OS Fingerprinting

Catherine Javadian, Kaitlynn Prescott,
and Brianne Trollo

We pledge our honor that we have abided by the Stevens Honor System.

What is it?

- The process of learning what operating system is running on a particular device
  - Analyze certain protocol flags, options, and data in the packets a device sends onto the network
- OS has a fingerprint
  - Unique characteristics in its communication implementation that can identify it on a network
  - Signatures:
    - Time to Live (TTL)
    - Window Size
    - Don’t Fragment bit (DF)
    - Type of Service (TOS)

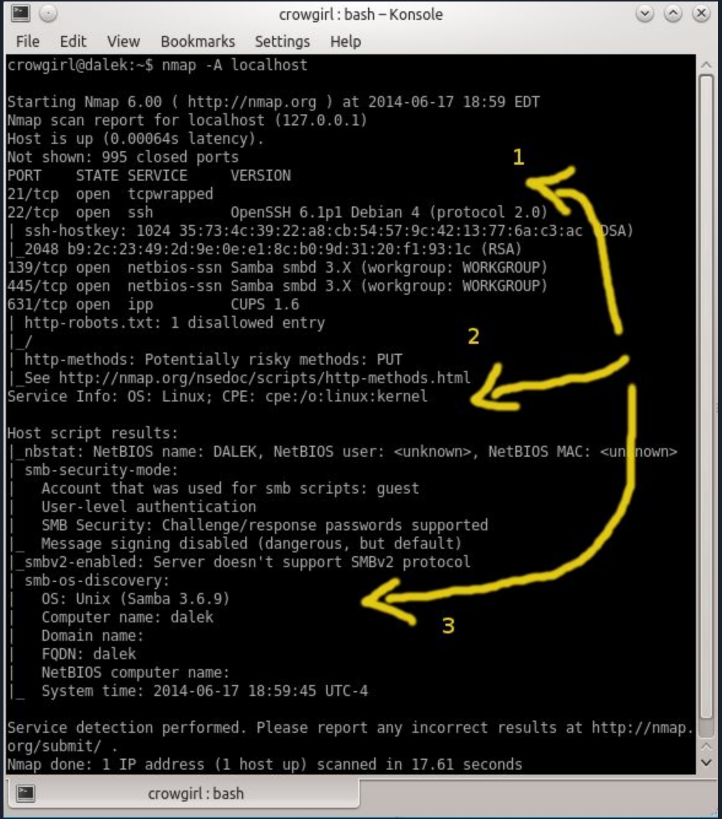
What is it used for?

- Hacking
  - Good reconnaissance
  - Importance of a device
- Network Maintenance
  - Notification of new device
  - Keep network inventory clean and up to date

Active Fingerprinting

- More likely to return information that will benefit an attacker
  - More accurate results a shorter amount of time
- Risk of being caught by an IDS, IPS, or a firewall
- Sending packets to target host
  - Analyzing the packets that are sent back
- Nmap
  - Monitor the security of networks
  - Firewalls are properly configured

Example



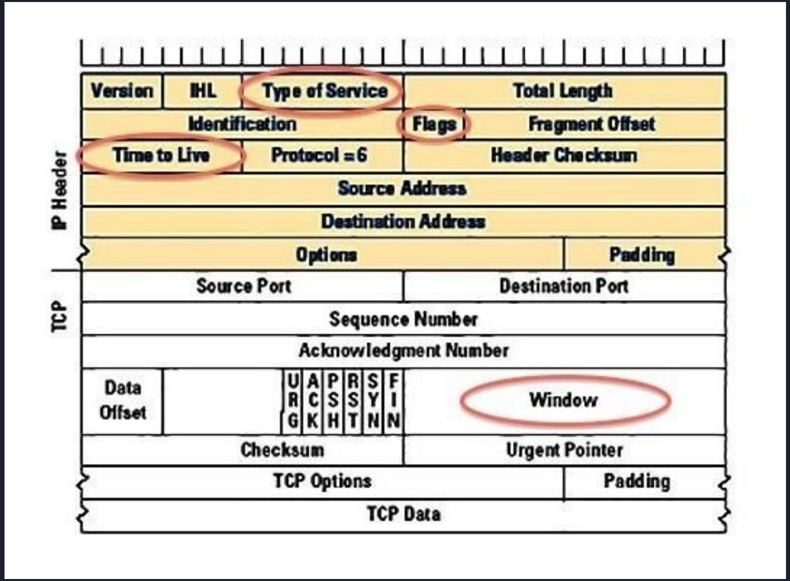
```
crowgirl@dalek:~$ nmap -A localhost

Starting Nmap 6.00 ( http://nmap.org ) at 2014-06-17 18:59 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00064s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE     VERSION
21/tcp  open  tcpwrapped
22/tcp  open  ssh         OpenSSH 6.1p1 Debian 4 (protocol 2.0)
| ssh-hostkey: 1024 35:73:4c:39:22:a8:cb:54:57:9c:42:13:77:6a:c3:ac (DSA)
|_2048 b9:2c:23:49:2d:9e:0e:e1:8c:b0:9d:31:20:f1:93:1c (RSA)
139/tcp open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
631/tcp open  ipp         CUPS 1.6
| http-robots.txt: 1 disallowed entry
|_/
| http-methods: Potentially risky methods: PUT
|_See http://nmap.org/nsedoc/scripts/http-methods.html
Service Info: OS: Linux; CPE: cpe:/o:linux:kernel

Host script results:
|_nbstat: NetBIOS name: DALEK, NetBIOS user: <unknown>, NetBIOS MAC: <unknown>
| smb-security-mode:
|   Account that was used for smb scripts: guest
|   User-level authentication
|   SMB Security: Challenge/response passwords supported
|_  Message signing disabled (dangerous, but default)
|_smbv2-enabled: Server doesn't support SMBv2 protocol
| smb-os-discovery:
|   OS: Unix (Samba 3.6.9)
|   Computer name: dalek
|   Domain name:
|   FQDN: dalek
|   NetBIOS computer name:
|_  System time: 2014-06-17 18:59:45 UTC-4

Service detection performed. Please report any incorrect results at http://nmap.
org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.61 seconds
```

