

NSU CyberSec Launchpad

Introduction to CTF & Cyber Security

Class 1: Foundations & Core Concepts

About Us

SHAFEE SADMAN TONROY

Red Team Specialist, CTF Player, Former
DecSecOps Engineer at MIST Cyber Range,, Former
President of MIST Cyber Security Club

Achivement: 4th Runner-up, WTISD Nattional
Hackathon 2025
9th position in EWU CTF

M.M. Tamim Sharif

DFIR Analyst, CTF Player, Vice President of
MIST Cyber Security Club

Achivement: 4th Runner-up, WTISD
Nattional Hackathon 2025
1st Runner-up , National MiniCTF(solo)
17th in HacktheBox Sharlocks (Globally)

What You'll Learn

Today's Core Concepts

Understanding the CIA Triad (Confidentiality, Integrity, Availability).

Ethical vs. Malicious Hacking

Exploring the intentions and methodologies behind different types of hacking.

Specialized Topics

- Kali Linux
- Cryptography
- Digital Forensics
- Web Hacking
- Reverse Engineering
- OSINT (Open Source Intelligence)
- Binary Exploitation

CTF vs. Cyber Security

Distinguishing between Capture The Flag challenges and real-world cyber security practices.

Networking Essentials

Fundamental concepts of network protocols, topologies, and common vulnerabilities.

Learning Resources & Platforms

Discovering tools, communities, and platforms for continuous learning and practice.

The CIA Triad: Foundation of Cybersecurity



Confidentiality

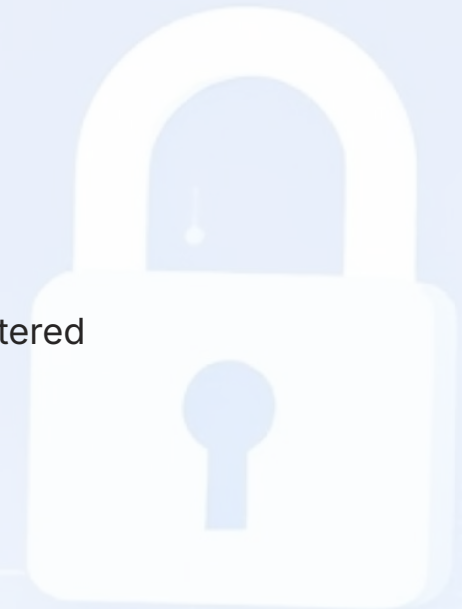
Protect information from unauthorized access

Integrity

Ensure data is accurate and unaltered

Availability

Keep systems and data accessible when needed



Ethical Hacking vs. Malicious Hacking

Ethical Hacking

- Authorized penetration testing
- Protects systems and data
- Legal and ethical responsibility
- Works with organizations
- Certified professionals (CEH, OSCP)

Malicious Hacking

- Unauthorized access
- Steals or damages data
- Illegal activities
- Criminal intent
- Causes financial and reputational harm

What is CTF? (Capture The Flag)

CTF is a cybersecurity competition where participants solve challenges to find hidden flags and earn points.

JEOPARDY-STYLE

Jeopardy-Style CTF

- Individual challenges in various categories
- Solve problems to earn points
- Categories: Web, Crypto, Forensics, Reverse Engineering, etc.
- Self-paced competition

ATTACK-DEFENSE

Attack-Defense CTF

- Teams defend their own systems
- Simultaneously attack opponent systems
- Real-time competition
- Dynamic and strategic gameplay

CTF & Cybersecurity: The Connection

Capture The Flag (CTF) competitions are more than just games; they are vital training grounds that directly enhance and validate cybersecurity skills for real-world application.



Practical Training Ground

CTF teaches real-world attack and defense techniques, fostering problem-solving and critical thinking essential for cybersecurity challenges.



Hands-on Skill Development

Participants gain invaluable experience with security tools and methodologies, building practical proficiency directly applicable to professional roles.



Career Advancement & Validation

CTF bridges the gap between theory and practice, offers industry-recognized skill validation, facilitates networking, and promotes continuous professional growth.

Cybersecurity Demand: Present Scenario & Future Outlook

Current Scenario: A Growing Imperative

Increasing Breaches

Rapid code deployment without adequate security checks leads to a daily increase in security incidents and vulnerabilities.

Security Over Speed

Organizations are shifting focus, prioritizing robust security measures and resilience over rapid feature deployment.

Multi-Million Dollar Costs

Data breaches continue to inflict substantial financial damages, regulatory fines, and long-term reputational harm to affected entities.

