Network Security – Ethical Hacking

Course code: GOC3

This five-day advanced course introduces and explains common hacking technics commonly used on current wired as well as wireless intranets which interconnect systems based on Microsoft Windows operating system platform. At least half of the time that the students spend in the classroom is dedicated for hands-on practical exercises. Students practice attacks against the Active Directory, DNS and DHCP server, SMB/CIFS servers and clients, VPN connections, Wireless networks, SSL protected servers and others. Students will capture the user credentials and other traffic from wired (switched), wireless as well as WAN connections. We will explain in great detail the misuse of passwords and hashes and use encryption cracking technics such as brute-force, rainbow tables, dictionary attacks and distributed attacks using clusters and graphical cards. The goal of the training is to provide attendees with precise understanding of common vulnerabilities found in Windows based networks and teach how to prevent such attacks and harden the network. The course is taught by our top level security professional (MCT, MCSA, MCSE, MCITP, CEH) who specializes on security auditing, infrastructure security assessment and hardening.

Who is the course for

The course is designed for network administrators who are responsible for network security and who want to get practical experience of thinking and methodology used by attackers that is neccessary to understand in order to implement proper security countermeasures. This week of hacking training will the best insight into the attacker's mind and can offer a deep dive security experience that standard safety courses and official Whitepapers explain only in theory. The course can recommend and administrators of the network infrastructure for a deeper understanding of the principles of TCP / IP protocol. The TCP / IP quick intro and network data analysis make this training perfect for everyone with the knowledge and experience level course GOC2 or at least one year's experience with the administration of network services and operating systems. During the course, we use tools for Windows and their equivalents in the Linux environment, but thanks to the detailed explanations and instructions during the course there is no requirement of previous knowledge of linux systems.

What we teach you

Our unique course GOC3 Hacking in practice will allow you to understand the methods used during attacks against networks and server systems in great detail. During the course we explain everything you need to know to defend against techniques for mapping the challenged companies to scan the network environment, ARP poisioning, storage and transmission of password hashes over the network and methods to capture and break down the hashes using the CPU, GPU and distributed attack. Thi insight into the authentication protocols used over the network will give you a deep dive experience of NTLM and Kerberos authentication protocols. In the next part of the course we will discuss the details of rainbow tables structure and you will create your own tables. Because there are a lot of misundrestanding of weaknesses of wireless networks we will explain the different types of traffic in the WiFi network and you have the opportunity to practically test the WiFi network monitoring and traffic generation techniques using WiFi injection, disconnect the clients on the network traffic capture in monitor mode and breaking of passwords to WEP and WPA1 or WPA2 networks. In the final part of the course we will show also advanced attacks Man in the Middle, which is now used to eliminate HTTPS security and you will be attacking operating systems with wrong patch management using the exploitation techniques to attack computer systems without any previous knowledge of usernames or passwrods of physical access. We will cover also the techniques used by attackers to hide the components of backdoors on the compromised systems.

Required skills

OS - Windows 7, 8, Windows Server systems; TCP/IP

Course Outline

Introduction

- Repeating the TCP/IP stack
- Capturing data in a network analyzer
- Searching information from Internet sources
- How to start malware or manual attacks using services to start mission critical tasks

Analysis of the environment and the first attacks

- Analysis of the environment susceptible to social engineering
- Scanning network services by scanning for open ports and banners
- The enumeration of operating systems and services
- Explanation and attacking well chosen targets using the ARP poisioning using both Microsoft Windows and Linux operating systems
- Defensive countermeasures

Passwords and breaking

- Principles of storing passwords in operating systems
- Transferring passwords for network authentication
- Authentication methods downgrade
- The attacks on passwords using brute force CPU, graphics cards and distributed attack
- Rainbow Tables - principles of searching, a method of generating specific environments and types of attacks, the time / memory tradeoff effect

Wireless Networks

- Types of frames used in wireless networks
- Analysis of wireless networks in range
- Misuse of unauthorized frames
- Injection and monitor mode of WiFi cards
- Attacks on WEP networks
- Attacks on WPA1 PSK and WPA2 PSK network
- Breaking EAPOL frames using graphics cards
- Alien APs
- WPS

Advanced attacks

- Sending fake certificate, importing the fake root certificate authorities and the creation of fake certificates for breaking the HTTPS security
- Stripping the SSL protocols
- Exploitation of remote unknown systems

- Hiding your tools and backdoors using rootkits