- Debian version of OpenSSH is running from port 22
  - Ubuntu, Xubuntu, original Debian
- OS kernel - Linux
- Samba server 3.6.9 - Unix version
- Overall: Debian-based Linux distro
  - May not know specific Linux kernel version
  - Vulnerabilities that apply to all current Debian-based OSes

Passive Fingerprinting

- Less likely to return information that will benefit an attacker
  - Less accurate and less control over the data analyzed
- Almost undetectable
- Sniffs for TCP/IP ports
  - Analyzing the network traffic
- Packet capture API
  - Time to Live
  - TCP window size
- NetworkMiner and Satori
- No question to legality nature

Example



- Type of Service
  - Minimize Delay, Maximize Throughput, Maximize Reliability, Minimize Monetary Cost
- Flags
  - SYN, RST, ACK, etc
  - Whether the packet has been fragmented
- Time to Live (TTL)
  - Maximum number of hops that packet can traverse before it times out
    - Windows - 32
    - Linux - 64
- Windows Field
  - Size of the buffer of sending system
    - 70-80% chance of determining OS

Scanners

- Nmap - Active scanner, most popular network scanner in use today
  - Rapidly scans large segments of a network for active devices
  - OS detection can only be performed after a port scan has been completed
- Xprobe2 - ICMP scanner, one of the quietest active scanners
  - Matrix based fingerprint matching
  - Fast results, little packet traffic
  - Very difficult to detect
- P0f - Passive OS detection, useful when stealth needed
  - Reads and analyzes packets without generating its own traffic
  - Four modes: SYN, SYN-ACK, RST, and stray ACK

How to prevent successful fingerprinting?

- This is only necessary when malicious reconnaissance is a concern
- Need to protect the edge of the network, or detect if someone is already on your network
- Preventing OS fingerprinting may not be 100% possible
- Make sure external hosts cannot scan internal hosts
- Change TCP/IP settings
  - This changes how network traffic appears and has an impact on networks performance
- Best advice: Perform scans against your own network, and document your findings
  - This will allow you to see what changes need to be made to your system.

Works Cited

Allen, Jon Mark. “OS and Application Fingerprinting Techniques.” SANS Institute InfoSec Reading Room, 22 Sept. 2007.

Gibb, Taylor. “OS Fingerprinting With TTL and TCP Window Sizes.” How-To Geek, How-To Geek LLC, 1 Feb. 2012, www.howtogeek.com/104337/hacker-geek-os-fingerprinting-with-ttl-and-tcp-window-sizes/.

“IP (DF) 'Don't Fragment Bit' Echoing Probe.” Common Attack Pattern Enumeration and Classification, MITRE, 4 Aug. 2017, capec.mitre.org/data/definitions/319.html.

Spitzner, Lance. “Passive Fingerprinting.” Symantec Connect, Symantec Corporation, 2 May 2000, www.symantec.com/connect/articles/passive-fingerprinting.

“What You Must Know About OS Fingerprinting.” InfoSec Resources, InfoSec Institute, 11 Mar. 2015, resources.infosecinstitute.com/must-know-os-fingerprinting/.