - Could include remote or physical techniques.

Phase III – Exploitation

- This is the phase when the exploit (or weapon) is successfully applied or executed.

- Depending on the attack weapon or strategy, this could be a **multi-step** process.
  - This is especially true when the target is a large organization or enterprise.
  - Also depending on the success of the employed attack weapon or strategy, multiple attempts may be required.

Phase IV – Post-Exploitation

- This post successful exploitation phase, typically comprises of two steps (in no particular order):
  - **Action towards goal or objective**: Here the attacker attempts, to accomplish the actual goal of the planned compromise (for example, data stealing or denial of service).
    - In this step, the attacker may need to accomplish vertical escalation or horizontal escalation on the target system/network to accomplish the goal/objective.
  - **Persistence**: This allows the attacker to maintain long-term communication/access to the compromised system.
    - Useful if there is value in maintaining such long-term access.
    - Not always needed and it increases risk of detection.
    - Accomplished by means of specially designed tools, often referred as trapdoors or backdoors.

What is Kali Linux?

- Kali is a Debian-derived Linux distro designed for digital forensics and penetration testing.
- Platform of choice for malevolent hackers/attackers!
- Developed by Mati Aharoni and Devon Kearns of Offensive Security through the rewrite of BackTrack (previous information security testing Linux distribution based on Knoppix).
- Originally, it was designed with a focus on kernel auditing, from which it got its name **K**ernel **A**uditing **LI**nux.
- Available in both 32-bit and 64-bit images for a variety of hardware devices (based on both x-86 and ARM architectures), including Android supported devices.
- Original Kali used to run in a "default root mode", i.e., root mode was default
  - As Kali came to be used as a main-stream OS, current versions of Kali run in a "default non-root mode".
  - Tools interactively ask for root access as needed!

Kali Linux Tools

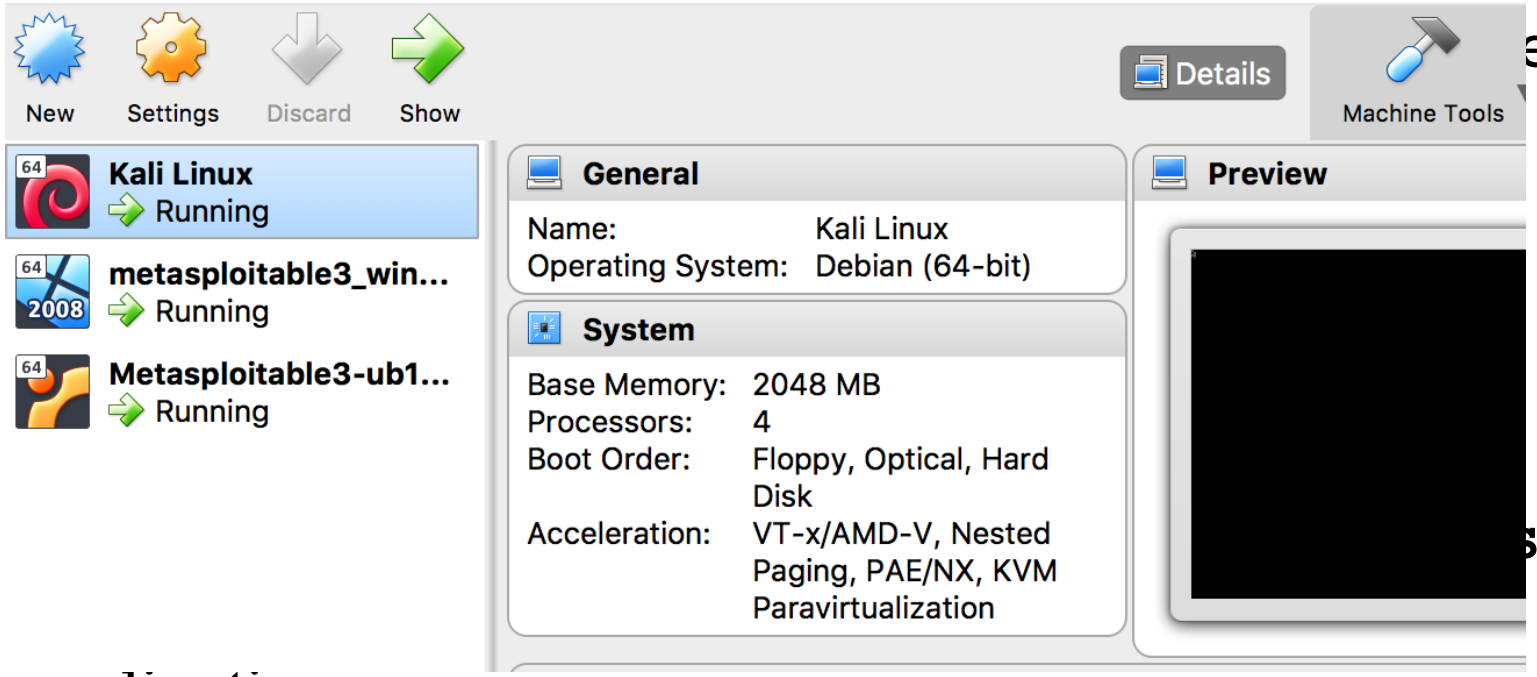
- Broad variety of tools for:
  - Information Gathering
  - Vulnerability Analysis
  - Wireless Attacks
  - Web Application Attacks
  - Exploitation Tools & Frameworks
  - Forensics
  - Stress Testing
  - Sniffing & Spoofing
  - Password Attacks
  - Maintaining Access and Persistence
  - Reverse Engineering
  - Hardware Hacking
  - Reporting

Accessing Kali Linux for this Camp

- Each student in the camp will have access to their own Kali Virtual Machine (VM).
- Username/passwords and credentials for the root account will be individually emailed to each student!
- Do not share your credentials with other students.
- Always adhere to the student code-of-conduct as outlined in the camp schedule.
  - If you feel something you are doing is wrong, it probably is! Check with the instructor before going ahead.

- How to access my Kali VM?
  1. Open a remote desktop (RDP) client on you operating system.
  2. For Computer/hostname type, range.secretlab.page:3310X. (note – 33310X is the port number. Each student must have received a unique port number in the email from me)
  3. For Username/Password: Enter the credentials provided to you.
  4. Connect.

Need Additional Practice?

- Install your own Kali Linux VM using a VM software such as Virtualbox or VMWare.
- 

- applications.
  - Available at https://github.com/webpwnized/mutillidae