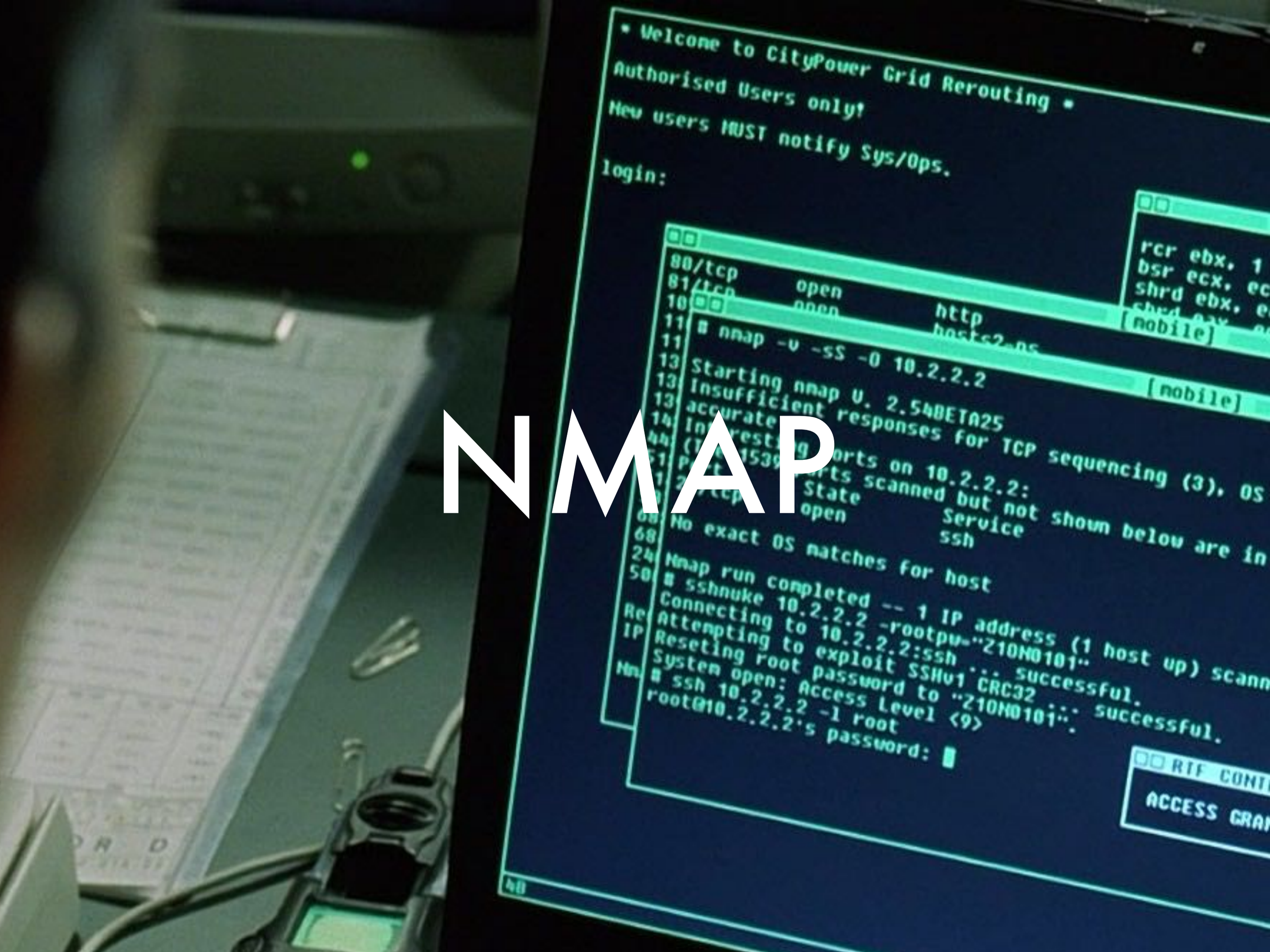

* Welcome to CityPower Grid Rerouting *
Authorised Users only!
New users MUST notify Sys/Ops.
login:
80/tcp open http
nmap -v -sS -O 10.2.2.2
Starting nmap V. 2.54BETA25
Insufficient responses for TCP sequencing (3), OS
accurate
Interesting ports on 10.2.2.2:
State Service
open ssh
No exact OS matches for host
Nmap run completed -- 1 IP address (1 host up) scann
sshnuke 10.2.2.2 -rootpw="Z1ON0101"
Connecting to 10.2.2.2:ssh ... successful.
Attempting to exploit SSHv1 CRC32
Reseting root password to "Z1ON0101".
System open: Access Level <9>
ssh 10.2.2.2 -l root
root@10.2.2.2's password:
ACCESS GRAN

NMAP

AGENDA DAY 1

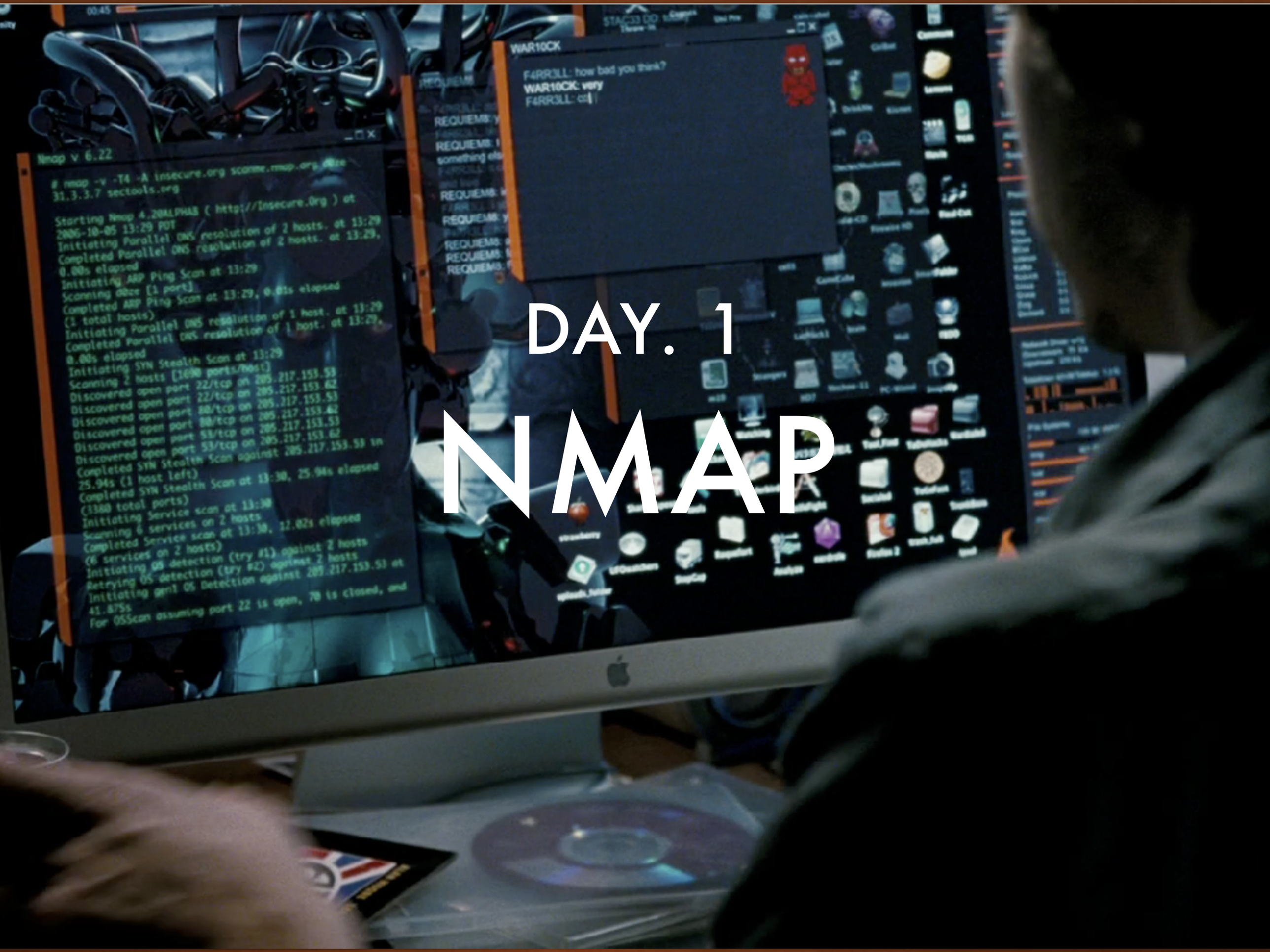
- Introduction to NMAP
- Installation
- Basic Scanning Techniques
- Host Discovery Options
- Port Scanning Basic
- Port Scanning Techniques and Options
- Service & Version Detection
- Operating System Detection

