OSY.SSI[2015][7]

Internet, Lab 1

Brace yourselves

You should all have received an e-mail.
If not, please install things as we go on.
If you can't please look on your neighbours.

Programme

- Packet interception, analysis, forge
- TCP scan, SYN/ACK prediction, ARP attacks
- Network mapping and port scanning
- Fingerprinting
- DNS attacks: Amplification and cache snooping
- (Wifi attacks)
- (Tor)
- (Zombie)

Table of Contents

Eavesdropping and packet analysis

We're gonna use something invented by this smiling guy.

Wireshark – Eavesdropping and packet analysis

by Gerald Combs, Riverbed technologies

Task:

- Launch `Wireshark`.
- Open `capture.cap` and analyse it (Demo)
- You can even capture packets if you want.

You can also capture Bluetooth, USB, ...

Table of Contents

Crafting packets

We're gonna use something invented by this Jesus guy (Defcon 10).

Scapy

by Philippe Biondi, EADS

Task: as `root` (why root?)

Scapy

by Philippe Biondi, EADS

Task: as `root` (why root?)

- `scapy`

Scapy

by Philippe Biondi, EADS

Task: as `root` (why root?)

- `scapy`
- `conf`

Scapy

by Philippe Biondi, EADS

Task: as `root` (why root?)

- `scapy`
- `conf`
- Generate a packet and look at it

Scapy

by Philippe Biondi, EADS

Task: as `root` (why root?)

- `scapy`
- `conf`
- Generate a packet and look at it

```
a=Ether()/IP(dst="www.ecp.fr")/TCP()/"GET /index.html HTTP/1.0 \n\n"
a
hexdump(a)
```

Scapy

Crafting packets

Task:

Scapy

Crafting packets

Task:

- Try the (layer 3) send-receive commands (`sr` and `sr1`):

Scapy

Crafting packets

Task:

- Try the (layer 3) send-receive commands (`sr` and `sr1`):

```
sr(IP(dst="x.x.x.x")/TCP(dport=[21,22,23]))
sr1(IP(dst="x.x.x.x")/TCP(dport=80,flags="S"))
_.summary()
```

Scapy

Crafting packets

Task:

- Try the (layer 3) send-receive commands (`sr` and `sr1`):

```
sr(IP(dst="x.x.x.x")/TCP(dport=[21,22,23]))
sr1(IP(dst="x.x.x.x")/TCP(dport=80,flags="S"))
_.summary()
```

- Hint:

Scapy

Crafting packets

Task:

- Try the (layer 3) send-receive commands (`sr` and `sr1`):

```
sr(IP(dst="x.x.x.x")/TCP(dport=[21,22,23]))
sr1(IP(dst="x.x.x.x")/TCP(dport=80,flags="S"))
_.summary()
```

- Hint: try `64.233.167.138`

Scapy

Crafting packets

Task:

- Try the (layer 3) send-receive commands (`sr` and `sr1`):

```
sr(IP(dst="x.x.x.x")/TCP(dport=[21,22,23]))
sr1(IP(dst="x.x.x.x")/TCP(dport=80,flags="S"))
_.summary()
```

- Hint: try `64.233.167.138`

Scapy

Some more functionalities

Task:

Scapy

Some more functionalities

Task:

- Use `sniff(count=20)` to listen to the connections

Scapy

Some more functionalities

Task:

- Use `sniff(count=20)` to listen to the connections
- (you can specify `filter=` or `iface=`)

Scapy

Some more functionalities

Task:

- Use `sniff(count=20)` to listen to the connections
- (you can specify `filter=` or `iface=`)
- Try `lsc()` to see a few more functions and `ls`

Scapy

Some more functionalities

Task:

- Use `sniff(count=20)` to listen to the connections
- (you can specify `filter=` or `iface=`)
- Try `lsc()` to see a few more functions and `ls`

Scapy

Forging packets

Task:

Scapy

Forging packets

Task:

- Send a forged IP packet with a *fake source IP*

Scapy

Forging packets

Task:

- Send a forged IP packet with a *fake source IP*
- Send an ARPing on the LAN

Scapy

Forging packets

Task:

- Send a forged IP packet with a *fake source IP*
- Send an ARPing on the LAN

Question:

Scapy

Forging packets

Task:

- Send a forged IP packet with a *fake source IP*
- Send an ARPing on the LAN

Question: how do you test that it works?