Talent Shortage

There's a critical global shortage of skilled cybersecurity professionals, leaving many organizations vulnerable and understaffed.

Sophisticated AI Attacks

The rise of AI-powered attack tools means threats are more adaptive, complex, and difficult to detect, challenging traditional defenses.

Role of AI in Cybersecurity: A Double-Edged Sword



AI for Defense

AI detects anomalies and threats faster, automates responses, and offers predictive security analytics to prevent attacks.



AI for Offense

Attackers also leverage AI to create more sophisticated phishing attempts, malware, and exploit new vulnerabilities, fueling an ongoing arms race.

Networking Essentials for Cybersecurity

A strong grasp of fundamental networking concepts is crucial for understanding and defending against cyber threats.



TCP/IP

The foundation of all modern internet communication, TCP/IP ensures reliable data transmission through its layered architecture.



DNS

Translates human-friendly domain names (like google.com) into numerical IP addresses, making web browsing possible. Vulnerable to spoofing attacks.



HTTP/HTTPS

HTTP transmits data unencrypted, while HTTPS secures web communication using SSL/TLS protocols, protecting sensitive information.



PORTS

Logical endpoints for network communication (e.g., 80 for web, 443 for secure web). Identifying open ports is a common reconnaissance technique.

What is Kali Linux?

Kali Linux is a specialized Debian-based Linux distribution pre-loaded with hundreds of open-source tools for penetration testing, ethical hacking, and cybersecurity research.

Key Features



Debian-based: Built on Debian Linux for stability and versatility.



Pre-installed Tools: Comes with essential security tools like Metasploit and Wireshark.



Customizable: Lightweight, flexible, and fully customizable to suit specific needs.



Open-Source: Free, open-source, and actively maintained by a global community.



Industry Standard: Widely adopted by security professionals and CTF competitors.

Common Use Cases



Penetration Testing: Conducting comprehensive penetration tests on systems and networks.



Vulnerability Assessments: Identifying and analyzing security weaknesses in applications and infrastructure.



Network Reconnaissance: Performing detailed network scanning and analysis to gather information.



Digital Forensics: Carrying out investigations to uncover digital evidence.



CTF Competitions: Participating in Capture The Flag events to test ethical hacking skills.






Important Note: Kali Linux is a powerful tool. It should only be used for authorized testing, educational purposes, or within legal frameworks. Unauthorized access to computer systems or networks is illegal and unethical.

Cryptography: Securing Data

Cryptography is the science of encoding information to protect it from unauthorized access. It's essential for data confidentiality and integrity, forming the backbone of secure digital communication and storage.

Types of Cryptography

Types of Cryptography		
<div> SYMMETRIC ENCRYPTION</div> <p>Uses the same secret key for both encryption and decryption, making it fast and efficient for large amounts of data. Examples: AES, DES</p>	<div> ASYMMETRIC ENCRYPTION</div> <p>Employs a pair of different keys (public and private) for encryption and decryption, enhancing security for key exchange and digital signatures. Examples: RSA, ECC</p>	<div> HASHING</div> <p>A one-way function that transforms data into a fixed-size string of characters (a hash or digital fingerprint), used for data integrity verification. Examples: MD5, SHA-256</p>

Key Concepts



Plaintext

The original, unencrypted data that is readable.



Key

A secret value or piece of information used by a cryptographic algorithm for encryption or decryption.



Ciphertext

The encrypted, unreadable form of data after cryptographic transformation.



Algorithm

A specific mathematical process or set of rules used to perform encryption or decryption.

Real-World Applications



Secure Messaging

Ensuring privacy and integrity for communication channels like email and instant messaging.



Password Storage

Storing user passwords securely, often using hashing functions, to prevent unauthorized access.



Online Transactions

Protecting financial data during online shopping and banking through protocols like TLS/SSL.



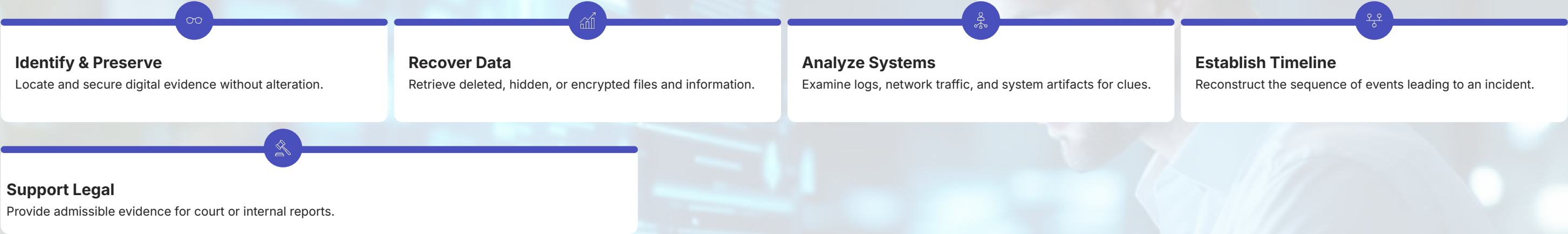
Digital Signatures

Verifying the authenticity and integrity of digital documents and software.