AGENDA DAY 2

- Advanced Scanning Options
  - Firewall Evasions
  - Timing Options
  - IPv6 Scanning
- Output Options
- Debugging and Troubleshooting

AGENDA DAY 3

- Nmap Scripting Engine (NSE)
  - Introduction
  - Usage and Examples
- Zen map
  - Introduction
  - Usage and Example
- Other Nmap bundle tools usage (Ncat, Ndiff, Nping)


WAR10CK
F4RR3LL: how bad you think?
WAR10CK: very
F4RR3LL:
Nmap v 6.22
DAY. 1
NMAP

INTRODUCTION

NMAP

- Nmap (Network Mapper) is a free and open source (license) utility for network discovery and security auditing
- Created by Gordon “Fyodor” Lyon
- First published in September 1997, as an article in Phrack Magazine with source-code included.

INTRODUCTION

NMAP SUITES

- Nmap suite includes an advanced GUI and results viewer (Zenmap), a flexible data transfer, redirection, and debugging tool (Ncat), a utility for comparing scan results (Ndiff), and a packet generation and response analysis tool (Nping).


* Welcome to CityPower Grid Rerouting *
Authorised Users only!
New users MUST notify Sys/Ops.
login:
80/tcp open http
nmap -v -sS -O 10.2.2.2
Starting nmap V. 2.54BETA25
Insufficient responses for TCP sequencing (3), OS
accurate
Interesting ports on 10.2.2.2:
(The 1539 ports scanned but not shown below are in
Port State Service
22/tcp open ssh
No exact OS matches for host
Nmap run completed -- 1 IP address (1 host up) scann
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:
[mobile]
[mobile]
ACCESS GRA


WAR10CK
F4RR3LL: how bad you think?
WAR10CK: very
Nmap v 6.22

INSTALLATION

NMAP

- Support: Linux (all distributions), Microsoft Windows, Mac OS X, FreeBSD, OpenBSD, and NetBSD, Sun Solaris, Amiga, HP-UX, and Other Platforms

- https://nmap.org/download.html

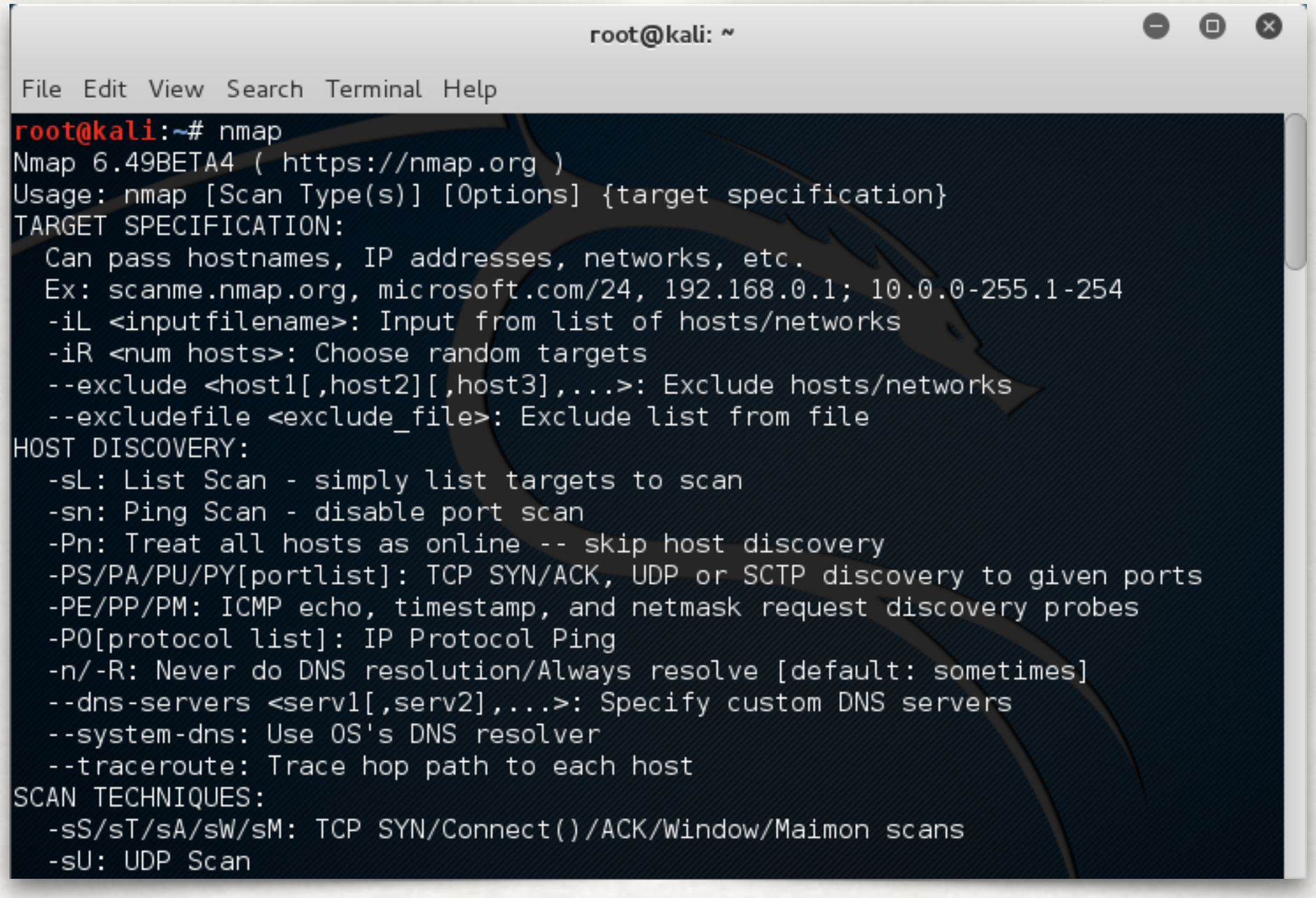
SCANNING ACTIVITY

NMAP

- PENETRATION TESTING/HACKING
- Footprinting/Scanning
  - Port Scanning
  - Service Scanning
  - OS Scanning
- BUT, NMAP more than just a port scanner!

