

CONTENTS ABOUT DIPLOMA IN CYBER SECURITY

1 Introduction to Ethical Hacking

- Definition of ethical hacking and its importance.
- Different types of hackers (white, black, grey hats) and cyber crimes.
- Ethical hacking phases and cyber kill chain.
- Rules and legal boundaries for ethical hackers.
- Tools used in ethical hacking.



2 Set-up Hacking Lab's

- Requirements for setting up a hacking lab.
- Virtualization software (vmware, virtualbox).
- Common operating systems for ethical hacking (kali linux, parrot os).
- Networking setup in a virtual environment.
- Common tools and packages to install.



3 Kali Linux & Red Hat

- Most important linux commands.
- Files and directory management.
- File sharing configuration.
- Linux system administration.
- Security and permission management.



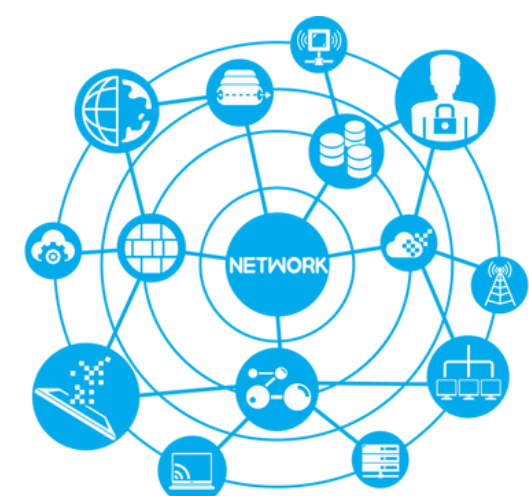
4 Information Gathering

- Identifying publicly available information.
- Whois lookups and domain information.
- Dns enumeration tools and techniques.
- Social media and osint (open source intelligence) tools.
- Google dorking for advanced search engine reconnaissance.



5 Networking & Scanning

- All about networking and types.
- Using nmap for network scanning.
- Network scanning different tools and techniques.
- Identifying open ports and services.
- Os detection and service version detection and bypassing firewall.



6 Cyber Laws

- Legal framework for cybercrime across various countries.
- Intellectual property laws and digital rights.
- Understanding data protection regulations punishments.
- The role of cybersecurity in corporate governance.
- Ethical hacker responsibilities under the it act 2000 and ipc law.



7 Social Engineering

- Types of social engineering attacks (phishing, baiting, pretexting, vishing).
- The psychology behind social engineering.
- Thinking like a hacker and their motivation.
- Real-world examples of successful social engineering attacks.
- How to train employees to spot and prevent social engineering attacks.



8 Anonymity

- Proxy servers and anonymity processes.
- Virtual private networks (vpns) for anonymity.
- The tor network and its role in anonymization.
- Mac address spoofing for identity masking.
- Use of anonymous browsers and encrypted communication.



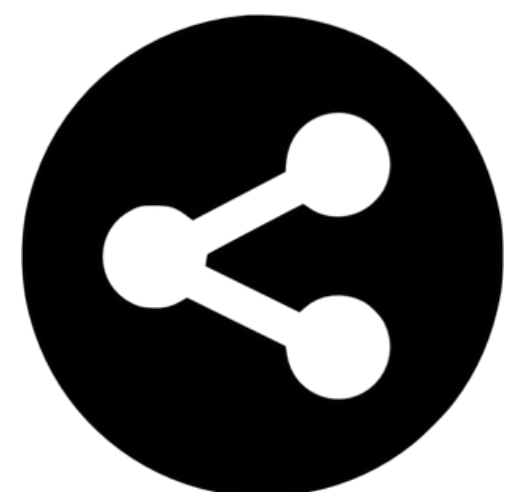
9 Spoofing & Sniffing Techniques

- What is sniffing, types, and its role in network attacks.
- Capturing data from same network, from other devices.
- Tools used for sniffing and spoofing ip, dns, mac address.
- How to sniff encrypted / unencrypted traffic.
- Location tracking with ip address & get ip address with phishing.



10 Secure Communication

- Techniques for secure file sharing.
- File encryption and its importance.
- Monitoring file-sharing activities on a network.
- Common file-sharing services used in hacking.



11 Vulnerability Analysis

- What is vulnerability analysis and its role in cybersecurity.
- Manual vs automated vulnerability scanning.
- Using common vulnerability databases.
- Tools used for vulnerability scanning.
- Exploit development and testing vulnerabilities.



12 Malware Threats & Analysis

- What is malware and types of malware.
- Methods of malware creating and delivery | creating automation program.
- Bind virus with image file , generate .Vbs , .Bat etc.
- Malware detection and removal.
- Preventive measures against malware.



13 Denial-of-Service Attack

- Types of dos attacks (syn flood, ping of death).
- Perform distributed denial-of-service (ddos) attacks.
- Tools used for launching dos attacks.
- Impact of dos attacks on networks and services.
- Detection and mitigation of dos attacks.



14 Firewalls, IDS & Honeypots

- Role of firewalls in network security.
- Types of firewalls (stateful, stateless).
- Intrusion detection systems (ids) vs intrusion prevention systems (ips).
- Types of ids (network-based, host-based).
- How honeypots are used to deceive attackers.