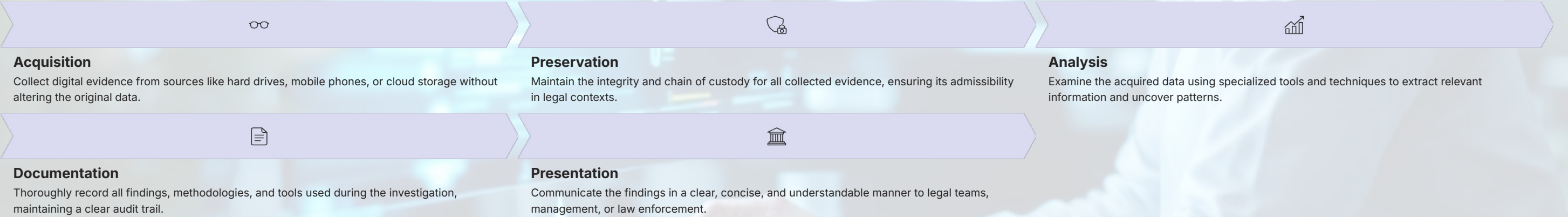
Digital Forensics: Investigating Cyber Crimes

Digital forensics is the systematic process of uncovering, preserving, and analyzing digital evidence from computers, networks, and storage devices. This crucial discipline helps reconstruct events, identify perpetrators, and support legal proceedings in the fight against cyber crimes and security incidents.

Key Objectives



The Forensic Process



Common Tools

- EnCase, FTK:** Comprehensive forensic suites.
- Wireshark:** Network protocol analyzer.
- Volatility:** Memory forensics framework.
- Autopsy:** Digital forensics platform for file system analysis.

Applications

- Criminal investigations (fraud, cyberterrorism).
- Incident response (malware, intrusions).
- Data breach investigations and root cause analysis.
- Compliance audits and regulatory adherence.

Web Hacking: Exploiting Web Vulnerabilities

Web hacking involves identifying and exploiting vulnerabilities in web applications and websites to gain unauthorized access, steal data, or disrupt services.

Common Web Vulnerabilities (OWASP Top 10)



SQL Injection

Inserting malicious SQL code into input fields.



Cross-Site Scripting (XSS)

Injecting malicious scripts into web pages.



Cross-Site Request Forgery (CSRF)

Forcing users to perform unwanted actions.



Broken Authentication

Weak password policies or session management.



Sensitive Data Exposure

Unencrypted or poorly protected data.



XML External Entities (XXE)

Exploiting XML parsers.



Security Misconfiguration

Improper server or application setup.



Insecure Deserialization

Exploiting object serialization flaws.



Using Components with Known Vulnerabilities

Outdated libraries.



Broken Access Control

Unauthorized access to resources.

Tools Used



Burp Suite

Web proxy and scanner.



OWASP ZAP

Security testing.



Postman

API testing.



SQLmap

SQL injection testing.

Real-World Impact

- Data breaches affecting millions
- Financial fraud and theft
- Website defacement
- Service disruption

Reverse Engineering: Understanding Software

Reverse engineering is the systematic process of analyzing software, often in its compiled or binary form, to understand its functionality, identify vulnerabilities, or extract proprietary information without access to the original source code.

Key Objectives

Functionality Insight

Gain a deep understanding of how software components operate.

Vulnerability Discovery

Uncover security flaws and weaknesses in applications.

Malware Analysis

Examine malicious code to comprehend its behavior and impact.

Source Code Recovery

Reconstruct lost or inaccessible source code from binaries.

Types of Reverse Engineering



Static Analysis

Examines code without execution, focusing on structure and logic.



Dynamic Analysis

Observes software behavior while it is running in a controlled environment.



Behavioral Analysis

Studies software interactions with the system, network, and other processes.

Tools & Applications

Common Tools



IDA Pro

Disassembler and debugger.



Ghidra

Open-source reverse engineering framework.



