

REMOTE PHYSICAL DEVICE FINGERPRINTING

Tadayoshi Kohno, Andre Broido, kc claffy

Presented by : Anuj Sawani

Hacking – done the right way!

2

- Nmap featured in *The Matrix Reloaded*



```
1 /tcn nnen hosts2-nc [mobile]
2
3 Starting nmap V. 2.54BETA25
4 Insufficient responses for TCP sequencing (3), OS detection may be less
5 accurate
6 Interesting ports on 10.2.2.2:
7 (The 1539 ports scanned but not shown below are in state: closed)
8 Port      State      Service
9 22/tcp    open      ssh
10
11 No exact OS matches for host
12
13 Nmap run completed -- 1 IP address (1 host up) scanned
14 # sshnuke 10.2.2.2 -rootpw='210N0101'
15 Connecting to 10.2.2.2:ssh ... successful.
16 Attempting to exploit SSHv1 CRC32 ... successful.
17 Resetting root password to '210N0101'.
18 System open: Access Level (9)
19 # ssh 10.2.2.2 -l root
20 root@10.2.2.2's password:
21
22 PRE-CONTROL> disable grid nodes 21 - 48
```

Fingerprinting

3

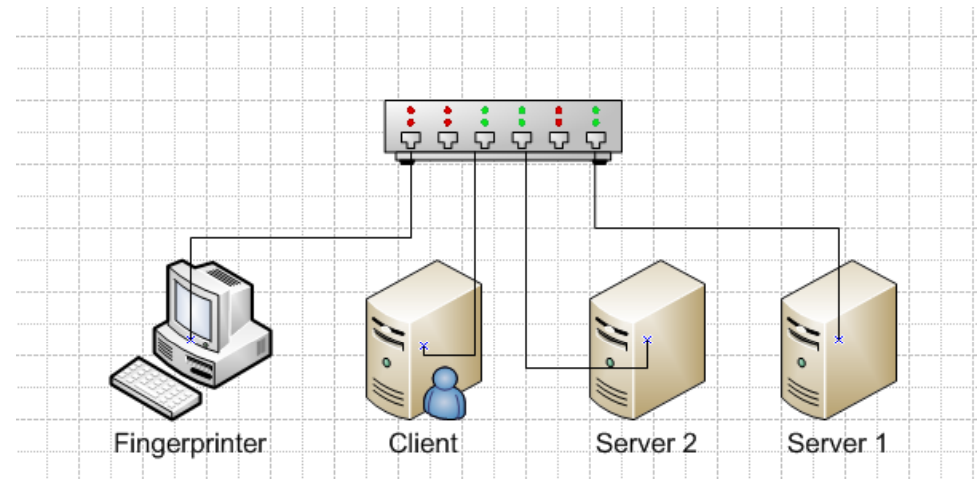
- What can we fingerprint?
 - ▣ Operating systems
 - ▣ A class of devices
 - ▣ A physical device
- The signals to exploit?
- What can we do with a fingerprint?
 - ▣ Check if a vulnerability exists
 - ▣ Tailor exploits
 - ▣ Forensics



Classes of fingerprinting techniques

4

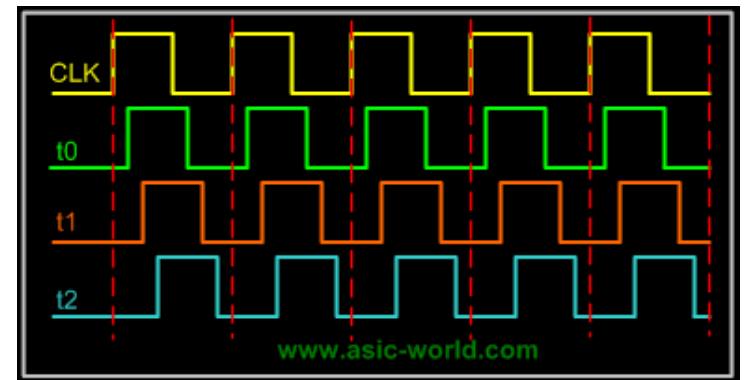
- Passive
- Active
- Semi-passive
- Active vs Passive?



Clock Skew

5

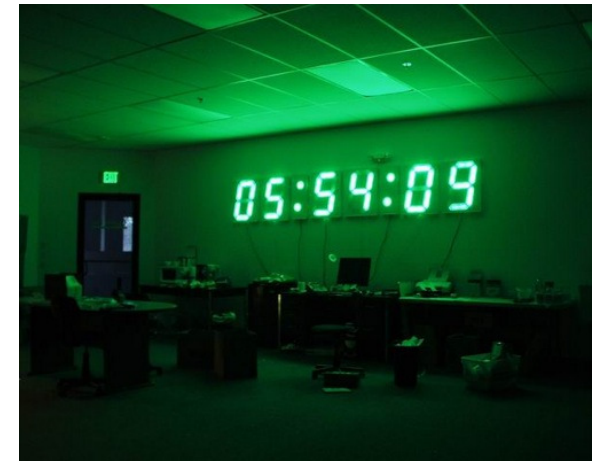
- Time inaccuracies in a clock
 - Causes?
- The clocks
 - System clock
 - Not frequently synchronized
 - TCP timestamp option(TSopt) clock
 - Virtual clock
- How can we use the skew?
 - System's perception of the time compared with true time



Exploiting clock skew

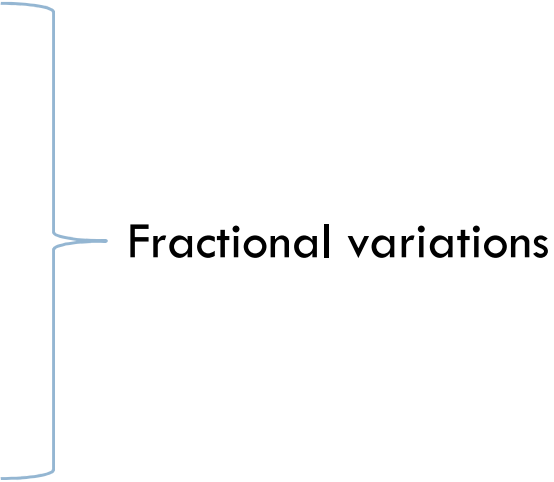
6

- System clock skew
 - ▣ ICMP Timestamp requests
 - Will not work behind NAT/firewall
 - ▣ Any other protocol revealing sys clock
- TCP clock skew
 - ▣ Passive
 - Observe tcp packets
 - ▣ Semi-passive/active
 - Prolong period of communication
 - ▣ Windows 2000/XP – timestamps disabled
 - The trick?



Factors affecting skew

7

- Access medium
 - Topology
 - Distance
 - Operating system
 - NTP
 - ▣ Does not affect T_{Sopt}
 - Power Source
 - ▣ Battery/AC power
- 
- Fractional variations

What can we use this for?

8

- Detect virtual machines on a network
 - ▣ No variability in the skew
- Counting devices behind NAT
 - ▣ Partition traces using TCP timestamp sequences
- Forensics
 - ▣ Not completely unique
- Unanonymizing Anonymized traces

Countermeasures

9

- Eliminate clock skews
 - ▣ Frequent NTP synchronization
 - ▣ Reduce hardware defects
- Introduce randomized clock skews
- Any other counter-measures?



Discussions

10

- Can clock skew serve as an unique identifier?
- Range of skew values?
 - ▣ Scalability?
- Time taken to fingerprint

Take Away

11

A piece of junk might be a fortune waiting
to be discovered

