SECGURU

Reconnaissance Cheat Sheet

Gathering information from Open Sources

□ Owner of IP-address range
□ Address Range
□ Domain Names
□ Computing Platforms
□ Network Architecture
□ User(name) Information
□ Physical Location
□ Active Services

□ Technical Contact
□ Business Partners
□ Administrative Contacts
□ Email Addresses
□ Technology being used
□ Phone No's
□ Route to target's
□ Internet Accessible data

□ Public Server's Banner Information.
□ DNS Servers
□ WEB Servers
□ SMTP Servers
□ Zones & Sub-domains
□ Locate Firewalls/Perimeter devices.

Techniques

▶ Target's Website

□ Mirror the web
□ Use Grep or Similar
□ Scan for keywords
□ Banner Information
□ Applications
□ Cgi's
□ Cookie style
□ Scripting language
□ Code-reading
□ Weblogs info [e.g. MRTG]

▶ Search Engines (Google)

□ intitle: "index of /etc"
□ inurl: "config.php.bak"
□ site:"target.com"
□ filetype:".bak"
□ Cross-Links
□ Search for group postings
□ News Articles

▶ Whois

▶ DNS

□ AXFR
□ Version
□ Zones & Sub-domains
□ Nmap -sL
□ DNSDig
□ Nslookup
□ Dig commands
□ Host commands
□ Active services

▶ Traceroute

□ ISP information
□ Locate Firewalls
□ Network Infrastructure
□ Tcptraceroute
□ Firewalk

▶ Finger

▶ SamSpade

▶ Netcraft

▶ SMTP

□ vrfy; email_enumeration
□ Banner information
□ Bounced Emails
□ Email Header
□ expn; email mapping

▶ Job Databases

□ Job requirements
□ Employee profile
□ Hardware information
□ Software information

▶ Personal Website

□ Employee job profile
□ Hardware information
□ Software information

▶ Ping

□ List of live systems
□ RTT, delays
□ N/W connectivity