Chapter 21
Fingerprinting

- **Module Network Reconnaissance: Curiosity killed the Cat**

"Fingerprint identification occurs when an expert determines that two impressions originated from the same finger or palm."

(Wikipedia.org)

Copyright Information

- Some rights reserved / Einige Rechte vorbehalten
- Michael Kafka, René Pfeiffer, Sebastian Meier
  C.a.T. Consulting and Trainings, Vienna, Austria
- You may freely use, distribute and modify this work under following agreement:
- Diese Arbeit darf frei genutzt, verbreitet und bearbeitet werden unter folgenden Bedingungen:

Authors must be referenced (also for modification)
Autoren müssen genannt werden (auch bei Bearbeitung)

Only for non commercial use
Nur für nichtkommerzielle Nutzung

Derivative work under same licence
Derivative Arbeit unter selber Lizenz

creative commons http://www.creativecommons.com

DeepSec Vienna 2007
7 Layers of Insecurity

Chapter 21
Fingerprinting

- Agenda
  - Fingerprinting Basics
  - Passive Fingerprinting
  - Protocol Headers
  - Active Fingerprinting
  - Identify Individuals

Fingerprinting Basics

- How to Find Valuable Hints?
  What to look for, what to ignore?
  What is it good for?

Fingerprinting Basics

- Systems may have unique signatures
  - Network stack responses
  - DCE RPC signatures
- Versions and protocols are crucial
  - for matching against weaknesses
  - for capability assessment
- Tools exist for automating scans
- Fingerprinting may be active or passive

Fingerprinting Basics
Why find out Details?

- Versions unveil state of maintenance
  - Look for “forgotten systems”
  - Identify “abandoned applications”
- Gather information for attack approach
- Determine dependencies
  - Important for indirect attacks
  - Proper chaining of exploits

Fingerprinting Information

- Collect everything
  - Scan and get all you can get
  - Useful to get the “big picture”
- Information can be used in social engineering
  - Facts improve credibility
  - Phone calls can confirm/reject results

Passive Fingerprinting

- **Just Watch or Listen!**

“Stop, look, listen”

“The Stylistics”
(1971)

p0f

- Passive method
- Identifies
  - systems that connect to you (SYN)
  - systems you connect to (SYN+ACK)
  - systems you cannot connect to (RST)
- Additionally detects network devices
  - NAT
  - load balancers

Protocol Headers

- **A Wealth of “Hidden” Information.**

Protocol Header Information

- Network distances
  - Round trip time, TTL
  - Analyse hop count, intermediate devices
- Hops that change information
  - Missing IP options, normalisation
  - NAT devices
- Risk: medium Impact: medium

Active Fingerprinting

- “Shout, shout, let it all out. …”

Banner Grabbing

- Layer 2 is full of announcements
- Layer 7 is full of banners
- Most Internet protocols are based on text
- Attackers look for
  - version strings
  - capabilities
  - host / domain names

Popular banners

- CDP/LLDP strings
- FTP servers
- SMTP dialogues
- SNMP communities
- HTTP responses
- SSH version information
- IMAP/POP3 servers
- DNS (with suitable tools)
- Risk: high Impact: medium

DNS Digging

- DNS zones are very important
- Public records disclose starting points
  - Avoid secret.fileserver.example.net
  - Attackers will use dictionaries
- Attackers will try to
  - zone transfer all data
  - identify DNS infrastructure
- Monitoring DNS queries can reveal attacks
- Risk: medium Impact: high

Firewalking

- Mapping packet filters by response
- Attackers investigate
  - IP TTL
  - ICMP responses
  - IP/TCP options
  - responses to invalid packets
- Name stems from tool “firewalk”
- Risk: medium Impact: medium

SNMP Walking

- SNMP offers rich informations
- Many network devices are SNMP-capable
- Attackers look for unprotected access
  - Port scanners on port 161/162 (UDP/TCP)
- Default information very useful
- Risk: medium Impact: high

Tools for Reconnaissance

- What to Use?