Scapy

Cartography

Task:

Scapy

Cartography

Task: Traceroute to a certain website:

Scapy

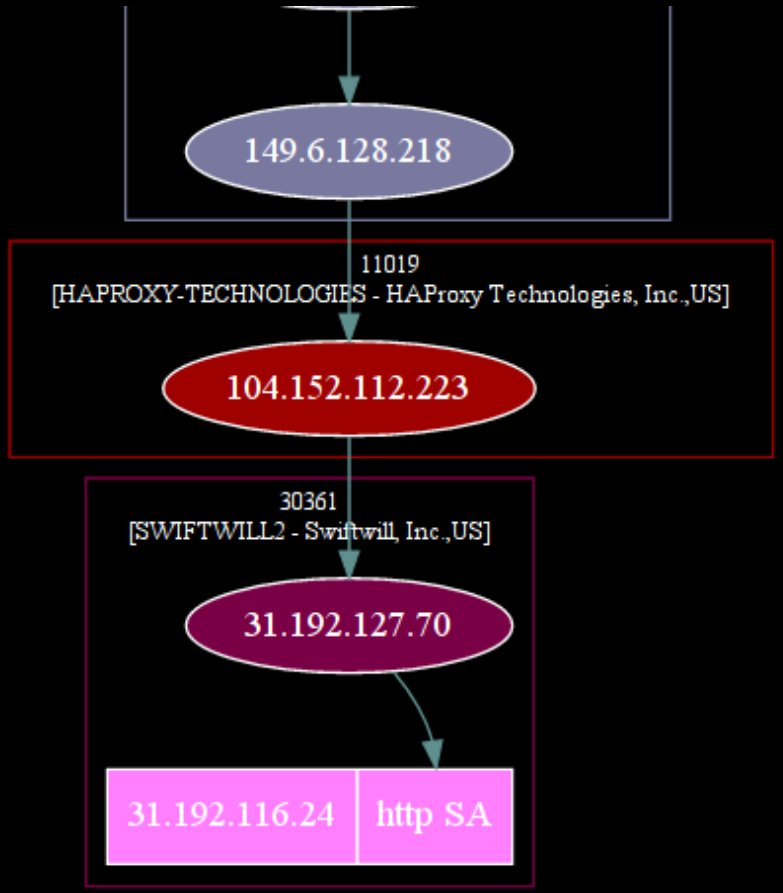
Cartography

Task: Traceroute to a certain website:

```
res, _ = traceroute("www.ecp.xxx",
                    dport=80,
                    maxttl=20,
                    retry=2)
res.graph(target="> graph.svg")
```

Scapy

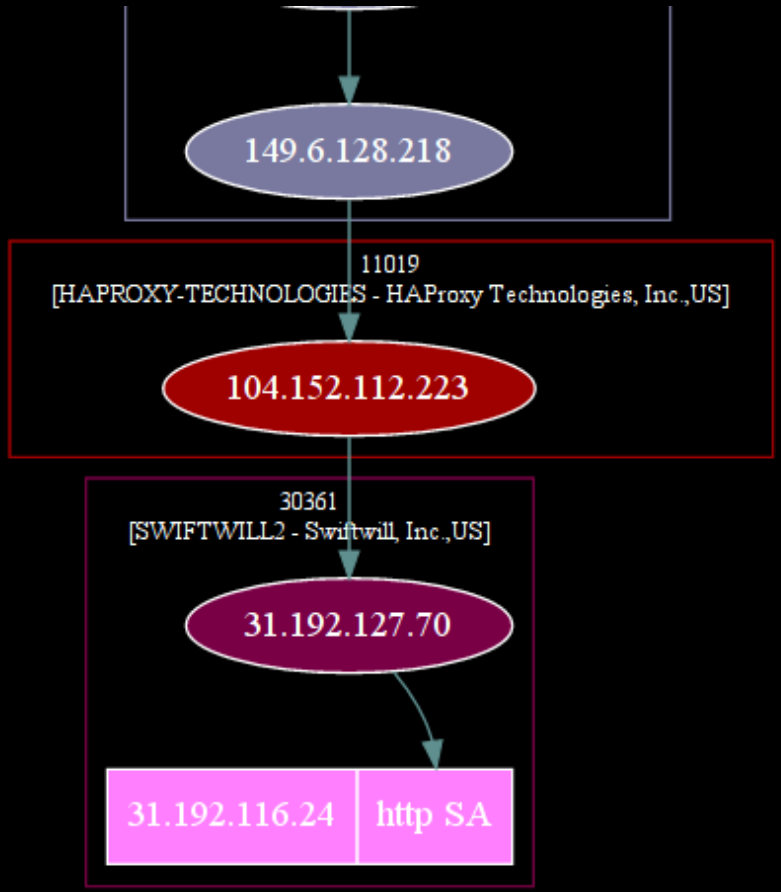
Cartography



Ad:

