Gaining Access

Nic Maurel

Active Scanning

- TCP Scanning
- Ftp bounce
- Idle Scanning
- UDP Scanning
- Version Scanning

- Nmap
- SuperScan
- Scanrand
- Amap

Wireless Attacks

- WEP, WPA & WPA2
- War driving
- Cracking encryption or Authentication Mechanisms
- Eavesdropping
- Ap Masquerading
- Mac Spoofing
- Netstumbler/Kismet
- AirSnort
- Mognet
- Aircrack
- SMAC
- Cowpatty

Physical Attacks – Low Tech

- Social Engineering
- Dumpster Diving
- Physical Break in &Theft
- Eavesdropping & Shoulder Surfing
- Observation

Brute Forcing

- Dictionary Attacks - Administrator
- Hybrid Attack - Adm1n1strator
- Brute Force Attack - Ms!tr245@F5a
- Rainbow Tables

- Lophtcrack, Cain and Abel & John the Ripper
- Obi Wan & Brutus
- Hydra
- Aircrack
- Cowpatty

Generic Vulerability Scanning

- www.packetstormsecurity.org
- www.cert.org
- www.securityfocus.com
- Source Code Scanners
- Application Level Scanners
- System Level Scanners
- Metasploit
- Nessus
- GFI Lan Guard

Web Attacks

- Version Vulnerability
- DNS Attacks
- File System Traversal
- Buffer overflow
- Source Disclosure
- Web-Based Password Attacks
- Cookies
- Url Obfuscation
- Cross-site scripting
- Intercepting Web Traffic
- Wikto & Paros
- Whisker & Nikto
- WebCracker & ObiWan
- CookieSpy
- URLSnarf

Database Attacks

- Sql Injection
- Information Disclosure
- Data Alteration
- Outside Access

- Ms-sql : 1433
- Mysql : 3306
- Postgresql : 5432
- Oracle : 1525
- Ibm-Db2 : 523
- SQLbf, SQLexec , SQLSmack & SQLrecon

Social Engineering (Hi Tech)

- Phishing & Pharming
- Spam
- ID Theft

Questions?

- insecure.org/nmap/download.html
- www.thc.org/thc-amap/
- www.netstumbler.com
- www.doxpara.com/paketto/
- www.kismetwireless.net/
- www.foundstone.com/us/resources/proddesc/superscan4.htm
- airsnort.shmoo.com/
- www.klcconsulting.net/smac/
- www.wirelessdefence.org/Contents/AircrackMain.htm
- www.node99.org/projects/mognet/
- www.oxid.it/cain.html
- www.openwall.com/john/
- www.thc.org/thc-hydra/
- www.hoobie.net/brutus/
- www.nessus.org/
- www.metasploit.com
- www.securityfocus.com/tools/727
- www.cirt.net/code/nikto.shtml
- www.sensepost.com/research/wikto/
- monkey.org/~dugsong/dsniff/
- www.parosproxy.org/
- www.wirelessdefence.org/Contents/coWPAttyMain.htm