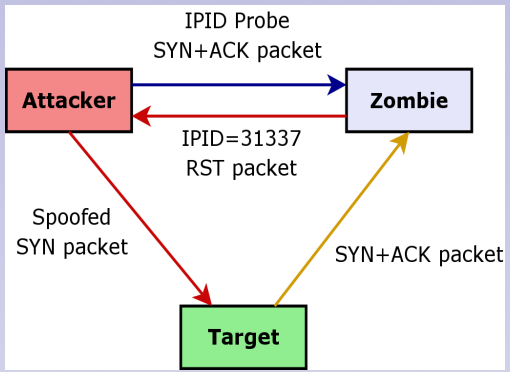
Tools of the trade

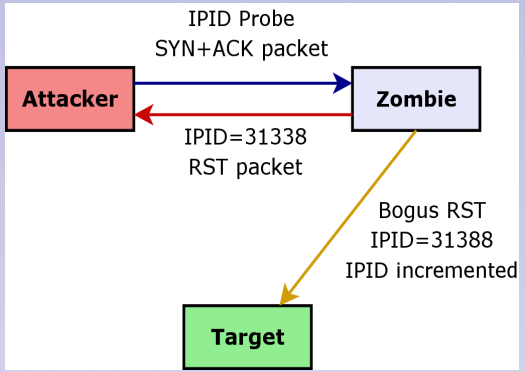
- Times change, tools adapt
  - telnet, ping, traceroute
  - telnet, hping2, tcptraceroute
- Any packet generator will do
- Any tool capable of TCP will do likewise
  - telnet is still common

nmap

- nmap is around since 1997
  - Host discovery
  - OS detection
  - Port scanning
  - Support for scripting
- nmap offers parallel scanning
- TCP, UDP, ICMP capability
- Protocol scan
- Idle scan
- Banner grabbing (version strings)

Idle Scan


IPID Probe
SYN+ACK packet
Attacker
Zombie
IPID=31337
RST packet
Spoofed
SYN packet
SYN+ACK packet
Target


IPID Probe
SYN+ACK packet
Attacker
Zombie
IPID=31338
RST packet
Bogus RST
IPID=31388
IPID incremented
Target

xprobe2

- Active scanning tool, around since 2001
- Early focus on ICMP footprints
- Key features include fuzzy fingerprinting
- Multiple signatures used
  - TCP, UDP, ICMP
  - SNMP V2
  - SMB

hping2/hping3

- “ping on steroids”
  - Sends crafted UDP, ICMP, TCP packets
  - Collects TCP ISN, pioneered Idle Scan
  - Has API for automated tests
- Useful for firewall/IDS/IPS testing
- More capable than standard tools

Large networks

- Attackers map large networks
  - Automated scans for popular ports
  - “Auto-r00ter” attached
- Parallel scans may appear on monitoring
- Large scans reduce number of ports
  - Bulk scanners look for specifics

Port Scanning Risks

- Risk: medium Impact: medium
- Mitigation
  - Drop malformed/useless/unwanted packets
  - Detect port sweeps, packet rates
  - Limit ICMP error rate
  - Reassemble fragments at border

Identify Individuals

- **Matching Addresses to People.**

Personal Information

- Look out for anything like
  - E-mail addresses
  - Telephone numbers, FAX numbers
  - “Personalised” network addresses
  - Personal namespaces (in DNS)
- Personal information improves credibility
  - Important for social engineering
  - Useful for faking other information
- Risk: medium Impact: high

Chapter 21
Fingerprinting

- Summary
  - Reconnaissance is about information.
  - Any protocol is affected.
  - Carefully design access to network(s).
  - Monitor incoming traffic.
  - Limit access wherever you can.
  - Know where your data is and what to do with it.

Thank you for your attention!

- Questions?

DeepSec Vienna 2007
7 Layers of Insecurity

Chapter 21
Fingerprinting

- **Module Network Reconnaissance: Curiosity killed the Cat**

"Fingerprint identification occurs when an expert determines that two impressions originated from the same finger or palm."

(Wikipedia.org)

DeepSec Vienna 2007
7 Layers of Insecurity

Fingerprinting is a reconnaissance technique which allows to identify systems, versions of operating systems, patch levels, services packs etc. by observing a target for individual responses or actions.

This chapter presents the latest developments in different techniques and discusses methods how risks can be mitigated.

Copyright Information

Chapter 21
Fingerprinting

- Agenda
  - Fingerprinting Basics
  - Passive Fingerprinting
  - Protocol Headers
  - Active Fingerprinting
  - Identify Individuals

DeepSec Vienna 2007
7 Layers of Insecurity

Fingerprinting Basics

- How to Find Valuable Hints?
  What to look for, what to ignore?
  What is it good for?

DeepSec Vienna 2007
7 Layers of Insecurity

Fingerprinting Basics

- Systems may have unique signatures
  - Network stack responses
  - DCE RPC signatures
- Versions and protocols are crucial
  - for matching against weaknesses
  - for capability assessment
- Tools exist for automating scans
- Fingerprinting may be active or passive

DeepSec Vienna 2007
7 Layers of Insecurity

Fingerprinting Basics
Why find out Details?