BASIC SCANNING

NMAP USAGE



**apt-get install —only-upgrade nmap*

BASIC SCANNING

TARGET SPECIFICATION

- Everything on the Nmap command-line that isn't an option (or option argument) is treated as a target host specification. The simplest case is to specify a target IP address or hostname for scanning

BASIC SCANNING

TARGET SPECIFICATION

- Targets are usually specified on the command lines or as file with list of targets.
- nmap [ip]/[ip1 ip2]/[hosname]/[network]/[network range]

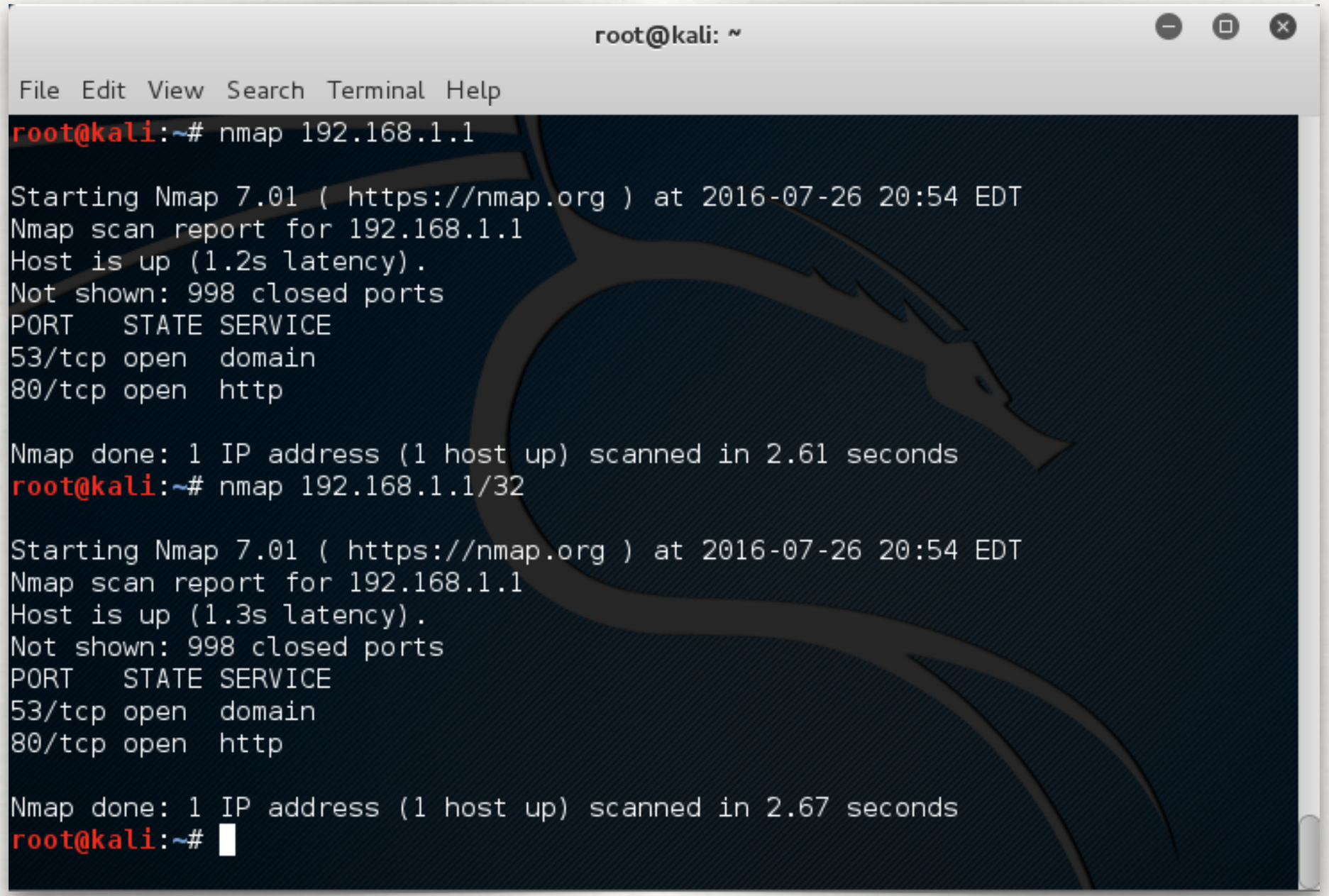
BASIC SCANNING

TARGET SPECIFICATION

- nmap 192.168.1.1
- nmap google.com
- nmap 192.168.1.1/32
- nmap 192.168.1.0/24

BASIC SCANNING

TARGET SPECIFICATION



BASIC SCANNING

STANDARD NMAP RESULT

- PORT: port number/protocol
- STATE: Status of the port
- SERVICE: Type of Service for the port
- VERSION: Version of the service

