OSY.SSI[2018][9]

We saw the theory

Now it's time to get real.

Programme:

- Basic networking (whois, DNS, reverse DNS)
- Packet interception and analysis (Wireshark)
- Ping and scan (nmap)
- Network mapping (nmap)
- Fingerprinting (nmap)
- DNS amplification (a la mano)
- And more if time allows (dnsoop, thc-ipv6, shodan-hq, p0f, vncroulette...)

Goal: gather a max of info on a target.

You need an Internet connection from inside the VM. You'll need `root` access to run some commands.

Table of Contents

Warming up

Setting up the forge

Creating a map

Warming up

ip/ifconfig, dig, host... whois ping. Ctrl + C! man woman children too sudo. tcpdump? Wireshark!

Table of Contents

Warming up

Setting up the forge

Creating a map

Scapy

by Philippe Biondi

Task:

- `scapy` (as `root`)

Scapy

by Philippe Biondi

Task:

- `scapy` (as `root`)
- Generate a packet and look at it

Scapy

by Philippe Biondi

Task:

- `scapy` (as `root`)
- Generate a packet and look at it

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

Notice that it is almost literally “Ethernet/IP/TCP/HTTP"

Scapy: Send and receive packets

Task:

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

Scapy: Send and receive packets

Task:

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

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

- Hint:

Scapy: Send and receive packets

Task:

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

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

- Hint: try `x.x.x.x = 64.233.167.138`

Notice that `sr` will wait for a reply! And will block until it gets one.

(For layer 2, use `srp`, `sendp` etc.)

Scapy: Fake sender IP

Task: Send a forged IP packet with a fake source IP (use `send`, not `sr`, why?)

Question: how do you test that it works?

Scapy: Sniffing and ARPing

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`
- Send an ARPing on the LAN

Scapy: Tracerouting

Task:

Scapy: Tracerouting

Task: Traceroute to a certain website:

Scapy: Tracerouting

Task: Traceroute to a certain website:

```
res, _ = traceroute("www.saclay.xxx", dport=80, maxttl=30, retry=2)
res.graph(target="> graph.svg")
```

Scapy: Tracerouting

Task: Traceroute to a certain website:

```
res, _ = traceroute("www.saclay.xxx", dport=80, maxttl=30, retry=2)
res.graph(target="> graph.svg")
```

You can recover the .svg file using `scp` to your own device and open it (e.g. with a browser).

Scapy: DNS amplification

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 :)

Scapy: QUANTUM

(Maybe too long for the lecture, do it at home)

Task: Using scapy, reproduce the NSA QUANTUM attacks

- Extract acknowledgement number and port from a TCP/IP packet
- Create a fake `RST` packets coming "from the server" to interrupt the connection
- Detect if the TCP/IP packet sent by the target uses HTTP
- Create a fake HTTP redirect response to send the target to another website

How would you test it in real conditions?

Table of Contents

Warming up

Setting up the forge

Creating a map

Network mapping

Having handy tools is good for diagnosis and toying around.

But sometimes we need to scan 1000's of hosts.

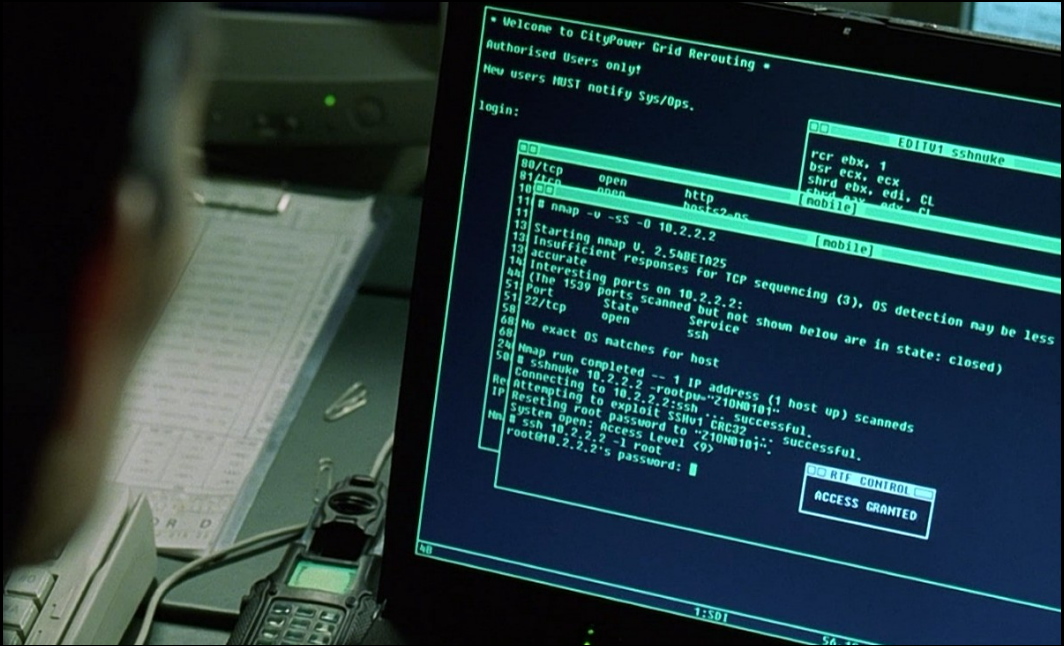
We need to be fast and precise, and automated.