- Versions unveil state of maintenance
  - Look for “forgotten systems”
  - Identify “abandoned applications”
- Gather information for attack approach
- Determine dependencies
  - Important for indirect attacks
  - Proper chaining of exploits

DeepSec Vienna 2007
7 Layers of Insecurity

Fingerprinting Information

- Collect everything
  - Scan and get all you can get
  - Useful to get the “big picture”
- Information can be used in social engineering
  - Facts improve credibility
  - Phone calls can confirm/reject results

DeepSec Vienna 2007
7 Layers of Insecurity

Passive Fingerprinting

- Just Watch or Listen!

"Stop, look, listen"

"The Stylistics"
(1971)

p0f

- Passive method
- Identifies
  - systems that connect to you (SYN)
  - systems you connect to (SYN+ACK)
  - systems you cannot connect to (RST)
- Additionally detects network devices
  - NAT
  - load balancers

DeepSec Vienna 2007
7 Layers of Insecurity

p0f is a passive fingerprinting sensor. It works by analysing the behaviour of the TCP/IP interaction (TCP handshake, options, MTU, MSS, parameters, patterns). It can detect firewalls, NAT devices, Internet connections and the like). p0f only needs to have access to the network packets. It can also work on recorded or mirrored packets.

Protocol Headers

- A Wealth of “Hidden” Information.

Protocol Header Information

- Network distances
  - Round trip time, TTL
  - Analyse hop count, intermediate devices
- Hops that change information
  - Missing IP options, normalisation
  - NAT devices
- Risk: medium Impact: medium

The hop count and the round trip time often give interesting information. Tracing the packet routes either with a *tcptrace*-like tool or the IP option *record route* let's you determine the AS number, the ISP and maybe load balancing devices as well as changing routes.

There are methods of detecting NAT devices and estimating the host behind them.

• Detecting NAT Devices using sFlow by Peter Phaal

• A Technique for Counting NATted Hosts by Steve Bellovin, AT&T

Proper packet inspection and normalisation can avoid these techniques. The Linux kernel, OpenBSD and recent FreeBSD systems apply countermeasures against the proposal by Steve Bellovin.

Mitigation:

• Deploy packet filters that “scrub” packets (OpenBSD has this option for example)

• Use layer 4/7 proxies

Active Fingerprinting

- “Shout, shout, let it all out. …”

Banner Grabbing

- Layer 2 is full of announcements
- Layer 7 is full of banners
- Most Internet protocols are based on text
- Attackers look for
  - version strings
  - capabilities
  - host / domain names

DeepSec Vienna 2007
7 Layers of Insecurity

Popular banners

- CDP/LLDP strings
- FTP servers
- SMTP dialogues
- SNMP communities
- HTTP responses
- SSH version information
- IMAP/POP3 servers
- DNS (with suitable tools)
- Risk: high Impact: medium

DeepSec Vienna 2007
7 Layers of Insecurity

Mitigation:

• Always try to get rid of standard banners.

• Change/delete any hint on version numbers or patch level; don't use fake version numbers, delete them altogether instead (version numbers makes your system more attractive)

• Avoid publishing all available options and every installed module

• Use filters to modify/delete banner strings if possible

DNS Digging

- DNS zones are very important
- Public records disclose starting points
  - Avoid secret.fileserver.example.net
  - Attackers will use dictionaries
- Attackers will try to
  - zone transfer all data
  - identify DNS infrastructure
- Monitoring DNS queries can reveal attacks
- Risk: medium Impact: high

DeepSec Vienna 2007
7 Layers of Insecurity

Mitigation:

• Use “split horizon” DNS – use an internal and an external DNS zone

• Use different servers for internal and external zone

• Keep your external DNS zone as uninteresting and generic as possible

• Allow zone transfers only to DNS peers as required by DNS operation (usually your backup DNS servers)

Firewalking

- Mapping packet filters by response
- Attackers investigate
  - IP TTL
  - ICMP responses
  - IP/TCP options
  - responses to invalid packets
- Name stems from tool “firewalk”
- Risk: medium Impact: medium

DeepSec Vienna 2007
7 Layers of Insecurity

firewalk was born out of research conducted with traceroute. The tool was first mentioned in a publication (1998).

Mitigation:

• Block ICMP TTL Exceeded packets from internal hosts to outside hosts if possible.

• Drop all packets to unused ports.

• NAT devices or proxy servers break firewalk probes.