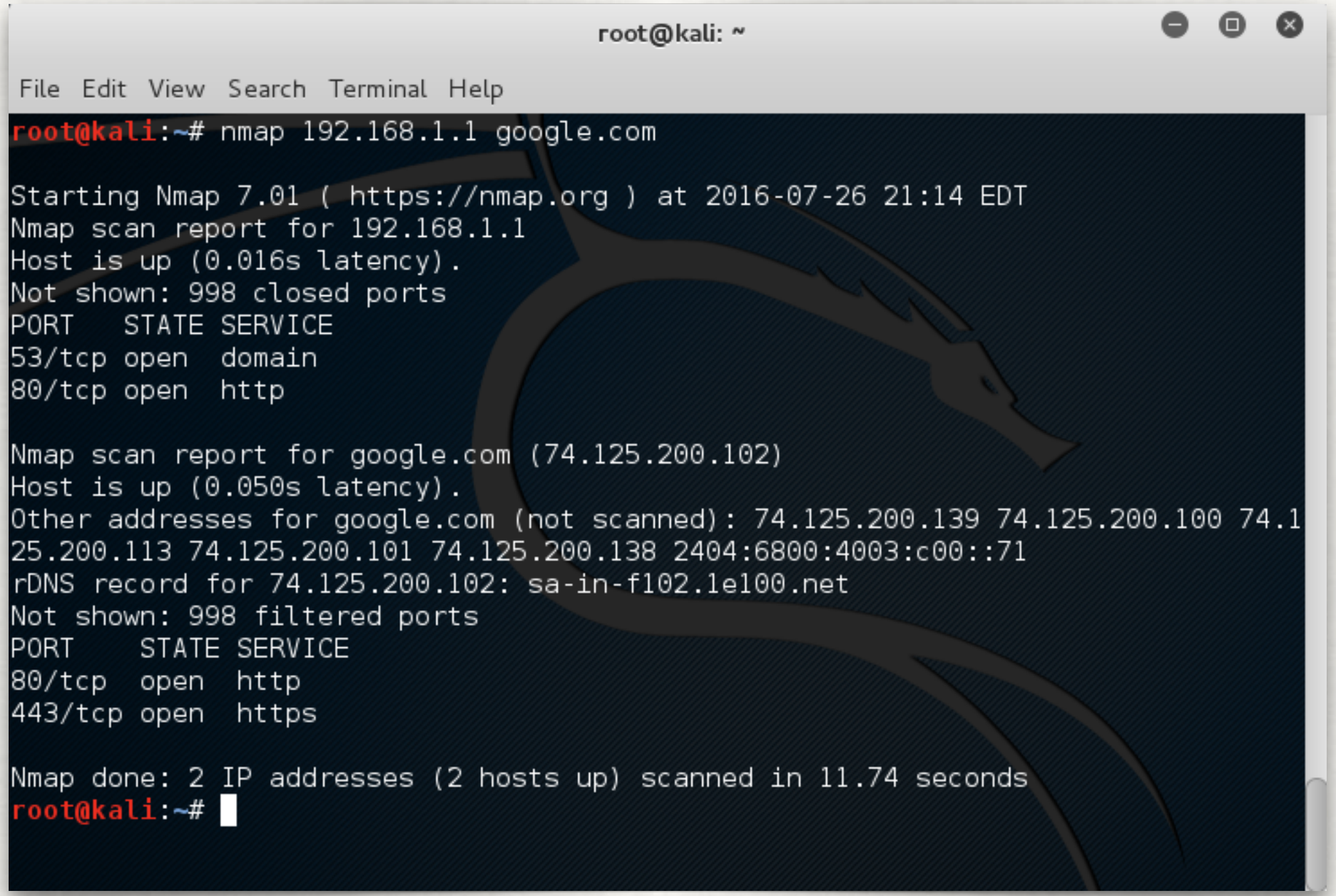
BASIC SCANNING

TARGET SPECIFICATION

- nmap 192.168.1.1 google.com
- nmap 192.168.1.0/24 google.com/24
- nmap 192.168.1.**1-254** 10.0.**0-255.1-254**

BASIC SCANNING

TARGET SPECIFICATION



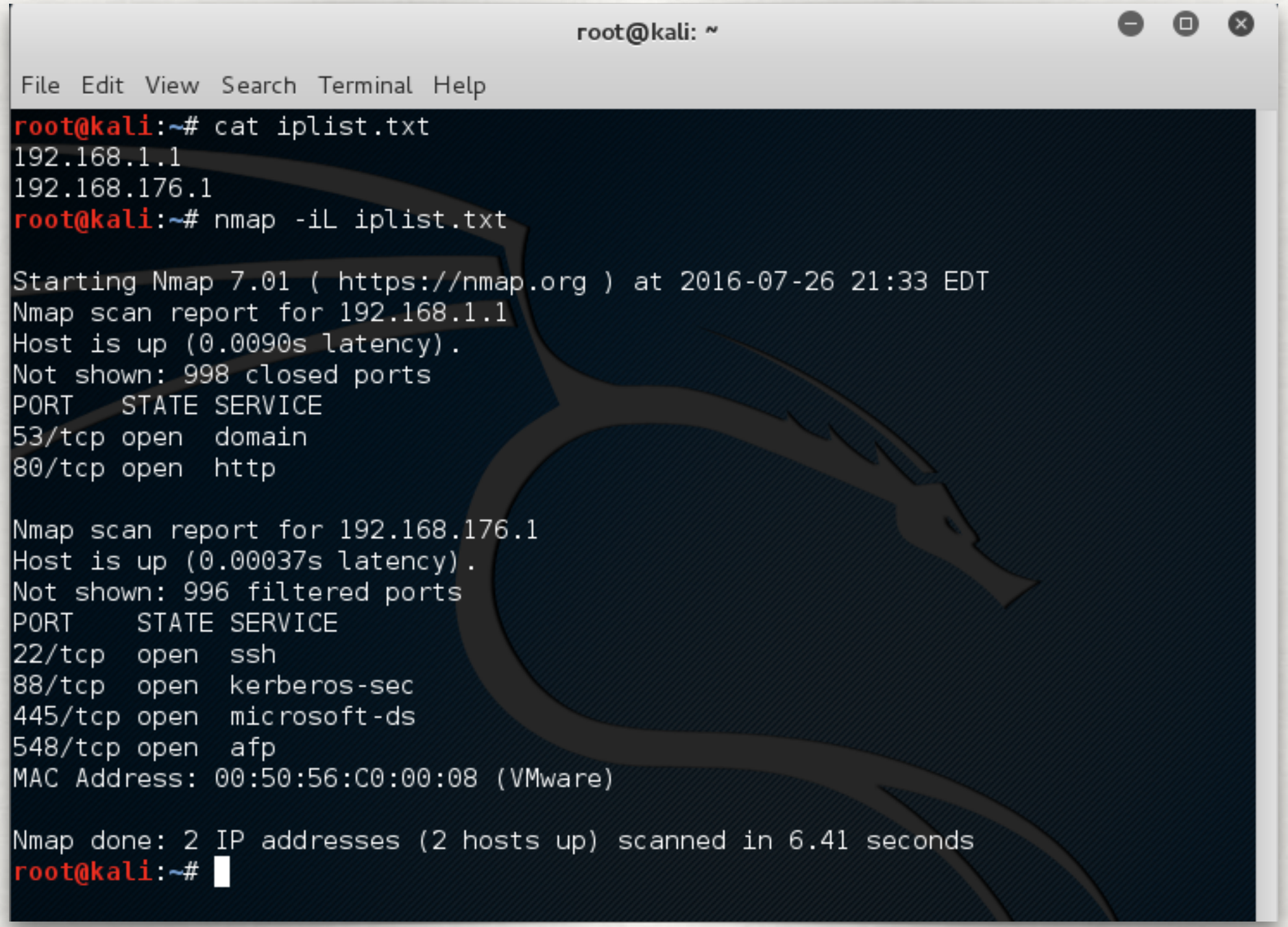
BASIC SCANNING

TARGET SPECIFICATION

- Reads target specifications from inputfilename
  - nmap -iL [file list]
  - nmap -iL iplist.txt