15 Hacking Wireless Network

- Types of wireless network encryption (wep, wpa, wpa2).
- Tools used for wireless network hacking (aircrack-ng, kismet).
- Deauth attacks and packet injection.
- Capturing wpa handshake for cracking.
- Rogue access points and evil twin attacks.



16 Windows System Hacking

- Common vulnerabilities in windows systems, generate spyware to hack windows .
- Creating malicious scrips to infect target system, privilege escalation in windows.
- Disable mouse , keyboard and monitor of victim system.
- Remotely access victim computer and hack web-camera using usb pendrive.
- Tools used for windows hacking (metasploite, gui rat).
- Bypassing user account control (uac) in windows.



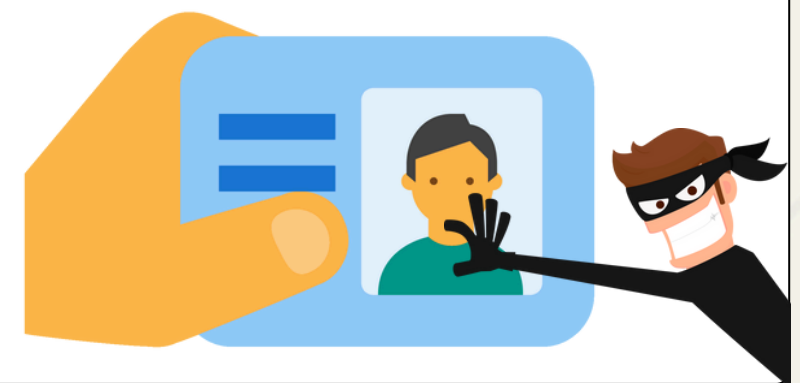
17 Android Hacking

- Exploiting vulnerabilities in android apps and os.
- Reverse engineering android apks , android-specific tools and rat malware.
- Get call details of target phone, listening call recording & crash all data.
- Access live front/back camera.
- Monitoring android live screen remotely.
- Social engineering attacks through malicious apps.



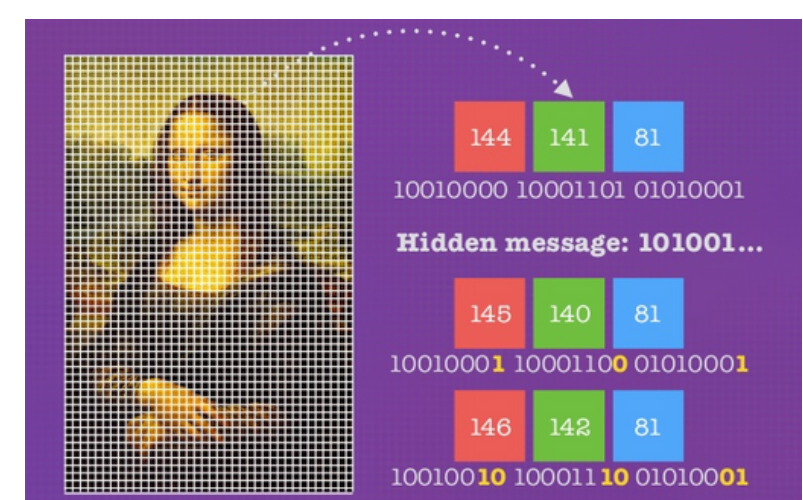
18 Legal Identity Theft

- Consequences of identity theft for victims.
- Laws governing identity theft (e.G., ID theft and assumption deterrence act).
- Tools for monitoring and protecting against identity theft.
- Creating fake account to trap the cyber criminal.
- Real-world case studies of identity theft.



19 Steganography

- Definition and methods of steganography.
- Types of steganography (image, audio, video).
- Tools used for steganography (openstego, steghide).
- How to detect steganography in digital media.
- Practical applications of steganography in cybersecurity.



20 Cryptography

- All about cryptography and symmetric vs asymmetric encryption.
- Hide your confidential data inside an image file.
- Hashing techniques (sha-256, md5).
- Use most secure encryption techniques to share the data.
- How encryption is used in data transmission.



Bonus: Full Black Hat Hacking Training

Certifications

Our Certificate Is Approved By Indian Government , ISO And UK Accreditation Forum



COURSE COMPLETION CERTIFICATE



HACKER ID CARD

ISO Certificate + Free Hacking Tools + 3 Months Cyber Security Internship Program

- Call Us / Whatsapp: [+916370634758](tel:+916370634758)
- E-mail: cyber@spyriotsecurity.in
agent.spyriot@gmail.com
- Instagram: [@spyriotsecurity](https://www.instagram.com/spyriotsecurity)
- YouTube: [Spyriotsecurity](https://www.youtube.com/Spyriotsecurity)
- LinkedIn: [spyriotsecurity](https://www.linkedin.com/company/spyriotsecurity)



UPI : [spyriot@ybl](https://upi.paytm.com/?id=spyriot@ybl)
Number: +91 6370634758



Founder of Spyriot Security:

Debadutta Chandan Dash

Visit Our Website
www.spyriotsecurity.in