Scapy

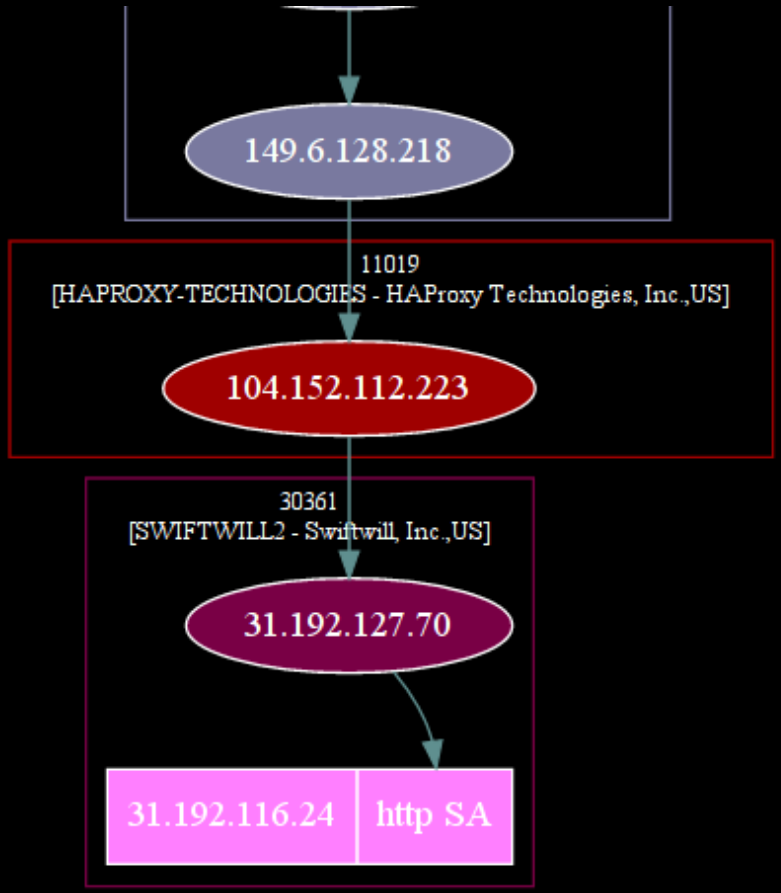
Cartography



Ad: `scapy` is simple, powerful and extensible.

Scapy

Cartography



Ad: `scapy` is simple, powerful and extensible. `import scapy`.

