0day Security

[IN]SECURITY IN NETWORKS

Discovery & Probing

- Discovery & Probing. Enumeration can serve two distinct purposes in an assessment: OS Fingerprinting Remote applications being served. OS fingerprinting or TCP/IP stack fingerprinting is the process of determining the operating system being utilised on a remote host. This is carried out by analyzing packets received from the host in question. There are two distinct ways to OS fingerprint, actively (i.e. nmap) or passively (i.e. scanrand). Passive OS fingerprinting determines the remote OS utilising the packets received only and does not require any packets to be sent. Active OS fingerprinting is very noisy and requires packets to be sent to the remote host and waits for a reply, (or lack thereof). Disparate OS's respond differently to certain types of packet, (the response is governed by an RFC and any proprietary responses the vendor (notably Microsoft) has enabled within the system) and so custom packets may be sent. Remote applications being served on a host can be determined by an open port on that host. By port scanning it is then possible to build up a picture of what applications are running and tailor the test accordingly.
  - Default Port Lists
    - Windows
    - *nix
  - Enumeration tools and techniques - The vast majority can be used generically, however, certain bespoke application require there own specific toolsets to be used. Default passwords are platform and vendor specific
    - General Enumeration Tools
      - nmap
        - nmap -n -A -PN -p- -T Agressive -iL nmap.targetlist -oX nmap.syn.results.xml
        - nmap -sU -PN -v -O -p 1-30000 -T polite -iL nmap.targetlist > nmap.udp.results
        - nmap -sV -PN -v -p 21,22,23,25,53,80,443,161 -iL nmap.targets > nmap.version.results
        - nmap -A -sS -PN -n --script:all ip_address --reason
        - grep "appears to be up" nmap_saved_filename | awk -F\('{print $2}' | awk -F\) '{print $1}' > ip_list
      - netcat
        - nc -v -n IP_Address port
        - nc -v -w 2 -z IP_Address port_range/port_number
      - amap
        - amap -bqv 192.168.1.1 80
        - amap [-A|-B|-P|-W] [-1buSRHUdqv] [[-m] -o <file>] [-D <file>] [-t/-T sec] [-c cons] [-C retries] [-p proto] [-i <file>] [target port [port] ...]
      - xprobe2
        - xprobe2 192.168.1.1
      - sinfp
        - ./sinfp.pl -i -p
      - nbtscan
        - nbtscan [-v] [-d] [-e] [-l] [-t timeout] [-b bandwidth] [-r] [-q] [-s separator] [-m retransmits] (-f filename) | (<scan_range>)
      - hping
        - hping ip_address
      - scanrand
        - scanrand ip_address:all
      - unicornscan
        - unicornscan [options `b:B:d:De:EFhi:L:m:MtpP:q:r:R:s:St:T:w:W:vVZ:'] IP_ADDRESS/CIDR_NET_MASK: S-E
      - netenum
        - netenum network/netmask timeout
      - fping fping -a -d hostname/ (Network/Subnet_Mask)
    - Firewall Specific Tools
      - firewalk
        - firewalk -p [protocol] -d [destination_port] -s [source_port] [internal_IP] [gateway_IP]
      - ftester
        - host 1 ./ftestd -i eth0 -v host 2 ./ftest -f ftest.conf -v -d 0.01 then ./freport ftest.log ftestd.log
    -
  - Active Hosts
    - Open TCP Ports
    - Closed TCP Ports
    - Open UDP Ports
    - Closed UDP Ports
    - Service Probing
      - SMTP Mail Bouncing

- Banner Grabbing
  - Other
  - HTTP
    - Commands
      - JUNK / HTTP/1.0
      - HEAD / HTTP/9.3
      - OPTIONS / HTTP/1.0
      - HEAD / HTTP/1.0
    - Extensions
      - WebDAV
      - ASP.NET
      - Frontpage
      - OWA
      - IIS ISAPI
      - PHP
      - OpenSSL
  - HTTPS
    - Use stunnel to encapsulate traffic.
  - SMTP
  - POP3
  - FTP
    - If banner altered, attempt anon logon and execute: 'quote help' and 'syst' commands.
- ICMP Responses
  - Type 3 (Port Unreachable)
  - Type 8 (Echo Request)
  - Type 13 (Timestamp Request)
  - Type 15 (Information Request)
  - Type 17 (Subnet Address Mask Request)
  - Responses from broadcast address
- Source Port Scans
  - TCP/UDP 53 (DNS)
  - TCP 20 (FTP Data)
  - TCP 80 (HTTP)
  - TCP/UDP 88 (Kerberos)
- Firewall Assessment
  - Firewalk
  - TCP/UDP/ICMP responses
- OS Fingerprint