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:
```

```
80/tcp
81/tcp     open         http
                        hosts2-ns
```

```
rcr ebx, 1
bsr ecx, ecx
shrd ebx, edi, CL
shrd eax, edx, CL
```

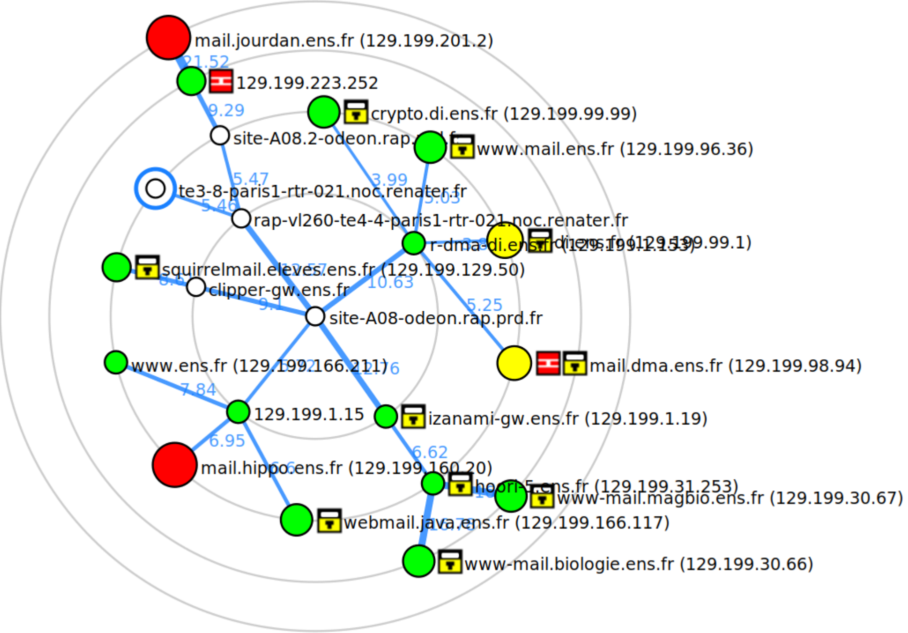
```
# nmap -v -sS -O 10.2.2.2
Starting nmap V. 2.54BETA25
Insufficient responses for TCP sequencing (3), OS detection may be less
accurate
Interesting ports on 10.2.2.2:
(The 1539 ports scanned but not shown below are in state: closed)
Port       State       Service
22/tcp     open        ssh

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:
```

nmap – The real Schweizertaschenmesser

- Choose a target
- Try different ping options `-PS, -PA, -PE, -PP, -PM, -PR, -PN, -sP`
- Try different scanning options `-sA, -sW, -sF, -sX, -sM, -sU --reason, -sY, -sZ, -sT, -sO`
- Try deactivating initial ping `-P0`
- Try using decoys `-D`
- Try fragmenting `-f`
- Try `--traceroute`
- Try OS fingerprinting : `-O --osscan-guess -v, -A`
- Try service fingerprinting: `-sV -sCV -v`
- Try all-fingers: `-A -v`
- Try spoofing your MAC address: `--spoof-mac <fakeMAC> <target>`
- And more: `-mtu, --data-length, --badsum`,...


mail.jourdan.ens.fr (129.199.201.2)
21.52
129.199.223.252
9.29
crypto.di.ens.fr (129.199.99.99)
site-A08.2-odeon.rap.prd.fr
www.mail.ens.fr (129.199.96.36)
5.47
3.99
te3-8-paris1-rtr-021.noc.renater.fr
5.03
5.46
rap-vl260-te4-4-paris1-rtr-021.noc.renater.fr
r-dma-di.ens.fr (129.199.1.153)
di.ens.fr (129.199.99.1)
squirrelmail.eleves.ens.fr (129.199.129.50)
12.57
10.63
clipper-gw.ens.fr
9.1
5.25
site-A08-odeon.rap.prd.fr
www.ens.fr (129.199.166.211)
mail.dma.ens.fr (129.199.98.94)
7.84
129.199.1.15
izanami-gw.ens.fr (129.199.1.19)
6.95
6.62
mail.hippo.ens.fr (129.199.160.20)
6.6
hoori-5.ens.fr (129.199.31.253)
www-mail.magbio.ens.fr (129.199.30.67)
webmail.java.ens.fr (129.199.166.117)
www-mail.biologie.ens.fr (129.199.30.66)

Finding candidates for DNS attacks

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

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

Let's stop here.

Thank you!