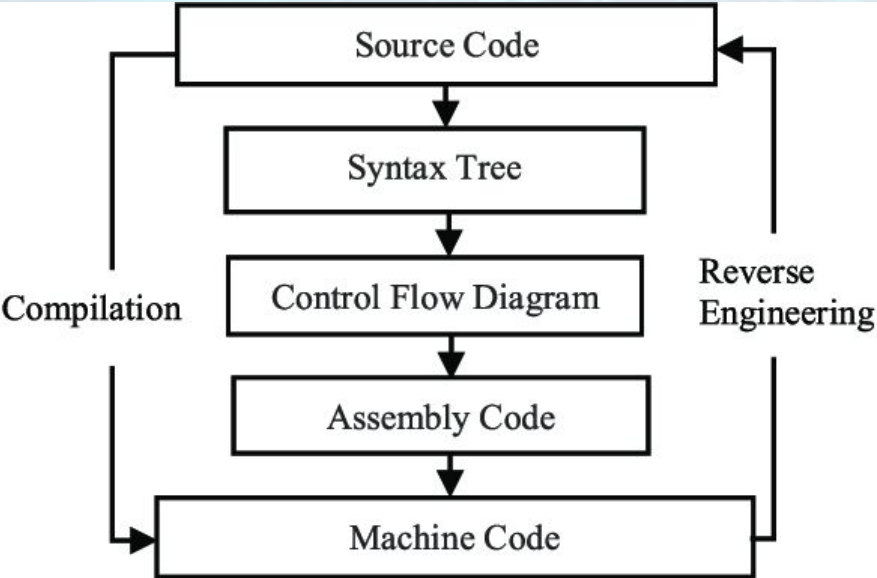
OllyDbg

Debugger for Windows executables.



Radare2

Command-line binary analysis framework.










OSINT: Open Source Intelligence Gathering

OSINT (Open Source Intelligence) is the systematic process of gathering and analyzing publicly available information from open sources to identify vulnerabilities, reconnaissance targets, or security threats. It's a critical component of cybersecurity, threat intelligence, and even business competitive analysis.




Key Techniques

01	02	03
Passive Reconnaissance Gathering information about a target without directly interacting with them, minimizing detection.	Domain Enumeration Discovering all associated subdomains and DNS records for a target domain to expand the attack surface.	Email Harvesting Collecting email addresses associated with an organization or individual, often used for phishing or social engineering.
04	05	
Social Engineering Using psychological manipulation to trick individuals into divulging confidential information.	Metadata Analysis Extracting hidden details from files, such as author, creation date, and software used, which can reveal sensitive information.	

Information Sources

 Search Engines Google, Bing, DuckDuckGo for general web searches.	 Social Media Platforms LinkedIn, Twitter, Facebook, Instagram for personal and professional connections, and public posts.	 Public Databases & Registries WHOIS, DNS records for domain ownership, and public record search tools.
 News & Public Records News articles, court documents, government filings, and archive sites.	 Code Repositories GitHub, GitLab for exposed code, credentials, or project details.	 Company Websites & Job Postings Revealing technologies used, internal structures, and employee names.
 IP Databases & Geolocation Shodan, Censys for internet-connected devices and geographic information.		

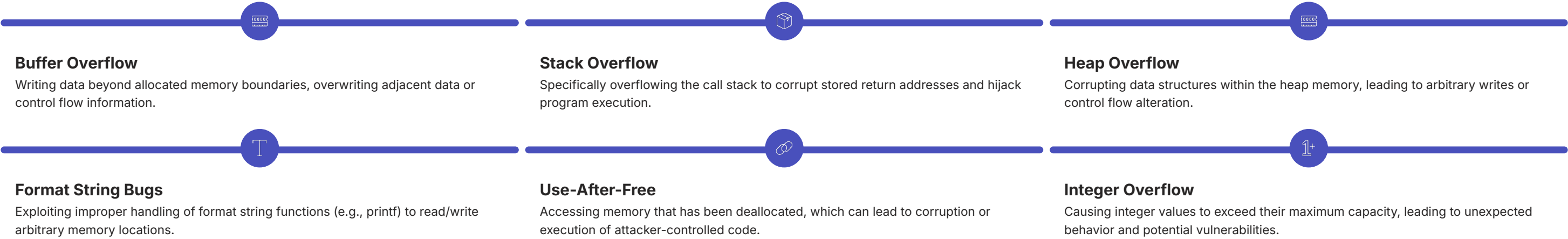
Common Tools

 Google Dorking Advanced search techniques to find specific information within websites.	 Whois Lookup Tools Retrieves registration information for domain names and IP addresses.	 Maltego Data mining and visualization tool for link analysis.
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------


Binary Exploitation (Pwn): Exploiting Software Vulnerabilities


Binary exploitation, often referred to as "Pwn," is the advanced practice of identifying and leveraging vulnerabilities within compiled software to achieve unauthorized control, execute arbitrary code, or circumvent existing security mechanisms. It involves a deep understanding of computer architecture, memory management, and low-level programming.


