OFFENSIVE SECURITY
Crash course

Think Like a Hacker, Defend Like a Pro

SESSION 1 HANDOUT

Foundations & Environment Setup

Prince Sultan University

Automated Systems & Computing Lab (ASCL)

Instructor: **Eng. Mahmoud Khalifa**

Cybersecurity Research Engineer at ASCL

Email: mzian@Psu.edu.sa

Table of Contents

1 Course Overview

Welcome, Future Security Professional!

You're about to embark on an exciting journey into Offensive Security - where you'll learn to think like a hacker to become an exceptional defender!

This three-day intensive training course is designed to give you a comprehensive understanding of how attackers think and operate, enabling you to better defend systems and networks.

Course Philosophy

"To defend effectively, you must think like an attacker."

By understanding offensive techniques, you'll be better equipped to:

- Identify vulnerabilities before malicious actors do
- Implement robust security measures
- Conduct security assessments
- Develop a security-conscious approach to system design

Course Structure

SESSION 1	SESSION 2	SESSION 3
Foundation & Setup	Attack Techniques	Advanced Topics
★ TODAY ★	Next Session	Final Session

Session 1 - Foundations (Today):

- Environment setup (VirtualBox + Kali Linux)
- Linux fundamentals and command line mastery
- Understanding the complete attack lifecycle
- Hands-on challenges with OverTheWire Bandit
- Research assignment on security topics

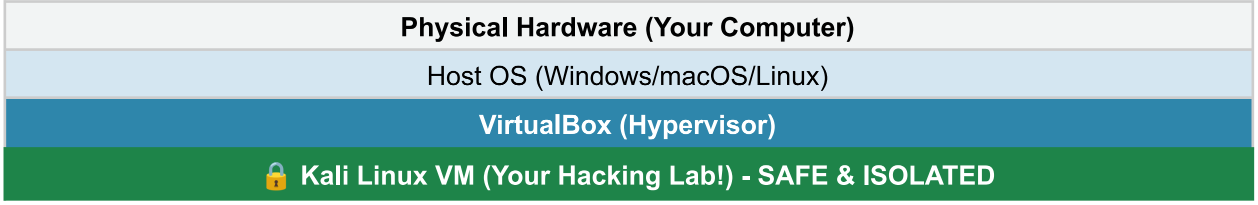
2 Setting Up Your Security Lab

Why VirtualBox and Kali Linux?

Virtualization allows you to run multiple operating systems on a single physical machine. Think of it as creating a "computer within a computer."

Benefits for Security Training:

- Isolation: Keep potentially dangerous tools separate from your main system
- Snapshots: Save and restore system states easily
- Safety: Experiment without risking your primary operating system
- Portability: Move your entire lab to different machines



Physical Hardware (Your Computer)

Host OS (Windows/macOS/Linux)

VirtualBox (Hypervisor)

🔒 Kali Linux VM (Your Hacking Lab!) - SAFE & ISOLATED

Installation Steps

Step 1: Download VirtualBox

- Visit: https://www.virtualbox.org
- Download the version for your operating system
- Run the installer and follow the wizard

Step 2: Download Kali Linux

- Visit: https://www.kali.org/get-kali/
- Download the VirtualBox pre-built VM image (.ova file)
- Choose the 64-bit version (~4GB download)

Step 3: Import and Configure

- File → Import Appliance → Select .ova file
- Settings: RAM: 2048 MB min, CPU: 2 cores, Storage: 20 GB
- Network: NAT mode for internet with isolation

Step 4: First Boot - Default Credentials

- Username: kali | Password: kali

⚠️ **IMPORTANT**

Change the default password immediately! Run: passwd

```
# Change your password:
passwd
# Enter old password: kali
# Enter new password: [your secure password]
```

3 Linux Fundamentals

Why Learn Linux?