BASIC SCANNING

TARGET SPECIFICATION



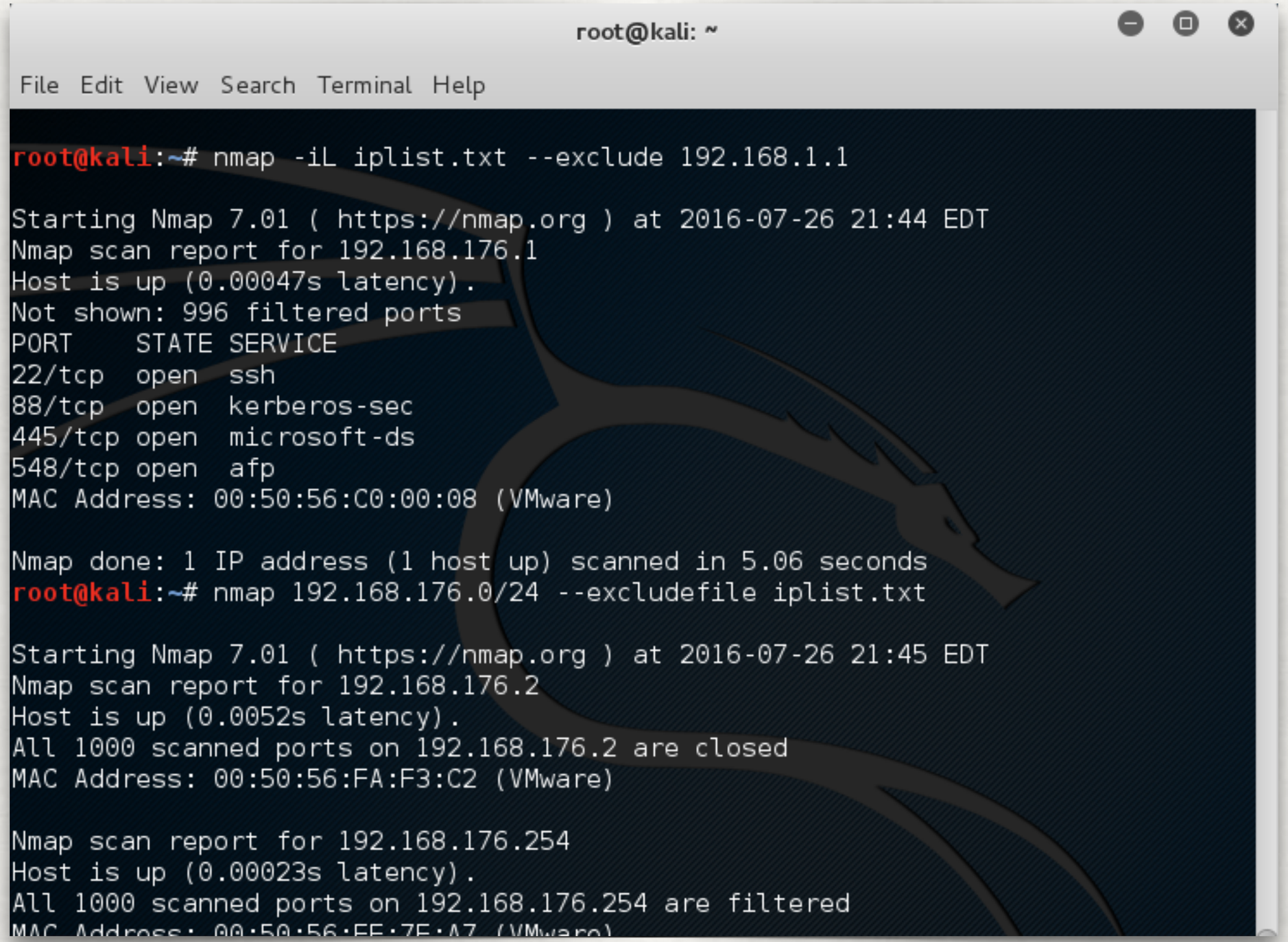
BASIC SCANNING

TARGET SPECIFICATION

- Exclude spesific target
  - nmap -iL iplist.txt --exclude [ip]
  - nmap 192.168.176.0/24 --excludelist iplist.txt

BASIC SCANNING

TARGET SPECIFICATION



BASIC SCANNING

HOST DISCOVERY

- One of the very first steps in any network reconnaissance mission is to reduce a (sometimes huge) set of IP ranges into a list of active or interesting hosts.
- An administrator may be comfortable using just an ICMP ping to locate hosts on his internal network, while an external penetration tester may use a diverse set of dozens of probes in an attempt to evade firewall restrictions.
- Because host discovery needs are so diverse, Nmap offers a wide variety of options for customizing the techniques used.
- Host discovery is sometimes called ping scan, but it goes well beyond the simple ICMP echo request packets associated with the ubiquitous ping tool.
- Users can skip the ping step entirely with a list scan (-sL) or by disabling ping (-Pn), or engage the network with arbitrary combinations of multi-port TCP SYN/ACK, UDP, SCTP INIT and ICMP probes.

BASIC SCANNING

HOST DISCOVERY OPTIONS

```
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
```

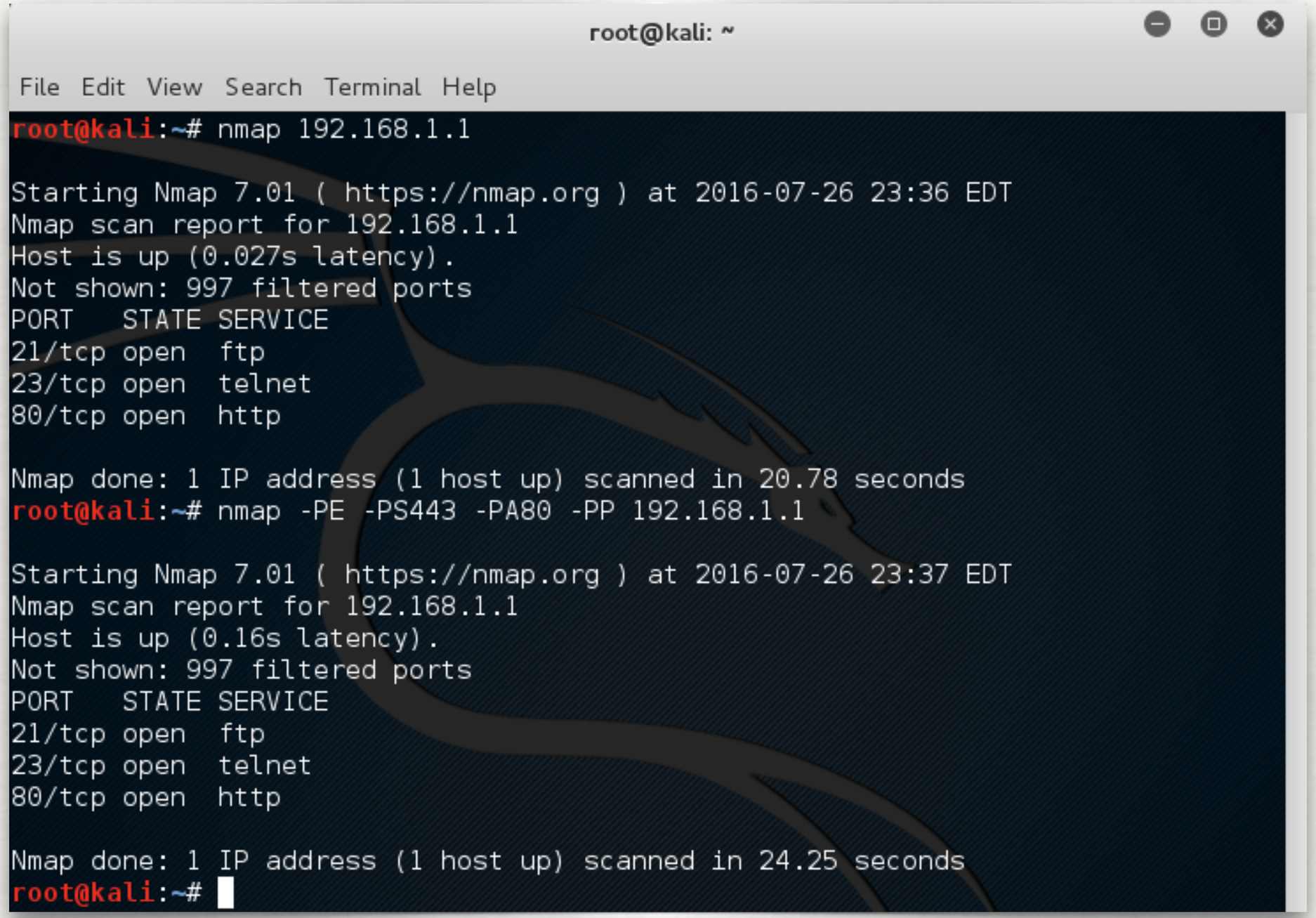
BASIC SCANNING

HOST DISCOVERY

- If no host discovery options are given, Nmap sends an ICMP echo request, a TCP SYN packet to port 443, a TCP ACK packet to port 80, and an ICMP timestamp request. (For IPv6, the ICMP timestamp request is omitted because it is not part of ICMPv6.) These defaults are equivalent to the -PE -PS443 -PA80 -PP options.

BASIC SCANNING

HOST DISCOVERY



BASIC SCANNING

HOST DISCOVERY OPTIONS

- -sL (list scan) - Didnt scan, just generate IP Address and do Reverse DNS lookup.