SNMP Walking

- SNMP offers rich informations
- Many network devices are SNMP-capable
- Attackers look for unprotected access
  - Port scanners on port 161/162 (UDP/TCP)
- Default information very useful
- Risk: medium Impact: high

DeepSec Vienna 2007
7 Layers of Insecurity

Mitigation:

• Block all untrusted access to SNMP ports.

• Collect all SNMP-accessible devices on a separate network or VLAN.

• Monitor SNMP probes and set alarms/warnings.

• Use and deploy SNMP v3 if possible (v3 offers encryption, integrity and authentication).

• Don't use SNMP writes with version prior to 3. Make sure write access is disabled.

Tools for Reconnaissance

- What to Use?

DeepSec Vienna 2007
7 Layers of Insecurity

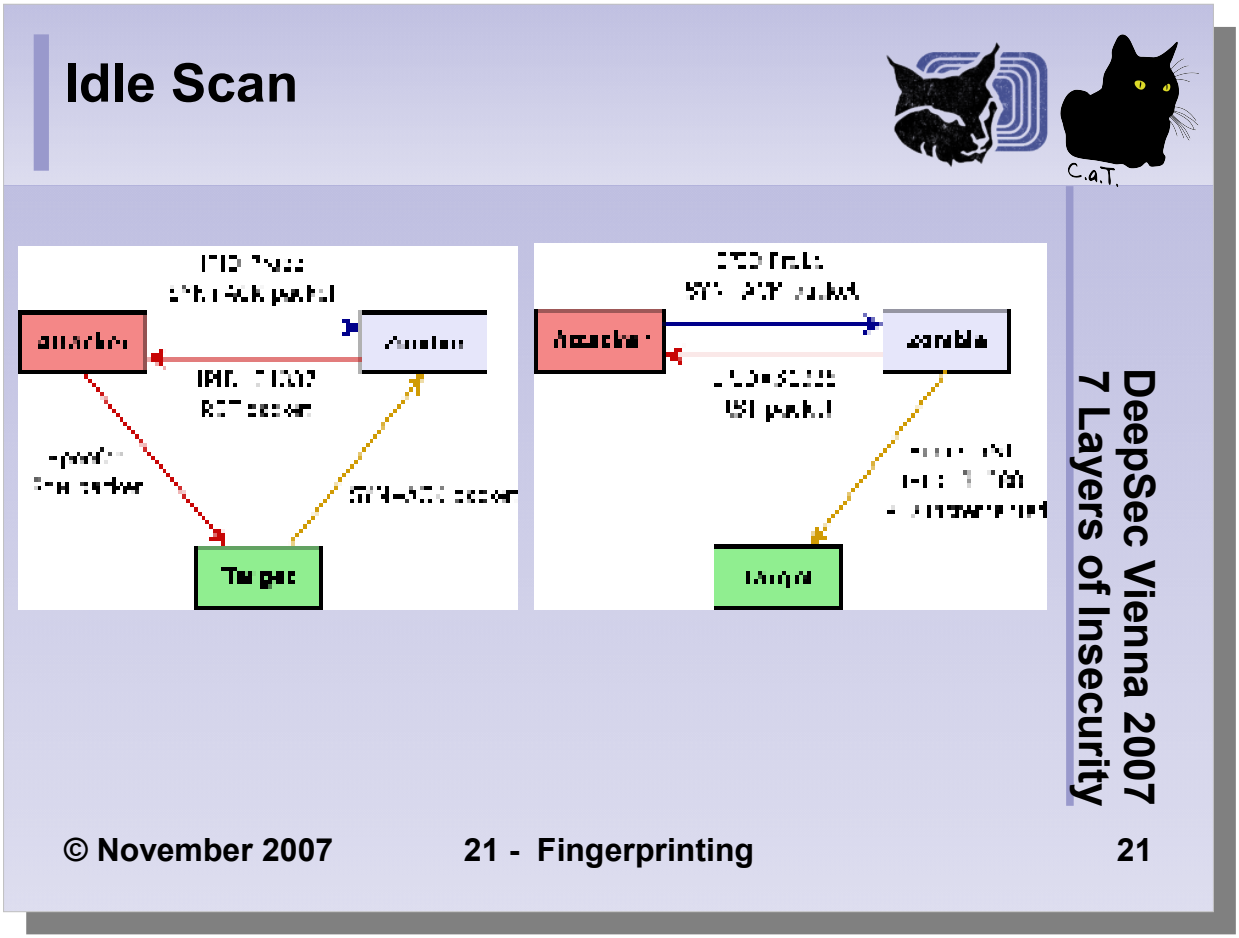
Tools of the trade

- Times change, tools adapt
  - telnet, ping, traceroute
  - telnet, hping2, tcptraceroute
- Any packet generator will do
- Any tool capable of TCP will do likewise
  - telnet is still common

nmap

- nmap is around since 1997
  - Host discovery
  - OS detection
  - Port scanning
  - Support for scripting
- nmap offers parallel scanning
- TCP, UDP, ICMP capability
- Protocol scan
- Idle scan
- Banner grabbing (version strings)

