BootCon: Hackable III

Emyrca Feliciano Estrada, Thomas Baquiran, Gerardo J. Rivera, Jeudy Torres

Table of Contents

Technical Background

Preview

Video Presentation

Recap

Mitigation

Q & A

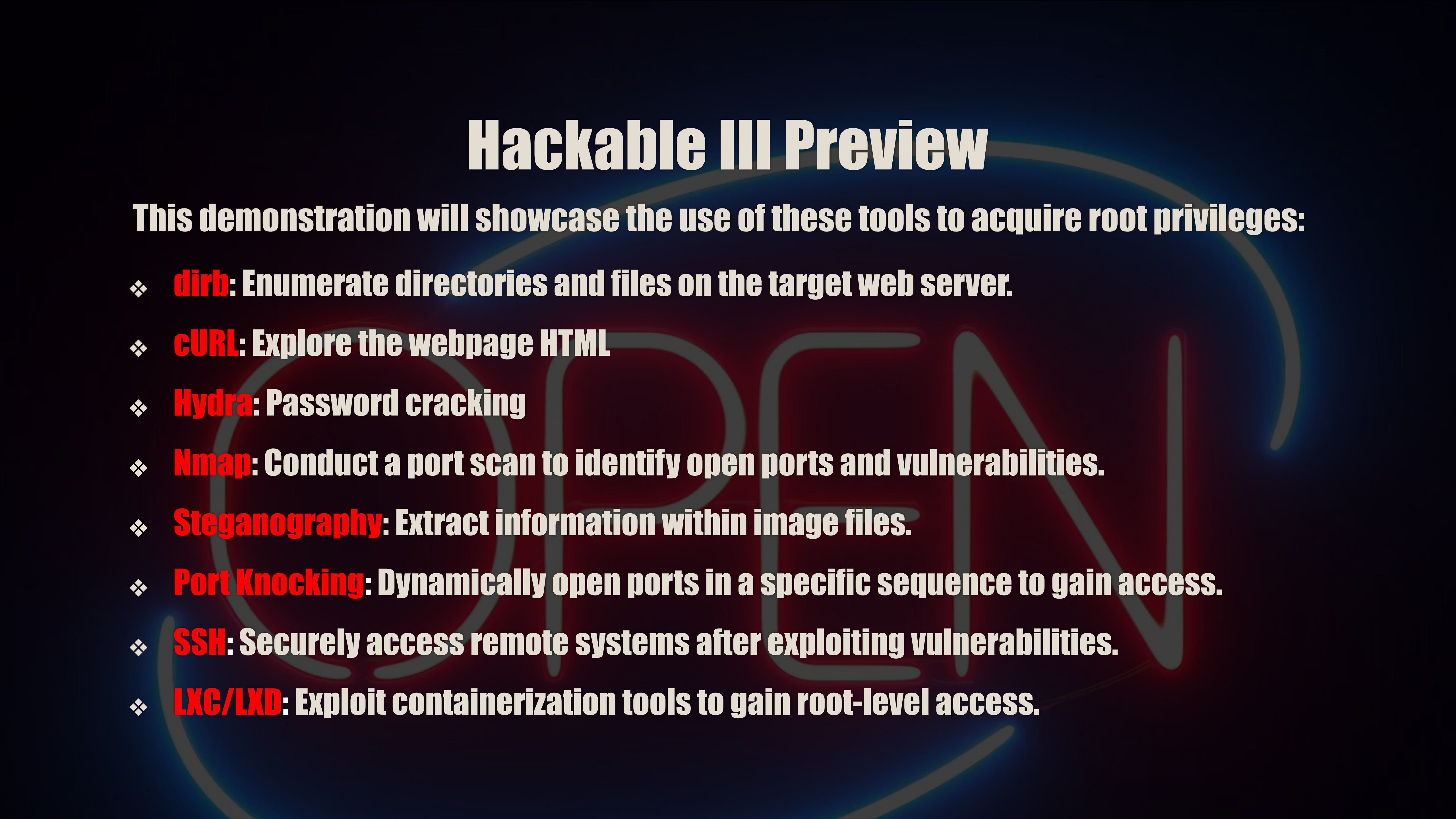
Technical Background

We have chosen to delve into the Hackable: III challenge by Elias Sousa from VulnHub.com, a platform renowned for its cybersecurity challenges.

