iSECUR1TY
INTEGRATED SECURITY SOLUTIONS
حلول امنية متكاملة

دورة اختبار الاختراق مع نظام Kali

مركز تدريبات
iSECUR1TY

Module 01 - Introduction:

1.1 - Why this course is different?

1.2 - What is penetration testing?

- 1.2.1 - Penetration testing VS. Vulnerability Assessment.

1.3 - Who is a penetration tester?

1.4 - Definitions.

1.5 - What do you need to know about hackers?

1.6 - Introduction to Kali Linux.

1.7 - Make your own penetration testing lab.

1.8 - Phases of penetration test.

- 1.8.1 - Penetration Testing Methodologies.

1.9 - Conclusion: What else should I know?

- 1.9.1 - Categories of Penetration Test.
- 1.9.2 - Types of Penetration Tests.
- 1.9.3 - Terms.

Module 02 - Essential Tools:

2.1 - Netcat.

2.2 - Wireshark.

2.3 - Tcpdump.

Module 03 - Pre-Engagement:

3.1 - Scoping.

3.2 - Milestones.

3.3 - Who should I call?

3.4 - I don't want to go to jail.

3.5 - The most important thing: The Payment :)

3.6 - Rules of engagement.

Module 04 - Intelligence Gathering:

4.1 - Introduction.

4.2 - Coping websites locally.

4.3 - Passive Reconnaissance:

- 4.3.1 - Practicing your Google-Fu.
- 4.3.2 - Email address harvesting.
- 4.3.3 - Whois.
- 4.3.4 - Netcat.

4.4. Active Reconnaissance:

- 4.4.1 - DNS Enumeration:
  - 4.4.1.1 - Host.
  - 4.4.1.2 - NSlookup.
  - 4.4.1.3 - DIG.
  - 4.4.1.4 - Fierce.

4.5 - Extracting Metadata.

4.6 - Wrapping Up.

4.7 - Port Scanning:

- 4.7.1 - Ping and Ping Sweeps.
- 4.7.2 - How TCP Works?
- 4.7.3 - TCP Scanning / SYN Scanning.
- 4.7.4 - UDP Scanning.
- 4.7.5 - How to perform Xmas Scan / Null Scan / Fin Scan?
- 4.7.6 - Nmap Scripting Engine (NSE).
- 4.7.7. Wrapping Up.

Module 05 - Threat Modeling:

5.1 - Introduction.

5.2 - What is Threat Modeling?

5.3 - Methodology of Threat Modeling?

Module 06 - Vulnerability Analysis:

6.1 - Introduction.

6.2 - Installing Nessus on Kali.

6.3 - Nessus:

- 6.3.1 - Nessus Policies.
- 6.3.2 - How to use Nessus?

Module 07 - Exploitation:

7.1 - Password Attacks:

7.1.1 - Brute Force Preparation.

7.1.2 - Local Password Cracking.

7.1.3 - Remote Password Cracking.

7.2 - Social Engineering:

7.2.1 - SET.

7.3 - Client Side Attacks:

7.3.1 - Browser Exploits.

7.3.2 - PDF Exploits.

7.3.3 - Java Exploits.

7.3.4 - Browser_Autopwn.

7.4 - Web-Based Exploitation:

7.4.1 - Introduction.

7.4.2 - Interrogating Web Servers.

7.4.3 - Spidering.

7.4.4 - Cross-Site-Scripting (XSS).

7.4.5 - SQL Injection.

7.4.6 - Zap OWASP Scanner.

7.5.7 - Automated SQL Injection Tools.

7.5 - Buffer Overflows:

7.5.1 - Introduction.

7.5.2 - Win32 Buffer Overflow.

7.6 - The Metasploit Framework:

7.6.1 - Metasploit User Interfaces.

7.6.2 - Auxiliary Modules.

7.6.3 - Exploit Modules.

7.6.4 - Metasploit Payloads:

7.6.4.1 - Staged vs. Non-Staged Payloads.

7.6.4.2 - Exploring Meterpreter Payload.

7.6.5 - Post Exploitation with Metasploit.

7.7 - Bypassing Antivirus.

Module 08 - Post-Exploiation:

8.1 - Introduction.

8.2 - Netcat: The Swiss Army Knife.

7.2.1 - Bind Shell.

7.2.2 - Reverse Shell.

8.3 - Local Privilege Escalation.

8.4 - Local Information Gathering.

Module 09 - Reporting:

9.1 - Introduction.

9.2 - Writing the penetration testing report.

9.3 - Examples.