Mapping, scanning, fingerprinting

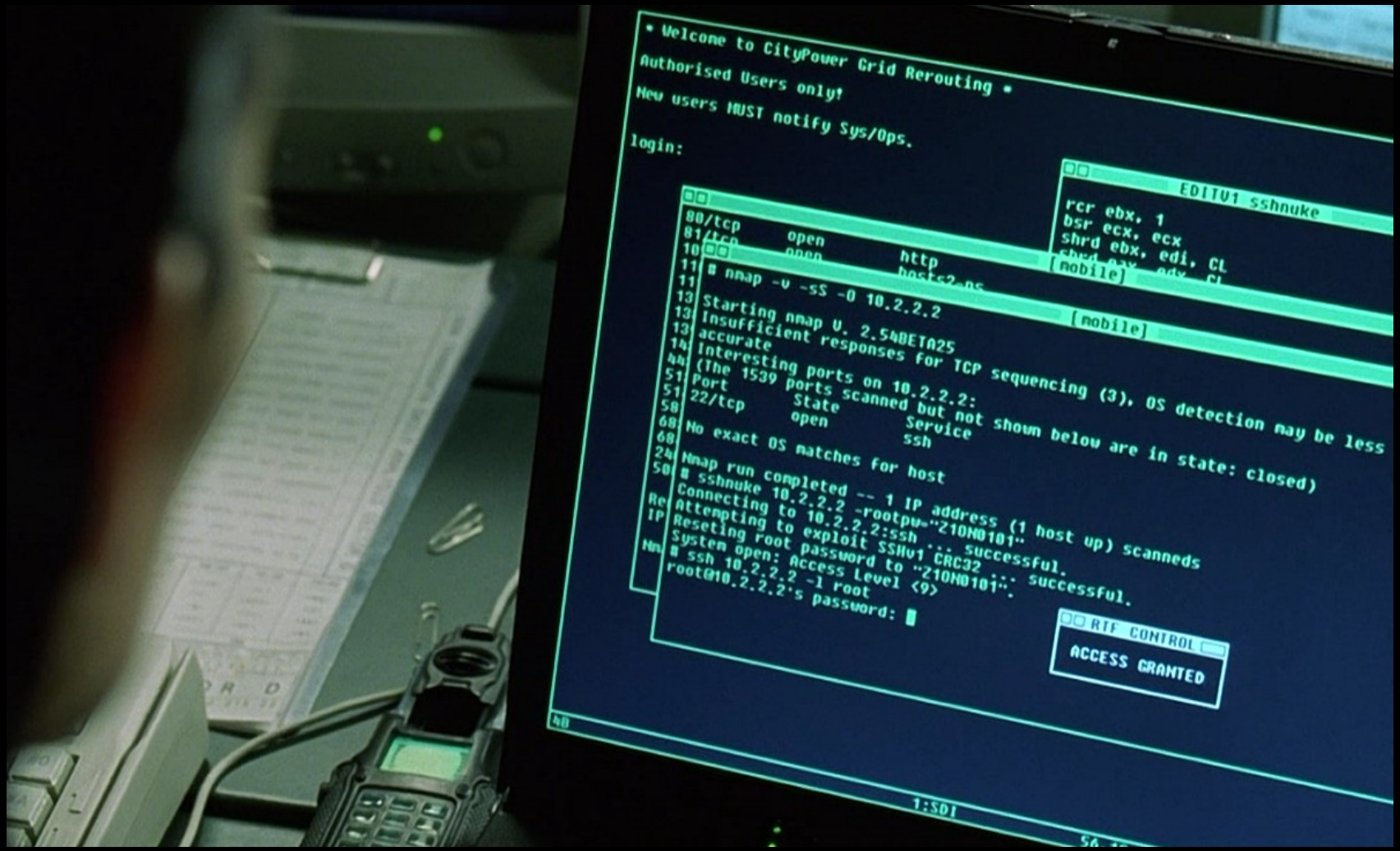
Now we're relying on this classy young lad's toys.

nmap

by Gordon “Fyodor” Lyon, Insecure.com LLC

One of the best tools of the trade, and the most famous.

- Host discovery (ping, `P`)
- Port discovery (scan, `s`)
- Service/OS discovery (fingerprinting)
- Vulnerability discovery (scripts, `v`)


• Welcome to CityPower Grid Rerouting •
Authorised Users only!
New users MUST notify Sys/Ops.
login:
EDITV1 sshnuke
rcr ebx, 1
bsr ecx, ecx
shrd ebx, edi, CL
[mobile]
80/tcp open http
81/tcp open
nmap -v -sS -O 10.2.2.2
Starting nmap V. 2.54BETA25
Insufficient responses for TCP sequencing (3), OS detection may be less accurate
Interesting ports on 10.2.2.2:
(The 1539 ports scanned but not shown below are in state: closed)
Port State Service
22/tcp open ssh
No exact OS matches for host
Nmap run completed -- 1 IP address (1 host up) scanneds
sshnuke 10.2.2.2 -rootpw="Z1ON0101"
Connecting to 10.2.2.2:ssh ... successful.
Attempting to exploit SSHv1 CRC32 ... successful.
Reseting root password to "Z1ON0101".
System open: Access Level <9>
ssh 10.2.2.2 -l root
root@10.2.2.2's password:
RIF CONTROL
ACCESS GRANTED
1:SDI

Mapping, scanning, fingerprinting

Host discovery

- Scan the /24
- Try different ping options PS, PA, PE, PP, PM, PR, PN, sP

Mapping, scanning, fingerprinting

Port and service scanning

- Scan your own ports
- Try different scanning options sA, sW, sF, sX, sM, sU, sY, sZ, sT, sO

Mapping, scanning, fingerprinting

Traceroute and mapping

nmap was originally designed to ease with network mapping.

- You can use `-traceroute`

Mapping, scanning, fingerprinting

Fingerprinting

- `-O -v <IP>`: OS fingerprinting
- `-sV -sCV -v <IP>`: Service fingerprinting

Table of Contents

Amplification attacks

A la mano

Task:

- DNS query `dig ANY isc.org @8.8.8.8`
- Intercept and analyse the packet
- Forge (i.e. with scapy) a DNS query with a fake source IP.
- Test it with one of your friends :)

You can use nmap to find candidate DNS servers, see `https://svn.nmap.org/nmap/scripts/dns-recursion.nse`

Snooping attacks

Using nmap scripts

DNS cache snooping is seomtimes useful, see
`https://svn.nmap.org/nmap/scripts/dns-cache-snoop.nse`