This challenge is rooted in its educational value and relevance to real-world cybersecurity scenarios. As aspiring professionals, we recognize the importance of hands-on experience in identifying and mitigating security threats. By dissecting this Medium-Level challenge, we hope to not only enhance our own skills but also contribute to the broader cybersecurity community by sharing insights, strategies, and lessons learned.

To prepare for this presentation, we conducted thorough research on the Hackable: III challenge, including its background, objectives, and potential vulnerabilities. This involved analyzing relevant resources and experimenting with similar challenges to refine our skills. Through a combination of hands-on experimentation, we have equipped ourselves with the knowledge and skills necessary to effectively navigate the Hackable: III challenge and provide valuable insights to the audience.

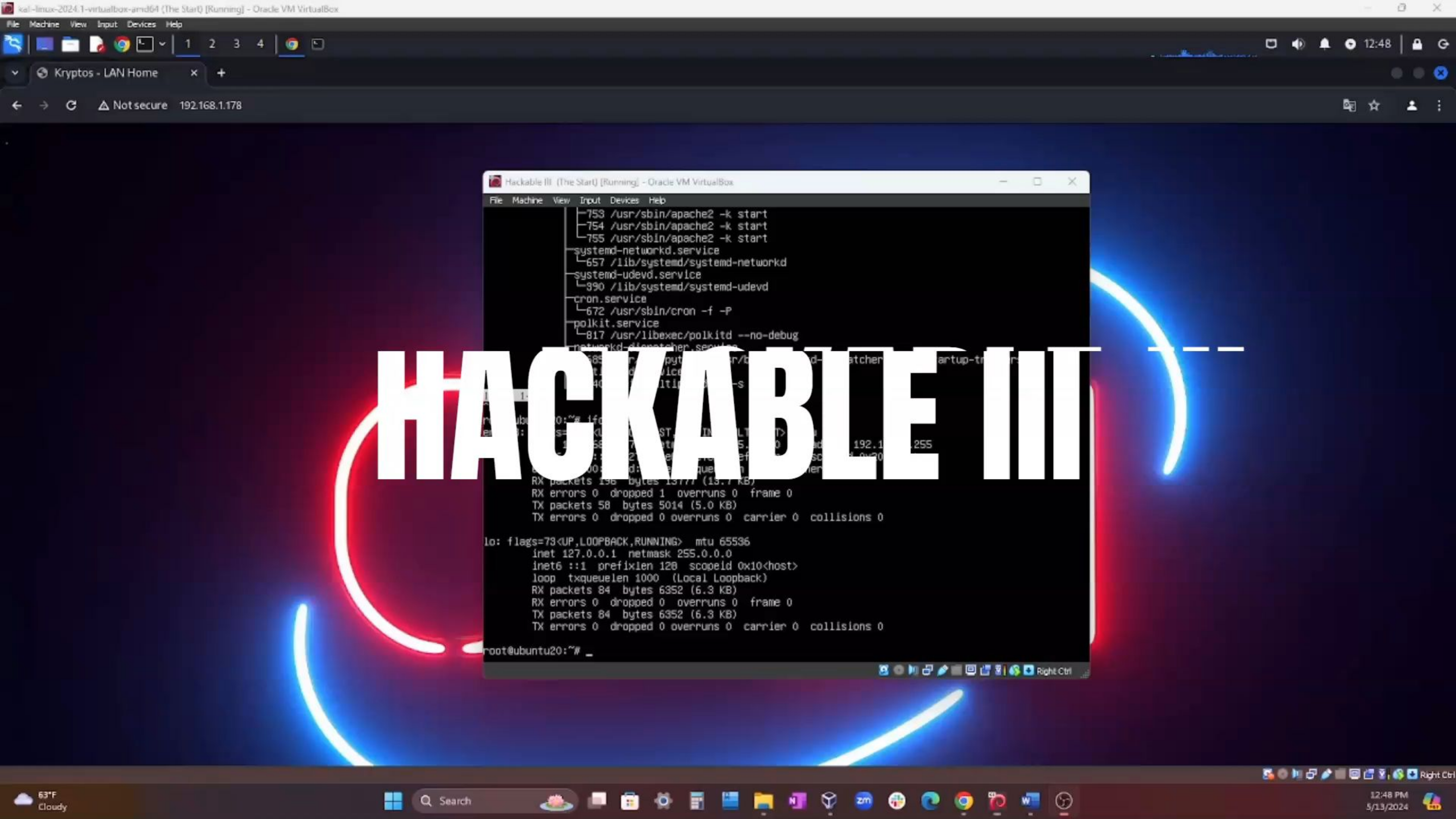
In our exploration, we engaged in network reconnaissance to enumerate directories and files on the target web server, explored webpage HTML for potential vulnerabilities, and conducted password cracking to uncover weak credentials. Additionally, we performed port scans to identify open ports and vulnerabilities on the target system, explored image files for hidden information, and investigated dynamic port access. Lastly, we securely accessed remote systems after exploiting identified vulnerabilities and attained root-level access on the target system through containerization tools.



