Formation Ethical Hacking Professionnel

5 jours

I) Les Bases

Basic Services

1. DHCP
2. Static IP assignment
3. Apache
4. SSHD
5. Tftpd
6. VNC Server

Basic Bash

1. Environment
2. Simple Bash Scripting

Netcat

1. Connecting to a TCP/UDP port with Netcat
2. Listening on a TCP/UDP port with Netcat
3. Transferring files with Netcat
4. Remote Administration with Netcat
    - Scenario 1 – Bind Shell
    - Scenario 2 – Reverse Shell

Wireshark (Ethereal)

1. Peeking at a Sniffer
2. Capture filters
3. Following TCP Streams.

2) La prise d'empreinte

Open Web Information

1. Google Hacking
2. Advanced Google Operators
3. Searching within a Domain
4. Email Harvesting
5. Finding Vulnerable Servers using Google.

Miscellaneous Web ressources

1. Other search engines
2. Netcraft
3. Whois Reconnaissance

3) Open Services Information Gathering.

DNS Reconnaissance

1. Interacting with a DNS server
    - MX Queries
    - NS Queries
2. Automating lookups
3. Forward lookup bruteforce
4. Reverse lookup bruteforce
5. DNS Zone Transfers

SNMP reconnaissance

1. Enumerating Windows Users
2. Enumerating Running Services
3. Enumerating open TCP ports
4. Enumerating installed software

SMTP reconnaissance

Microsoft Netbios Information Gathering

- Null sessions
- Scanning for the Netbios Service
- Enumerating Usernames

4) Port Scanning

TCP Port Scanning Basics

UDP Port Scanning Basics

Scanning Pitfalls

Nmap

Scanning across the network

Unicornscan

5) ARP Spoofing

The Theory

Doing it the hard way

1. Victim Packet
2. Gateway Packet

Ettercap

1. DNS Spoofing
2. Fiddling with trafic

6) Buffer overflow Exploitation (Win32)

Looking for the Bugs

Fuzzing

Replicating the Crash

Controlling EIP

1. Binary Tree analysis
2. Sending a unique string

Locating Space for our Shellcode

Redirecting the execution flow

Finding a return address

1. Using OllyDbg

Getting our shell

Improving exploit stability

7) Working With Exploits

Looking for an exploit on BackTrack

1. RPC DCOM Example
2. Wingate Example

Looking for exploits on the web

1. Security Focus
2. Milw0rm.com

8) Transferring Files

The non interactive shell

Uploading Files

1. Using TFTP
    - TFTP Pros
    - TFTP Cons
2. Using FTP
3. Inline Transfer - Using echo and DEBUG.exe.

9)Exploit frameworks

Metasploit

1. Metasploit Command Line Interface (MSFCLI)
2. Metasploit Console (MSFCONSOLE)
3. Metasploit Web Interface (MSFWEB)
4. Interesting Payloads
    - Meterpreter Payload
    - PassiveX Payload
    - Binary Payloads
5. Framework v3.0
    - Framework 3 Auxiliary Modules
6. Framework v3.0
    - Kernel Payloads

10) Client Side Attacks

Client side attacks

MS04-028

MS06-001

Client side exploits in action

11) Port Fun

Port Redirection

SSL Encapsulation – Stunnel

HTTP CONNECT Tunneling

ProxyTunnel

SSH Tunneling

What about content inspection

12) Password Attacks

Online Password Attacks

Hydra

1. FTP Bruteforce
2. POP3 Bruteforce
3. SNMP Bruteforce
4. Microsoft VPN Bruteforce
5. Hydra GTK

Password profiling

1. WYD
2. Offline Password Attacks
3. Windows SAM
4. Windows Hash Dumping – PWDump / FGDump
5. John The Ripper
6. Rainbow Tables

Physical Access Attacks

1. Resetting Microsoft Windows
2. Resetting a password on a Domain Controller
3. Resetting Linux Systems
4. Resetting a Cisco Device

13) Web Application Attack vectors

SQL Injection

1. Identifying SQL Injection Vulnerabilities

2. Enumerating Table Names
3. Enumerating the column types
4. Fiddling with the Database
5. Microsoft SQL Stored Procedures
6. Code execution

Web Proxies

Command injection Attacks

14) Trojan Horses

Binary Trojan Horses

Open source Trojan horses

1. Spybot
2. Insider

World domination Trojan horses

1. Rxbot

15) Windows Oddities

Alternate NTFS data Streams

Registry Backdoors

16) Rootkits

Aphex Rootkit

HXDEF Rootkit