UNIVERSITY of WASHINGTON

Hacking 310

Lesson 4: Invasive Reconnaissance

Review

Lesson 1 & 2 – Intro to Penetration Testing

- Penetration testing phases and types of tests
  - Intelligence gathering
  - Threat modeling
  - Vulnerability analysis
  - Exploitation
  - Post-exploitation
  - Reporting
- Ethical hacking – using your skills for good, rather than evil
- Legal aspects
- Vulnerability classes
- Setting up a lab

Review – Continued

Lesson 3

- Passive versus active
- Google hacking
- Whois / ICANN / IANA / BGP looking glass
- DNS enumeration via search
- Maltego

Objectives

- Discussion of the types of active foot-printing that exists.
- Conduct an external port scan with Netcat and NMAP.
- Perform banner grabbing, SNMP port sweeps, DNS zone transfer, and DNS discovery.

Active Techniques

- Ping sweeps
- Port scanning
- Banner grabbing
  - Version detection
  - Patch levels
- SNMP sweeps
- DNS Zone transfers
- SMTP bounce-back
- DNS discovery
- Forward/reverse DNS lookups
- DNS brute-force
- Web application discovery
- Virtual host detection & enumeration
- Account lockout threshold

Active Techniques – Internal

- Internal network ranges
- Identify internal infrastructure
  - Directory services
    - Active Directory, Novell, Sun, LDAP
  - Intranet sites
    - Wiki, SharePoint, Phone directories
  - Enterprise applications
    - ERP, CRM, Accounting
  - Sensitive network segments
    - Accounting, R&D, payments, building control systems
    - PCI requires segmentation
  - VoIP infrastructure
  - Authentication types
    - Kerberos, Cookies
  - Web proxy

Port Scanning

- What is it?
- Tools
  - NMAP – de facto standard
    - Capabilities
      - » Ping sweeps – identify hosts that are alive
      - » Port scans – identify ports that are open
      - » Service interrogation – identify the type, vendor and version of a service listening on a port
      - » OS detection – identify the operating system and version
      - » NSE scripts – additional scripts to do other fun things like enumeration
  - Unicorn Scan
    - Capabilities
      - » Similar options to NMAP
      - » Attempts to apply randomness to avoid detection by pattern based scanning detection controls
      - » No longer under active development
  - Masscan
    - Capabilities
      - » Scan entire internet in less than 6 minutes, sends 10 million packets/sec

NMAP - Common Scans

- Scan single IP
  - nmap 192.168.1.1
  - nmap scanme.nmap.org
- Scan range of Ips
  - nmap 192.168.1.0/24
  - nmap 192.168.1.1-100
- Detect operating system
  - nmap –A 192.168.1.1
- Output to file
  - nmap 192.168.1.1 –oA output-nmap-scan.txt

NMAP – Scan Types

- SYN Scan
  - -sS
- Connect Scan
  - -sT
- UDP Scan
  - -sU
- NULL, FIN, XMAS Scan
  - -sN, -sF, -sX
- Custom scans
  - --scan-flags

Netcat

- What is it?
  - Opens a connection/listens on an arbitrary port
  - Reads from STDIN
  - Outputs to STDOUT
- What does this mean?
  - Banner grabbing
  - File transfer
  - Flying shells
  - TCP scanning

Demo - Netcat, NMAP

SNMP Sweeps

- What is it?
  - SNMP – Simple Network Management Protocol
  - MIB – Management Information Base
  - Community strings
    - Shared secret
    - Read-only / read write
- Tools
  - onesixtyone
  - snmpwalk
  - snmp-check
  - NMAP NSE scripts
    - snmp-info
    - snmp-brute
    - snmp-interfaces
    - snmp-sysdescr
  - Metasploit
    - search snmp
    - use auxiliary/scanner/snmp/snmp_login

Demo - Metasploit

Challenge - Research

Research a method of DNS brute force and share the discovered method with the class in chat.

DNS Zone Transfer

- What is it?
- Tools
  - dig
    - dig axfr @dns-server domain.name
  - host
    - host –t axfr domain.name dns-server
- Example: zonetransfer.me
  - dig axfr @nsztm1.digi.ninja zonetransfer.me
  - host –t axfr zonetransfer.me @nsztm1.digi.ninja

Demo – DNS Zone Transfer

Web Application Enumeration

- Use the HTTP/HTTPS ports that were discovered through NMAP
- Tools
  - Manual browsing
  - Eyewitness