Hackable III Preview

This demonstration will showcase the use of these tools to acquire root privileges:

- dirb: Enumerate directories and files on the target web server.
- cURL: Explore the webpage HTML
- Hydra: Password cracking
- Nmap: Conduct a port scan to identify open ports and vulnerabilities.
- Steganography: Extract information within image files.
- Port Knocking: Dynamically open ports in a specific sequence to gain access.
- SSH: Securely access remote systems after exploiting vulnerabilities.
- LXC/LXD: Exploit containerization tools to gain root-level access.


kali-linux-2024.1-virtualbox-amd64 (The Start) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
12:48
Kryptos - LAN Home
Not secure 192.168.1.178
Hackable III (The Start) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Right Ctrl
63°F
Cloudy
Search
12:48 PM
5/13/2024

HACKABLE III

```
              ├─753 /usr/sbin/apache2 -k start
              ├─754 /usr/sbin/apache2 -k start
              └─755 /usr/sbin/apache2 -k start
             ├─systemd-networkd.service
             │ └─657 /lib/systemd/systemd-networkd
             ├─systemd-udevd.service
             │ └─390 /lib/systemd/systemd-udevd
             ├─cron.service
             │ └─672 /usr/sbin/cron -f -P
             ├─polkit.service
             │ └─817 /usr/libexec/polkitd --no-debug

        RX packets 196  bytes 13777 (13.7 KB)
        RX errors 0  dropped 1  overruns 0  frame 0
        TX packets 58  bytes 5014 (5.0 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 84  bytes 6352 (6.3 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 84  bytes 6352 (6.3 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@ubuntu20:~# _
```

Hackable III Recap

- Identified login page and potential entry points on webpage
- Extracted files, usernames, and concealed information
- Systematically tried login credentials for access
- Conducted scans for vulnerabilities and changes in network
- Cracked passwords and gained unauthorized access
- Leveraged obtained credentials for machine entry
- Investigated files and directories for sensitive data
- Elevated privileges and gained additional access rights
- Attained root access through containerization exploitation

Mitigations

- Directory Enumeration: Implement directory listing restrictions and access controls on the web server to prevent unauthorized enumeration of directories and files.
- HTML Exploration: Regularly review and sanitize HTML code to remove malicious scripts or hidden elements and implement content security policies (CSP) for controlled resource loading.
- Password Cracking: Enforce strong password policies and implement account lockout mechanisms to deter brute force attacks.
- Port Scanning: Utilize firewalls to block unauthorized access to open ports and implement intrusion detection systems (IDS) for monitoring network traffic.
- Image File Analysis: Restrict file upload permissions, validate uploaded files, and use steganalysis tools to detect hidden information in images.
- Port Knocking: Establish strong firewall rules and utilize port knocking techniques with encryption and authentication to control port access.
- Secure Remote Access: Enforce strong authentication methods, such as public key and multi-factor authentication (MFA), and regularly update SSH server software.
- Containerization Security: Maintain updated containerization tools and host systems and enforce proper network segmentation to prevent lateral movement within containerized environments.

Hackable III Q & A

Did you Enjoy the presentation?

...But Before We Go, We Have a Final Slide!

A Heartfelt Thank You!

To our dedicated Teacher and TA's,

Your unwavering support and dedication throughout the six-month course have been nothing short of extraordinary. You've not only been our guides in this educational journey but also our mentors, friends, and inspirations.

The knowledge you've imparted and the wisdom you've shared have transformed this course into a memorable adventure. The fun, laughter, and camaraderie we've shared will forever be etched in our hearts.

As we conclude this chapter, we want to express our deepest gratitude for everything you've done. We will miss your guidance, your patience, and your infectious enthusiasm for learning.

While we may be parting ways for now, we look forward to the day we cross paths again. Until then, please remember the difference you've made in our lives and the fond memories we've created together.

From the bottom of our hearts, thank you!