Common Vulnerability Types




Tools Used

- 

GDB (GNU Debugger)
Powerful debugger for low-level analysis.
- 

Radare2
Open-source reverse engineering framework and debugger.
- 

Pwntools
Python library designed to simplify exploit development.
- 

Ghidra
Software reverse engineering suite (disassembler, decompiler).

Applications

- CTF Challenges:** Core skill in capture-the-flag binary exploitation categories.
- Vulnerability Research:** Discovering new flaws in software products.
- Exploit Development:** Creating functional exploits for identified vulnerabilities.
- Security Assessment:** Evaluating software security posture through hands-on testing.

Guidelines for CTF & Cybersecurity Learning Platforms

Embarking on a journey into cybersecurity requires practical experience and continuous learning. These platforms and tips are designed to help you build and hone essential skills in Capture The Flag (CTF) challenges and general cybersecurity.

Recommended Platforms



TryHackMe (THM)

Beginner-friendly interactive labs with guided learning paths. Offers a wide range of cybersecurity topics, ideal for newcomers to quickly grasp core concepts.

tryhackme.com



CTFTime

The go-to resource for the global CTF community. Provides an event calendar, team rankings, comprehensive writeups, and other community-driven resources for all skill levels.

ctftime.org



HackTheBox (HTB)

Features realistic penetration testing scenarios and virtual labs. Caters to intermediate to advanced users with challenging machines and an active community.

hackthebox.com



PortSwigger Web Security Academy

Offers free, interactive training on web security vulnerabilities and exploitation techniques. Its industry-standard content is highly valuable for aspiring web penetration testers.

portswigger.net/web-security



PicoCTF

An educational CTF competition organized by Carnegie Mellon University. It's free, beginner-friendly, and excellent for learning foundational cybersecurity skills through challenges.

picoctf.org

Learning Tips for Success



Start with beginner challenges: Build a strong foundation before tackling more complex problems.



Read writeups and solutions: Learn from others' approaches and understand different methodologies even if you solved a challenge.



Join CTF teams and communities: Collaboration and shared knowledge accelerate learning. Online forums and Discord groups are great resources.



Practice regularly: Consistency is key to skill development in cybersecurity. Dedicate specific time slots for practice.



Document your learning journey: Keep notes on techniques, tools, and vulnerabilities encountered. This aids recall and reinforces understanding.



Participate in live CTF events: Apply your skills in a competitive environment, gain experience, and network with other enthusiasts.






Your Cybersecurity Journey Starts Here

The path to becoming a cybersecurity expert is dynamic and rewarding. You've gained a comprehensive overview of core principles, specialized domains, and practical learning resources.






What You've Learned

- Core Security Principles:** The Confidentiality, Integrity, and Availability (CIA) Triad forms the bedrock of information security.
- Ethical Hacking:** Understanding the crucial difference between ethical and malicious activities in the digital realm.
- CTF Competitions:** How Capture The Flag events are invaluable for hands-on skill development and testing.
- Networking Fundamentals:** The essential building blocks of how systems communicate and vulnerabilities arise.
- Specialized Domains:** A deep dive into areas like Kali Linux, Cryptography, Forensics, Web Hacking, Reverse Engineering, OSINT, and Binary Exploitation.
- Learning Platforms:** Key platforms and resources to continue your education and practical training.

Key Takeaways

-  **Cybersecurity is a critical and growing field**, offering endless opportunities for impact.
-  **Hands-on practice through CTF is essential** for translating theoretical knowledge into practical skills.
-  **Continuous learning is necessary** in an ever-evolving threat landscape.
-  **Ethical responsibility is paramount**; use your skills for good and protection.
-  **Community and collaboration accelerate growth**, so connect with peers and mentors.

Next Steps

-  **Choose a Learning Platform**
Dive into TryHackMe, HackTheBox, or PicoCTF to start your practical journey.
-  **Start with Beginner Challenges**
Build confidence and fundamental skills before tackling complex problems.
-  **Join a CTF Team**
Collaborate, share knowledge, and learn from others in a supportive environment.
-  **Build Your Portfolio**
Showcase your achievements, write-ups, and projects to demonstrate your expertise.
-  **Stay Updated**
Follow cybersecurity news, trends, and new vulnerabilities to remain at the forefront.