Hacking Intermediate Path

1. Ethical hacking starter

2. Physical Access Attacks

-OS Login Bypass • Introduction to Authentication Mechanisms • Tools to Defeat Authentication

3. Malware Introduction

Study

Watch

Practice

Create Virus -Create Trojans -Evade Antivirus & Firewalls -Scan System for Malicious Applications

Penetration Testing Introduction

-Penetration Testing Methodologies -Customers and Legal Agreements -Legal documents -Penetration Testing Planning and Scheduling -Pre Penetration Testing Checklist -Checklist for each security check -Scope Analysis -Penetration testing steps

4. Network Attacks

-Introduction to Network Attacks -Network Sniffing -Packet Sniffing - Wireshark -Packet Analysis -Display & Capture Filters -Network Attacks - Ettercap o DNS Poisoning o ARP Poisoning o Denial of Service

-Man in the Middle Attack o ARP Poisoning o SSL Stripping Router and Switch attacks o Brute Force Attacks o Device Exploitation o Framework reset

5. Wireless Network Attacks - WIFI

-Introduction to Wireless Technology -Hardware requirements -MAC Filtering -Packet Encryption -Packet Sniffing -Types of Authentication -Types of Attacks o ARP Replay Attack o Fake Authentication Attack o De-Authentication Attack Evil twin Wep cracking Wpa2 cracking -Security Countermeasures

https://github.com/0x90/wifi-arsenal

6. Network Vuln scan and hardening

-Introduction to Network Vulnerability Scanning -Vulnerability Assessment using Nessus -Scanning Policies -Vulnerability Assessment using Open VAS -Report Generation -Patch Critical Loopholes -System Hardening -Secure System Configuration

8. Explotation and delivery

-Reverse shell vs bind shell Staged vs nonstaged payload Finding exploits and using them

9. Metasploit Framework

-OS Detection -Open Port & Service Detection -Metasploit Framework Architecture -Various Interfaces of Metasploit Framework -Basic Terminologies -Vulnerability Analysis -Exploitation on Various Platforms -Evade Anti-Virus & Firewalls -Metasploit Scripting -Configure Nmap with Metasploit Framework -Ways to deliver Exploits -Covering your tracks

- Metasploit https://tryhackme.com/room/rpmetasploit

10. Post exploitation

-File transfer -Maintaining access -Privilege Escalation

- Linux Privesc https://tryhackme.com/room/linuxprivesc

-Pivoting -Cleaning up

-Checklists and cheatsheets -Penetration Testing Analysis -Penetration Testing Report

Study

Pentest methodology

Watch

Practice

Keeping notes during a pentest

Scoping a Pentest

12. Cloud Security

-Types of cloud -Security on the cloud -Cloud security tools

13. Getting ready for an entry-level cybersecurity job and moving on

-Blue, red and purple teaming Cyber security specialisations -Resume -Professional email -Certifications https://github.com/harisqazi1/Cybersecurity

-The interview process -Q&A

14. Recommendations and moving further

- Practice programming and scripting
- Play wargames
- Play beginner to advanced CTF
- Study ctf writeups
- Watch YouTube cybersecurity and CTF channels
- Follow Instagram feeds
- Join cybersecurity communities on platforms like discord

Dont be a skiddie

A skiddie or Script Kiddie is someone who uses prebuilt tools and scripts to attack a network or a website. The difference between skiddies and professional penetration testers is that the later use tools but they know the way their internals work. So, when an error shows up or a problem occurs, they know how to troubleshoot and fix the error to continue their attacks. Instead a skiddie would stop attacking or even not understand what happened during the penetration test.

The need of creative thinking

Hacking requires a different mindset than traditional IT troubleshooting and development roles. To become good at hacking, you would have to find your own way and think differently. Out of the box thinking can be a useful trait. You have to think how can the application or script be altered and make it work in a way it was not supposed to work. Learning these skills requires years of experience and patience.

Revision #1

Created Fri, Dec 18, 2020 4:01 PM by Ervelon

Updated Fri, Dec 18, 2020 4:10 PM by Ervelon