BASIC SCANNING

HOST DISCOVERY OPTIONS

```
bash-3.2# nmap -sL 192.168.2.115-125

Starting Nmap 7.00 ( https://nmap.org ) at 2016-07-27 20:50 WIB
Nmap scan report for 192.168.2.115
Nmap scan report for 192.168.2.116
Nmap scan report for 192.168.2.117
Nmap scan report for 192.168.2.118
Nmap scan report for 192.168.2.119
Nmap scan report for 192.168.2.120
Nmap scan report for 192.168.2.121
Nmap scan report for 192.168.2.122
Nmap scan report for piko (192.168.2.123)
Nmap scan report for 192.168.2.124
Nmap scan report for 192.168.2.125
Nmap done: 11 IP addresses (0 hosts up) scanned in 13.01 seconds
```

BASIC SCANNING

HOST DISCOVERY OPTIONS

- -sn (No port scan) - This option tells Nmap not to do a port scan after host discovery, and only print out the available hosts that responded to the host discovery probes. The default host discovery done with -sn consists of an ICMP echo request, TCP SYN to port 443, TCP ACK to port 80, and an ICMP timestamp request by default.

BASIC SCANNING

HOST DISCOVERY OPTIONS

```
root@kali:~# nmap -sn 192.168.176.200-255

Starting Nmap 7.01 ( https://nmap.org ) at 2016-07-27 09:53 EDT
Nmap scan report for 192.168.176.226
Host is up (0.00038s latency).
MAC Address: 00:0C:29:BA:E6:DD (VMware)
Nmap scan report for 192.168.176.254
Host is up (0.00011s latency).
MAC Address: 00:50:56:FE:7E:A7 (VMware)
Nmap scan report for 192.168.176.225
Host is up.
Nmap done: 56 IP addresses (3 hosts up) scanned in 26.86 seconds
root@kali:~#
```

BASIC SCANNING

HOST DISCOVERY OPTIONS

- -Pn - This option skips the Nmap discovery stage altogether.
- -PS [port] [list] (TCP SYN Ping) - This option sends an empty TCP packet with the SYN flag set.

BASIC SCANNING

HOST DISCOVERY OPTIONS

```
root@kali:~# ping 192.168.176.226
PING 192.168.176.226 (192.168.176.226) 56(84) bytes of data.
^C
root@kali:~# nmap -Pn 192.168.176.226

Starting Nmap 7.01 ( https://nmap.org ) at 2016-07-27 10:00 EDT
Nmap scan report for 192.168.176.226
Host is up (0.00014s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:0C:29:BA:F6:DD (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.95 seconds
root@kali:~#
```

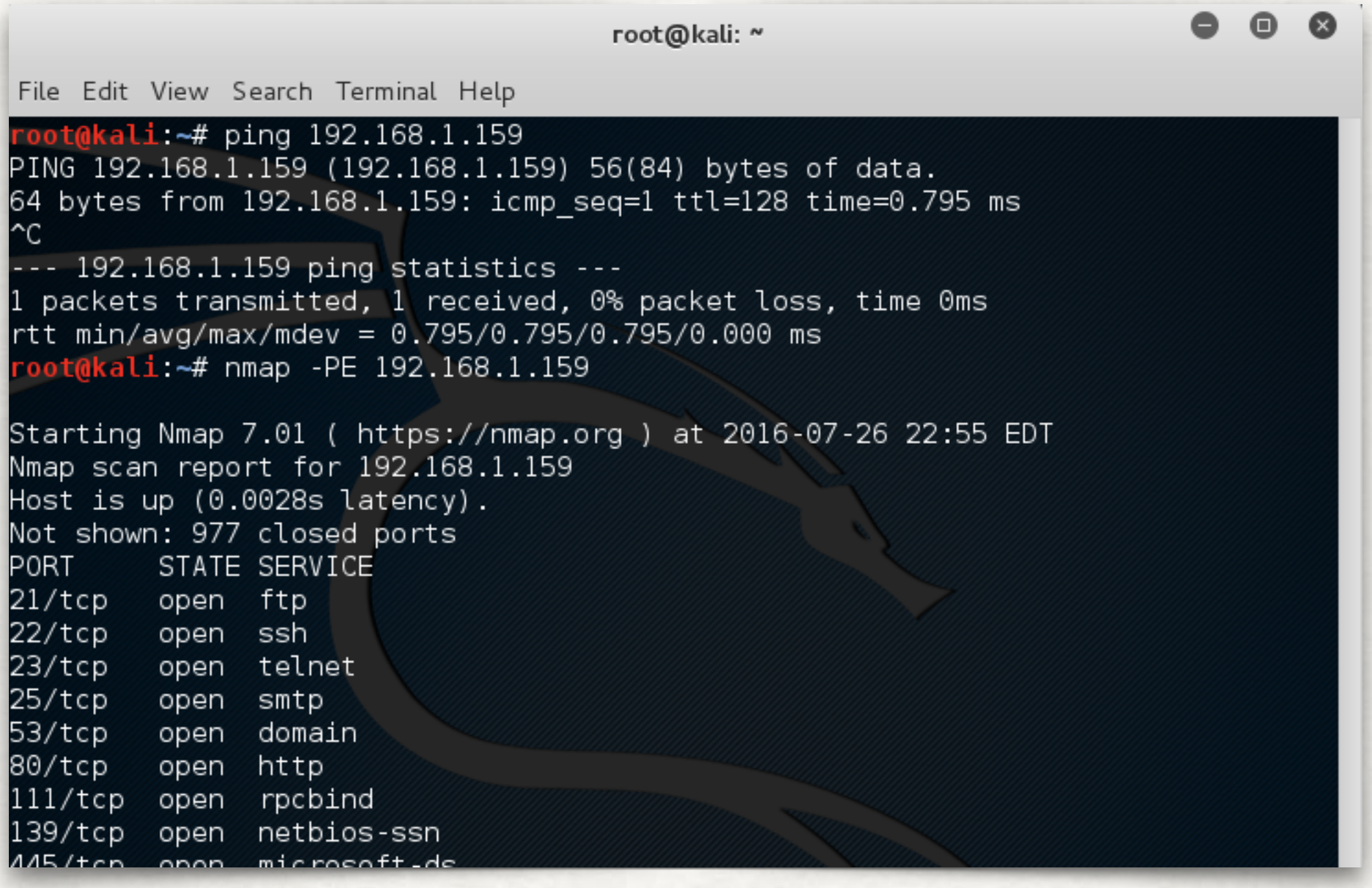
BASIC SCANNING

HOST DISCOVERY OPTIONS

- -PA [port] [list] (TCP ACK Ping) - This option sends an empty TCP packet with the ACK flag set
- -PU [port] [list] (UDP Ping) - This options sends a UDP packet to the given ports.
- -PY [port] [list] (SCTP INIT Ping) - This option sends an SCTP packet containing a minimal INIT chunk that suggests to the remote system that you are attempting to establish an association
- -PE; -PP; -PM (ICMP Ping Types) - This option sends an ICMP Echo Messages, Timestamp and address mask queries