DeepSec Vienna 2007
7 Layers of Insecurity



The idle scan requires an intermediate host, called a *zombie*, that produces predictable IP IDs. The scans works by sending spoofed TCP/IP SYN packets to the target to be analysed. The sender address is the one from the zombie host. An open port at the target will produce a SYN+ACK packet which is sent to the zombie. Since the zombie didn't send the packet it replies with a RST and increases the IP ID. The attacker can then check for the next IP ID and deduce the state of the port at the target.

This technique was discovered by Salvatore 'Antirez' Sanfilippo, the author of *hping*, in 1998. There are still systems in use that are vulnerable to simple IP ID generation and thus can be used as zombies in idle scans.

xprobe2

- Active scanning tool, around since 2001
- Early focus on ICMP footprints
- Key features include fuzzy fingerprinting
- Multiple signatures used
  - TCP, UDP, ICMP
  - SNMP V2
  - SMB

DeepSec Vienna 2007
7 Layers of Insecurity

xprobe2 is the result of Ofir Arkin's research on ICMP. The results were published in a paper called *ICMP Usage in Scanning* (2001). Fyodor Yarochkin and Ofir Arkin coded the first version of xprobe and published it with the paper. xprobe2 sends UDP and ICMP datagrams to the target, trying to provoke ICMP answers. Surprisingly the handling of ICMP by different TCP/IP stacks provides enough information to identify the system that created the packets.

hping2/hping3

- "ping on steroids"
  - Sends crafted UDP, ICMP, TCP packets
  - Collects TCP ISN, pioneered Idle Scan
  - Has API for automated tests
- Useful for firewall/IDS/IPS testing
- More capable than standard tools

DeepSec Vienna 2007
7 Layers of Insecurity

hping has a long history. The tool was first used to punch holes into firewalls (by using suitable forwarding/tunneling ports) and TCP/IP protocol checks. hping3 offers a full API in Tcl and enables the user to automate all tests by constructing scripts.

```
foreach i [list 5 6 7 8 9 10] {
   hping send "ip(daddr=192.168.1.8,ttl=$i)+icmp(type=8,code=0)"
}
```

This snipped of code sends ICMP type 8 code 0 packets with varying TTL. Construction of packets can be easily done with a few commands.

Large networks

- Attackers map large networks
  - Automated scans for popular ports
  - “Auto-r00ter” attached
- Parallel scans may appear on monitoring
- Large scans reduce number of ports
  - Bulk scanners look for specifics

DeepSec Vienna 2007
7 Layers of Insecurity

Port Scanning Risks

- Risk: medium Impact: medium
- Mitigation
  - Drop malformed/useless/unwanted packets
  - Detect port sweeps, packet rates
  - Limit ICMP error rate
  - Reassemble fragments at border

DeepSec Vienna 2007
7 Layers of Insecurity

Identify Individuals

- Matching Addresses to People.

Personal Information

- Look out for anything like
  - E-mail addresses
  - Telephone numbers, FAX numbers
  - “Personalised” network addresses
  - Personal namespaces (in DNS)
- Personal information improves credibility
  - Important for social engineering
  - Useful for faking other information
- Risk: medium Impact: high

DeepSec Vienna 2007
7 Layers of Insecurity

Keeping corporate information locked is not an easy task. A lot of information will be published by normal business or organisational processes.

Mitigation:

• Classify information and publish guidelines how to deal with data according to classification levels.

• Publish generic contact information (central phone number, central address).

• Keep personalised namespaces internal.

• Control access to directory services (limit to authorised access if possible).

• Create and publish guidelines for use of email and email addresses.

Chapter 21
Fingerprinting

- Summary
  - Reconnaissance is about information.
  - Any protocol is affected.
  - Carefully design access to network(s).
  - Monitor incoming traffic.
  - Limit access wherever you can.
  - Know where your data is and what to do with it.

Thank you for your attention!

- Questions?

DeepSec Vienna 2007
7 Layers of Insecurity