NIRMA UNIVERSITY
INSTITUTE OF TECHNOLOGY
NAAC ACCREDITED 'A' GRADE

ACES
ASSOCIATION OF COMPUTER ENGINEERING STUDENTS

Ethical Hacking Workshop

Organized by - ACES

- Pranav Gajjar

Who am I?

18BCE064@NIRMAUNI.AC.IN
Let's Connect over Linkedin:
https://www.linkedin.com/in/pranav-gajjar/

Final Year Student at Nirma University
Software Developer Intern at Searce Inc

Certified Ethical Hacker
Bug Bounty Hunter
Freelancer
Web Security Penetration Tester

Appreciation Letter by
University of Cambridge
Avans Hogeschool

Hall of Fame by
University of Victoria
United Nations
Resmed
University of Melbourne Australia

Workshop Outline

Introduction
Impact of various Cyber Attacks
Career Paths
Diversity
Types of Attacks
Vulnerabilities & Attacks
Steps of Hacking
How to Protect Yourself?
Phishing
Google Dork
Website Penetration Testing
Android Hacking
WiFi Hacking
FM Radio Hacking
Resources

Introduction

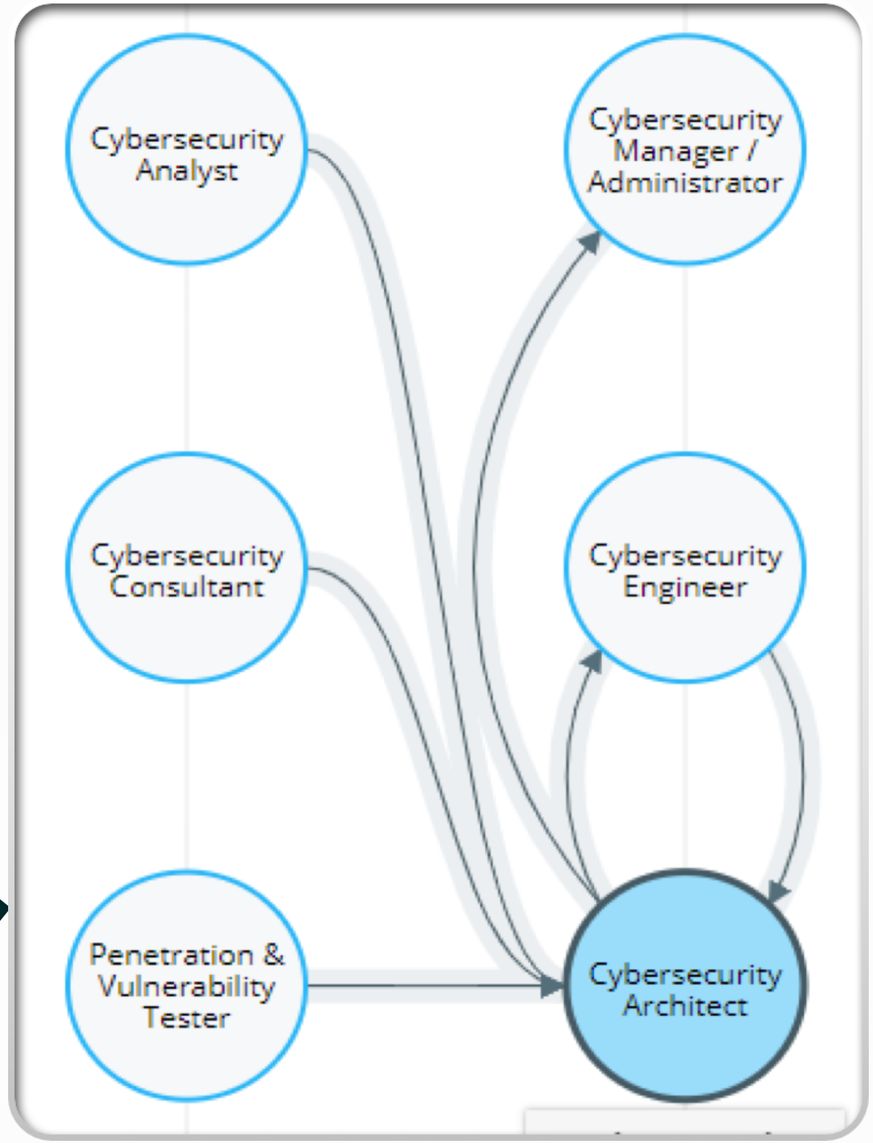
- Protection of computer systems and networks from information disclosure, theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide.
- An attempt of gaining access to someone else's device without authorization.
- Exploiting machine with malicious intention.
- Data leaks
- Phishing

Impact of various Cyber Attacks

- Governments worldwide saw a 1,885% increase in ransomware attacks, and the health care industry faced a 755% increase in those attacks in 2021, according to the 2022 Cyber Threat Report
  - SonicWall, an internet cybersecurity company

- Increase in Phishing Attacks
- Spam Email
- Fake Netflix MOD Application
- Pirated Software

Career Paths in Cyber Security



- Security branches off into many different pathways.
- These pathways can vary from security monitoring to ethical hacking.
- Penetration Tester
- Malware analysis
- Security Researcher

Diversity

Network Testing

IDS/IPS Firewall

Cryptography

Website Testing

Cloud Security

Real Life Attacks

Mobile App Testing

Malware Analysis

Hacking Devices

Types of Hacker

01 Black Hat Hacker

Unethical Hacker
hack the system illegally to achieve their own illegal goals.