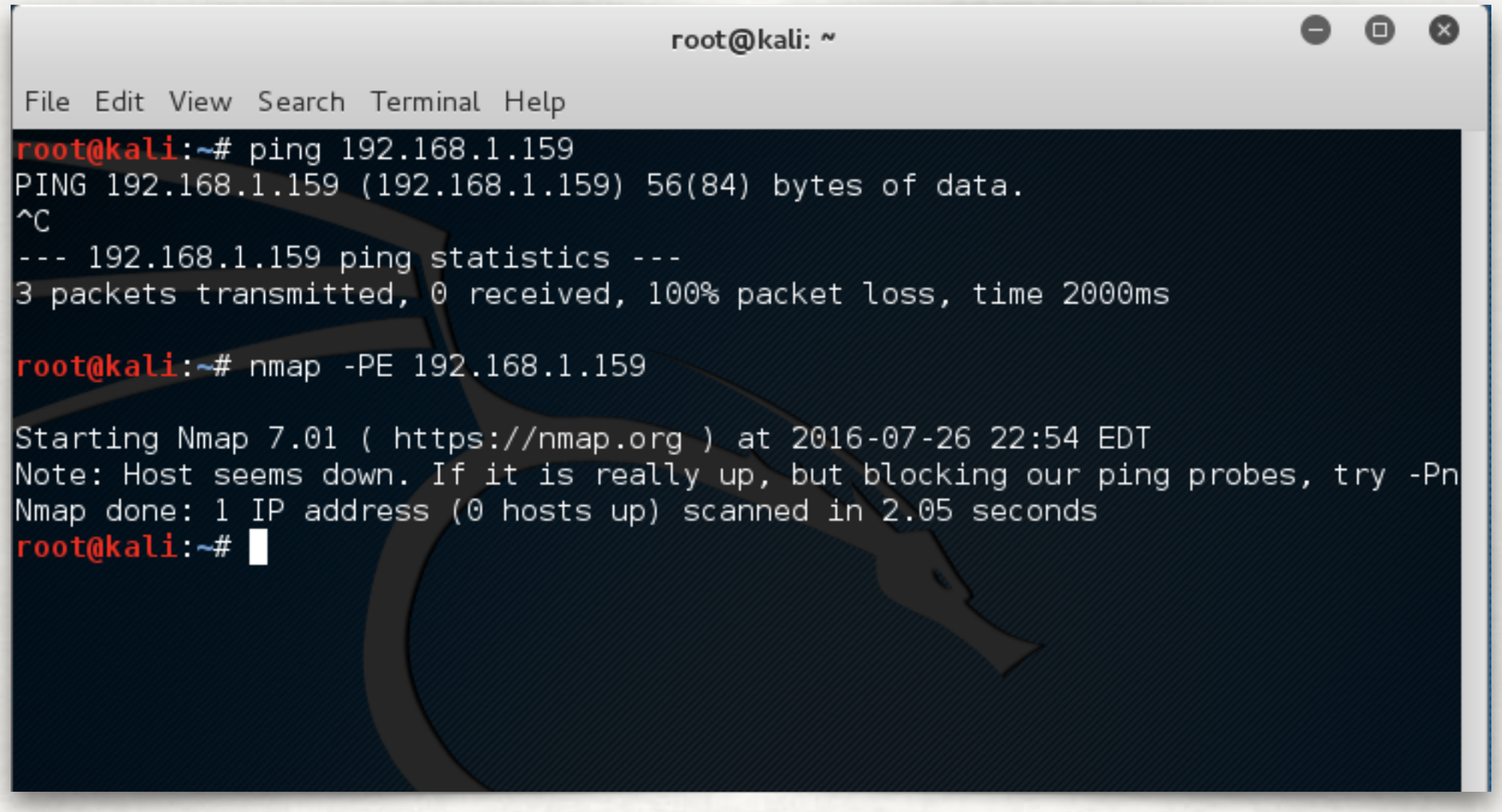
BASIC SCANNING

HOST DISCOVERY



BASIC SCANNING

HOST DISCOVERY



**echo "1" > /proc/sys/net/ipv4/icmp_echo_ignore_all*

BASIC SCANNING

HOST DISCOVERY OPTIONS

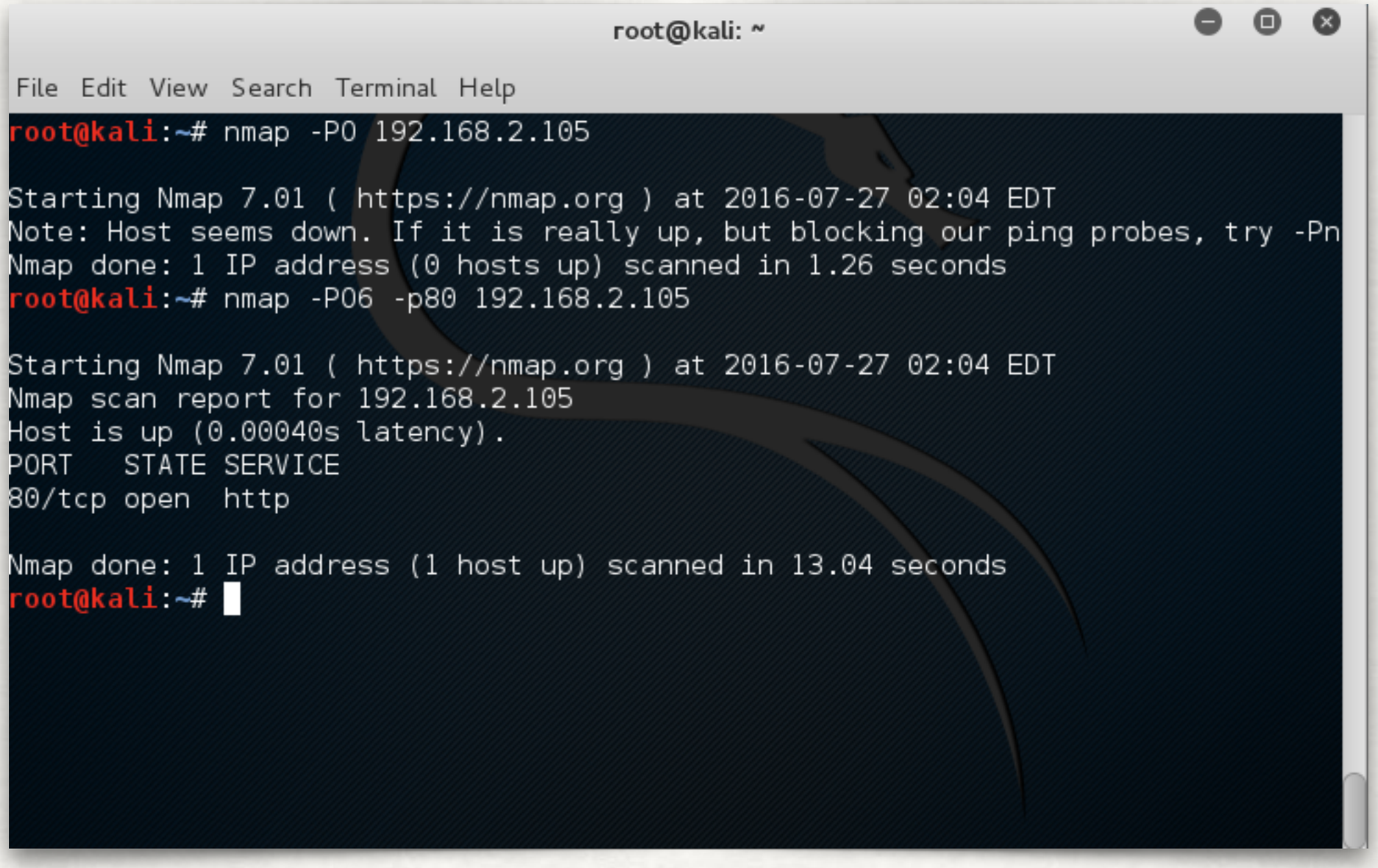
- -PO [protocol] [list] (IP Protocol Ping) - This option sends IP packets with the specified protocol number set in their IP header. If no protocols are specified, the default is to send multiple IP packets for ICMP (protocol 1), IGMP (protocol 2), and IP-in-IP (protocol 4)

- -PR (ARP Ping) - One of the most common Nmap usage scenarios is to scan an ethernet LAN, even if different ping types (such as -PE or -PS) are specified, Nmap uses ARP instead for any of the targets which are on the same LAN.