- Most servers run Linux - it's the backbone of the internet
- Essential for security professionals - most tools are Linux-based
- Command-line proficiency is crucial for penetration testing
- Understanding Linux is fundamental to offensive security

Linux File System Structure

/	Root directory (top of file system)
/home	User home directories
/etc	System configuration files
/var	Variable data (logs, temporary files)
/bin	Essential command binaries
/tmp	Temporary files

Essential Commands - Navigation

```
pwd                   # Print working directory
ls                    # List files
ls -la                # List all files with details
cd /home/kali         # Change directory
cd ..                 # Go up one directory
cd ~                  # Go to home directory
mkdir folder_name     # Create directory
touch file.txt        # Create empty file
cp file1 file2        # Copy file
mv old.txt new.txt    # Move/rename file
rm file.txt           # Remove file
rm -rf folder/        # Remove directory (CAREFUL!)
```

Essential Commands - Text & Search

```
cat file.txt          # Display file contents
less file.txt         # View file page by page
head -n 10 file.txt   # Show first 10 lines
tail -n 10 file.txt   # Show last 10 lines
grep "pattern" file   # Search for pattern
grep -r "pass" /etc/  # Recursive search
find / -name "*.txt"  # Find files by name
```

File Permissions

Permission values: r (4) = Read | w (2) = Write | x (1) = Execute

```
chmod 644 file.txt    # rw-r--r-- (owner read/write)
chmod 755 script.sh   # rwxr-xr-x (executable)
chown user:group file # Change ownership
```

4 The Cyber Attack Lifecycle

Every cyber attack follows a structured approach. Understanding this lifecycle helps defenders anticipate and prevent attacks at each stage.

PREPARATION	FOOTHOLD	EXPANSION	MISSION
01-Recon 02-Resource Dev 03-Initial Access 04-Execution	05-Persistence 06-Priv. Escalation 07-Defense Evasion 08-Credential Access	09-Discovery 10-Lateral Move 11-Collection 12-C2	13-Exfiltration 14-Impact

This framework is based on the MITRE ATT&CK framework.

Key Stages Explained

Stage 01: Reconnaissance

Gathering information about the target. Passive (no interaction) vs Active (direct probing).

```
whois example.com      # Domain info
nmap -sV target.com    # Port scanning
dig example.com        # DNS queries
```

Stage 03: Initial Access

Gaining first foothold: phishing, exploiting vulnerabilities, credential attacks.

Stage 05: Persistence

Maintaining access: backdoors, new accounts, scheduled tasks, SSH keys.

Stage 06: Privilege Escalation

Gaining higher permissions: SUID exploits, kernel exploits, sudo misconfigurations.

```
find / -perm -4000 2>/dev/null  # Find SUID binaries
sudo -l                         # Check sudo privileges
```

5 Essential Commands Cheat Sheet

Command	Description
`ls -la`	List all files with details
`cd / pwd`	Change directory / Print working directory
`cat / less / head / tail`	View file contents
`grep pattern file`	Search for pattern in file
`find / -name file`	Find files by name
`chmod 755 file`	Change file permissions
`ps aux`	List running processes
`netstat -tuln`	Show network connections
`whoami / id`	Show current user / user ID
`ssh user@host`	Secure shell connection
`nmap -sV target`	Network/port scanner
`nc host port`	Netcat - network utility
`wget / curl url`	Download files from web
`tar -czf / -xzf`	Create/extract archives

6 Hands-On Assignment: OverTheWire Bandit

🎯 YOUR FIRST CHALLENGE!

Complete Bandit levels 0-20 to build fundamental Linux command-line skills essential for penetration testing.

Assignment Details:

- URL: https://overthewire.org/wargames/bandit/
- Objective: Complete levels 0 through 20
- Deadline: Before Session 2
- Expected Time: 4-6 hours (spread across multiple days)
-

Getting Started:

```
ssh bandit0@bandit.labs.overthewire.org -p 2220
# Password: bandit0
```

Document your solutions with: level number, commands used, and explanations.

