PEN540

WIRELESS PENTESTING & NETWORK EXPLOITATION

PEN540 - Wireless Pentesting and Network Exploitation introduces students to all manner of reconnaissance, scanning, enumeration, exploitation and reporting for 802.11 networks.

The lab topics expose students to a variety of survey, database creation, scripting, and attack methods that can be used to gain a foothold in to a client's network during a penetration test.

TARGET AUDIENCE

Penetration testers looking to broaden their overall penetration testing skill set, wireless engineers, system administrators and developers

OBJECTIVE

Provide in-depth exposure to all facets of 802.11 penetration testing, encryption cracking, post-exploitation pillaging and report writing

CYBRScore™

DAY 1

Students will learn how to conduct wireless penetration tests using open source tools against 802.11 a/b/g/n networks. In addition, students will identify characteristics and common vulnerabilities associated with WiFi.

Topics List

- Scoping and Planning WiFi Penetration Tests
- 802.11 Protocols and Standards
- Authentication vs Association
- WiFi Security Solutions
- WiFi Hacking Hardware
- Connectors and Drivers
- Recon and Custom Password Generation with Cupp and CeWL

DAY 2

Students will learn to use open source tools and hardware to conduct both mobile and static 802.11 a/b/g/n surveys. Planning and executing surveys will be covered in depth as well as data management and database management techniques.

Topics List

- Conducting Surveys Using Airodump-ng and Kismet
- Creating SQL Databases of Survey Data
- Specialized SQL and AWK Commands to Manipulate Data for Reporting
- Cracking WEP
- Setting Up MAC Filters
- Bypassing MAC Filters

DAY 3

Students continue their use of Kismet and Airodump-ng to conduct mobile surveys, database the information and create .kml files in order to visualize survey data. Students are then exposed to an in-depth discussion on advanced encryption security processes followed by learning how to use open source tools to exploit the security process.

Topics List

- Planning and Conducting Mobile WiFi Survey
- GISKimset to Database Survey Information
- Creating Custom SQL Queries
- AWK Tool to Format Output from SQL Queries for Reporting
- GISKismet to Create .kml Files
- Stream and Block Ciphers, Block Cipher Modes
- WPA2 AES-CCMP Security Process
- Cowpatty to Recover WPA2 Passphrase
- Pyrit to Survey and Attack Encryption
- Databasing and Recovering WPA2 Passphrases

DAY 4

Building on the skills learned in the first three days, the students will learn how to conduct Man-in-the-Middle attack using easy-creds and a fake access point. Students will learn how to conduct various types of attacks, traffic capture, and credential harvesting once a victim connects.

Topics List

- Man-in-the-Middle Attack Theory
- Attacking Preferred Network Lists via Rogue AP
- Easy-Creds to set up Fake AP
- SSLStrip to Conduct Attack Against SSL Traffic
- URLSnarf to Capture Victim HTTP Traffic
- Ettercap to Poison ARP Cache on WiFi Network and Conduct Various Attacks Against Clients
- Custom Ettercap Filters
- Rusty Cobra Tool to Automate WiFi Survey
- Visualization, Database Management and Report File Creation

DAY 5

The last day of the course comprises a full-spectrum WiFi penetration test that the students must scope, plan and conduct. Final exercise serves to replicate a variety of network hardware, services and configurations, target website for recon, with multiple WiFi access points and clients using a variety of security mechanisms as provided.

Capstone Exercise

All the material covered in the course will be put to use in the final exercise.

PEN540

WIRELESS PENTESTING & NETWORK EXPLOITATION

CYBRScore™