02 White Hat Hacker

Ethical Hacker
hack the system that they have permission to hack

03 Grey Hat Hacker

A mixture of Black hat Hackers and White hat hackers
Hack any system even if they don't have permission but they will never damage

Vulnerabilities & Attacks

- Backdoor
- Denial of Service Attack (DOS)
- Eavesdropping
- Phishing
- Privilege Escalation
- Social Engineering
- Spoofing
- Malware, Virus & Worm

Steps of Hacking

Reconnaissance

collect information about the target from various sources like NewsPaper, Website, Email, Social Media Platforms.

Scanning

Use tools in order to find open ports, network layout, vulnerabilities, IP address, User Details.

Gaining Access

Execute attack or exploit vulnerabilities in order to Gain access of the target system.

Maintaining Access

Maintaining access for future purposes via installing backdoors and malware.

Clearing Tracks

Deleting Log files, temp files, command history etc in order to remove any track of attack.

How to Protect Yourself?

- Be aware on social media of fake accounts.
- Use complex Password.
- Enable 2-factor authentication.
- Make sure to check the URL of the Website and check for any spelling errors.
- Verify the source of contact.
- Don't open any link directly without knowing. (https://wheregoes.com/)
- Use Antivirus software
- Update software, services and various library to the latest and patched versions.
- Have different passwords for different accounts (Check for any leaked account credentials on https://haveibeenpwned.com/)

LIVE DEMONSTRATION OF ATTACKS

PRESENTATION

PHISHING

Phishing

- It is an attack that attempts to steal your money or personal identity by getting you to reveal personal information by pretending to be legitimate.
- Information like
  - Credit card numbers, bank information
  - Passwords, Addresses, Phone Numbers, Security Numbers, Government Documents, OTP can be fetched.
- SETOOLKIT - Tool to perform various social engineering and phishing attacks.

GOOGLE DORK

Google Dork

- Using advanced operators in the Google search engine to find a specific type of results.
- For example:
  - Finding Specific Vulnerable version of Web Application or server
  - Finding IP WebCam
  - Admin Login Portal
  - Finding Password Files
  - SQL Dumps

Google Dork

- Example:
- intitle:"Index of"
- intitle:"Index of" "sql"
- ext:sql
- ext:sql intext:password
- inurl:/view.shtml
- site:example.com
- Some Reference site for Google Dorks:
  - https://www.exploit-db.com/google-hacking-database
  - https://www.boxpiper.com/posts/google-dork-list

WEBSITE PENETRATION TESTING

OWASP Top 10 Vulnerabilities

- A1: Injection
- A2: Broken Authentication
- A3: Sensitive Data Exposure
- A4: XML External Entities (XEE)
- A5: Broken Access Control
- A6: Security Misconfiguration
- A7: Cross-Site Scripting
- A8: Insecure Deserialization
- A9: Using Components with Known Vulnerabilities
- A10: Insufficient Logging and Monitoring

Open Redirect Vulnerabiltiy

- Redirect the victim to any other malicious website via a legitimate domain.
- For example https://example.com/?redirect=evil.com
- Live Demo: https://web.stanford.edu/cgi-bin/redirect?dest=https://evil.com

PoC Video of Vulnerabilities

Example of following vulnerability on Live Website

- Cross-Site Scripting (XSS)
- CSV injection
- Price Manipulation

MALICIOUS APK ANDROID HACKING

Android hacking Via Malicious APK

- By installing malicious APK we can hack any android device very easily.
- Attacks that can be performed after infection:
- dump_sms
- dump_calllog
- send_sms
- geolocation, file upload, delete files,
- microphone, webcam, screenshot, live screen monitoring etc.

WIFI HACKING

WiFi Hacking

- Three types of WiFi Protocols: 1) WEP 2)WPA 3)WPA2
- Very Easy to hack WEP WiFi
- Need to brute force WPA/WPA2 WiFi Handshake
- Disconnect any nearby devices from the respective Access Point without any Password. (WiFi Jammer Tool)
- https://github.com/PranavGajjar0305/WifiJammer
- Can perform Social Engineering Attack (Ex: EvilTwin Attack) to gain Password of your WiFi.

FM RADIO HACKING

FM Radio Hacking

- FM Radio Frequency range from 88 to 108 MHz
- Transmit Radio waves on a specific radio frequency
- Hijack active Radio Station for a certain range.
- Create your own Radio station at any frequency.
- Raspberry Pi: Use to transmit signals.

RESOURCES

Resources

Udemy:

- https://www.udemy.com/course/learn-ethical-hacking-from-scratch/
- https://www.udemy.com/course/network-hacking-continued-intermediate-to-advanced/
- https://www.udemy.com/course/learn-python-and-ethical-hacking-from-scratch/
- https://www.udemy.com/course/learn-website-hacking-penetration-testing-from-scratch/

Youtube:

- HackerSploit
- Joseph Delgadillo
- Null Byte
- The Cyber Mentor

Contact:

Linkedin: https://www.linkedin.com/in/pranav-gajjar/

Gmail: 18bce064@nirmauni.ac.in

Youtube Channel: Cyber Web
(https://www.youtube.com/channel/UCpj4Tfy-De_uOwvx8mlkn6Q)

THANK YOU!