Share the last password for challenge 20 on mzian@psu.edu.sa

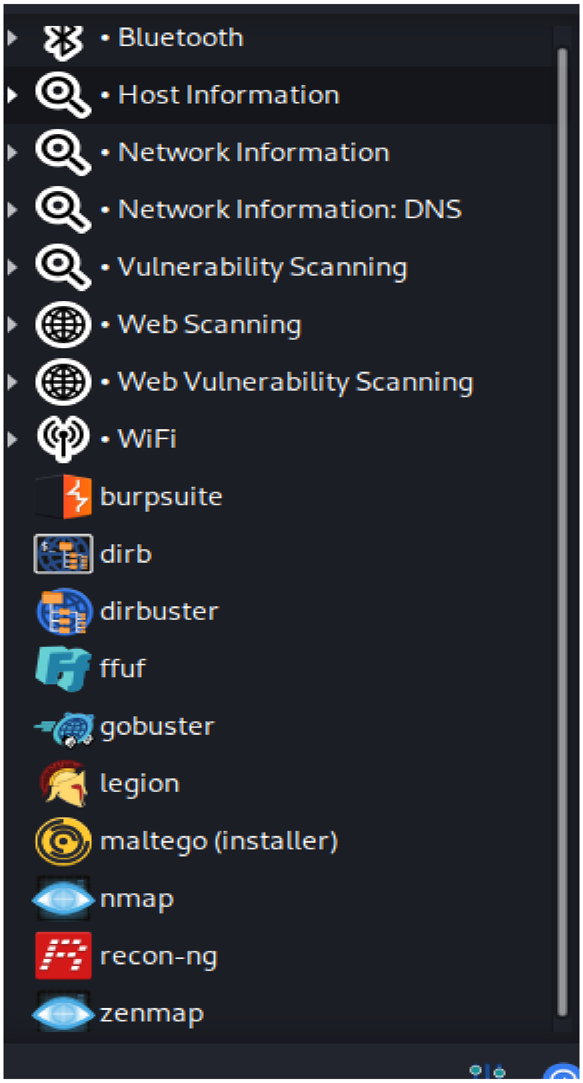
7 Research Assignment

📋 REQUIRED RESEARCH ASSIGNMENT

Due: Before Session 2

Assignment Overview

You are required to research and practice on reconnaissance tools. This assignment will help you understand real-world attack scenarios and how the concepts we learn apply in practice.



📋 Your Task:

For the reconnaissance , research and document:

- Do research on tools used in this stage
- Brief description of each tool (2-3 sentences)
- Screenshot from each tool during the experiment
- Basic command syntax and usage examples

Submission Format

- Written Report: (PDF or Word document)
- Include references/sources
- Submit via email to: mzian@psu.edu.sa
- Subject line: "[Cyber security workshop] Research Assignment - [Your Name]"

📅 Due: Before Session 2

8 Additional Resources

Essential Websites

- OverTheWire: https://overthewire.org - Practice CTF challenges
- TryHackMe: https://tryhackme.com - Guided security learning
- HackTheBox: https://www.hackthebox.com - Advanced challenges
- OWASP: https://owasp.org - Web application security
- MITRE ATT&CK: https://attack.mitre.org - Attack framework reference

Recommended Reading

- The Web Application Hacker's Handbook - Dafydd Stuttard
- Penetration Testing - Georgia Weidman
- The Hacker Playbook 3 - Peter Kim

Certifications to Consider

- CEH - Certified Ethical Hacker
- OSCP - Offensive Security Certified Professional
- CompTIA Security+ - Foundational certification

9 Important Legal & Ethical Notes

⚠️ CRITICAL REMINDERS

1. Authorization is MANDATORY
NEVER test systems you don't own. ALWAYS get written permission.

2. Illegal Activities Have Consequences
Unauthorized access is a crime with fines and imprisonment.

3. Safe Practice Environments Only
Use: OverTheWire, TryHackMe, HackTheBox, your own isolated VMs.

With great power comes great responsibility.

Session 1 Complete! 🎉

"The journey of a thousand hacks begins with a single command."

Keep practicing, stay curious, and remember:

Every expert was once a beginner!

📝 Before Session 2 Checklist

- Complete Bandit levels 0-20 share the password for challenge 2 on email
- Complete Research Assignment Send the pdf on email (not allow to use Gen AI content)

Email mzian@psu.edu.sa

See you in Session 2!

Prince Sultan University
Automated Systems & Computing Lab (ASCL)
Eng. Mahmoud Khalifa | ASCL@Psu.edu.sa