- --disable-arp-ping (No ARP or ND Ping)

BASIC SCANNING

HOST DISCOVERY



**Note that for the ICMP, IGMP, TCP (protocol 6), UDP (protocol 17)*

BASIC SCANNING

HOST DISCOVERY OPTIONS

- —traceroute - Traceroutes are performed post-scan using information from the scan results to determine the port and protocol most likely to reach the target. It works with all scan types except connect scans (-sT) and idle scans (-sI).

  Traceroute works by sending packets with a low TTL (time-to-live) in an attempt to elicit ICMP Time Exceeded messages from intermediate hops between the scanner and the target host. Standard traceroute implementations start with a TTL of 1 and increment the TTL until the destination host is reached. Nmap's traceroute starts with a high TTL and then decrements the TTL until it reaches zero. Doing it backwards lets Nmap employ clever caching algorithms to speed up traces over multiple hosts.

BASIC SCANNING

HOST DISCOVERY

```
bash-3.2# nmap --traceroute pgorelease.nianticlabs.com

Starting Nmap 7.00 ( https://nmap.org ) at 2016-07-27 13:27 WIB
Nmap scan report for pgorelease.nianticlabs.com (130.211.14.80)
Host is up (0.098s latency).
rDNS record for 130.211.14.80: 80.14.211.130.bc.googleusercontent.com
Not shown: 997 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
8080/tcp open  http-proxy

TRACEROUTE (using port 443/tcp)
HOP RTT       ADDRESS
1   92.09 ms  192.168.1.1
2   ...
3   153.71 ms 10.1.12.50
4   153.74 ms 61.1.1.1
5   158.62 ms lynx-static-116-68-229-45.lynx.net.id (116.68.229.45)
6   154.96 ms fm-dyn-111-95-244-86.fast.net.id (111.95.244.86)
7   154.49 ms 108.170.240.33
8   153.94 ms 108.170.234.225
9   154.00 ms 80.14.211.130.bc.googleusercontent.com (130.211.14.80)

Nmap done: 1 IP address (1 host up) scanned in 30.64 seconds
bash-3.2#
```

BASIC SCANNING

HOST DISCOVERY OPTIONS

- -n (No DNS resolution) - Tells Nmap to never do reverse DNS resolution on the active IP addresses it finds. Since DNS can be slow even with Nmap's built-in parallel stub resolver, this option can slash scanning times.

- -R (DNS resolution for all targets) . - Tells Nmap to always do reverse DNS resolution on the target IP addresses. Normally reverse DNS is only performed against responsive (online) hosts.

- --system-dns (Use system DNS resolver) - Specify this option to use your system resolver instead (one IP at a time via the getnameinfo call). This is slower and rarely useful.

- --dns-servers server1[,server2[,...]] (Servers to use for reverse DNS queries) . By default, Nmap determines your DNS servers (for rDNS resolution) from your resolv.conf file (Unix) or the Registry (Win32).

BASIC SCANNING

HOST DISCOVERY

```
bash-3.2# nmap --traceroute -n pgorelease.nianticlabs.com

Starting Nmap 7.00 ( https://nmap.org ) at 2016-07-27 13:33 WIB
Nmap scan report for pgorelease.nianticlabs.com (130.211.14.80)
Host is up (0.085s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
8080/tcp open  http-proxy

TRACEROUTE (using port 443/tcp)
HOP RTT       ADDRESS
1   80.39 ms  192.168.1.1
2   ...
3   135.64 ms 10.1.12.50
4   135.21 ms 61.1.1.1
5   146.14 ms 116.68.231.237
6   135.87 ms 111.95.244.86
7   143.40 ms 108.170.240.97
8   143.63 ms 108.170.234.225
9   144.10 ms 130.211.14.80

Nmap done: 1 IP address (1 host up) scanned in 10.99 seconds
bash-3.2#
```

BASIC SCANNING

PORT SCAN

- Nmap simple command scans 1,000 TCP ports on the host target.
- Nmap divides ports into six states: open, closed, filtered, unfiltered, open|filtered, or closed|filtered.

BASIC SCANNING

PORT SCAN

```
root@kali:~# head -n 50 /usr/share/nmap/nmap-services
# THIS FILE IS GENERATED AUTOMATICALLY FROM A MASTER - DO NOT EDIT.
# EDIT /nmap-private-dev/nmap-services-all IN SVN INSTEAD.
# Well known service port numbers -*- mode: fundamental; -*-
# From the Nmap Security Scanner ( http://nmap.org )
#
# $Id: nmap-services 35292 2015-10-02 07:52:30Z fyodor $
#
# Derived from IANA data and our own research
#
# This collection of service data is (C) 1996-2011 by Insecure.Com
# LLC.  It is distributed under the Nmap Open Source license as
# provided in the COPYING file of the source distribution or at
# http://nmap.org/data/COPYING .  Note that this license
# requires you to license your own work under a compatable open source
# license.  If you wish to embed Nmap technology into proprietary
# software, we sell alternative licenses (contact sales@insecure.com).
# Dozens of software vendors already license Nmap technology such as
# host discovery, port scanning, OS detection, and version detection.
# For more details, see http://nmap.org/book/man-legal.html
#
# Fields in this file are: Service name, portnum/protocol, open frequency, optional comments
#
tcpmux  1/tcp   0.001995        # TCP Port Service Multiplexer [rfc-1078]
tcpmux  1/udp   0.001236        # TCP Port Service Multiplexer
compressnet     2/tcp   0.000013        # Management Utility
compressnet     2/udp   0.001845        # Management Utility
compressnet     3/tcp   0.001242        # Compression Process
compressnet     3/udp   0.001532        # Compression Process
unknown 4/tcp   0.000477
rje     5/udp   0.000593        # Remote Job Entry
unknown 6/tcp   0.000502
echo    7/sctp  0.000000
echo    7/tcp   0.004855
echo    7/udp   0.024679
unknown 8/tcp   0.000013
```

BASIC SCANNING

PORT SCAN STATE: OPEN

- An application is actively accepting TCP connections, UDP datagrams or SCTP associations on this port.
- Finding these is often the primary goal of port scanning.
- Security-minded people know that each open port is an avenue for attack. Attackers and pen-testers want to exploit the open ports, while administrators try to close or protect them with firewalls without thwarting legitimate users.
- Open ports are also interesting for non-security scans because they show services available for use on the network.

BASIC SCANNING

PORT SCAN STATE: OPEN

```
root@kali:~# nmap -p21 192.168.176.159

Starting Nmap 7.01 ( https://nmap.org ) at 2016 07 27 03:13 EDT
Nmap scan report for 192.168.176.159
Host is up (0.00088s latency).
PORT   STATE SERVICE
21/tcp open  ftp
MAC Address: 00:0C:29:83:ED:59 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds
```

BASIC SCANNING

PORT SCAN STATE: CLOSED

- A closed port is accessible (it receives and responds to Nmap probe packets), but there is no application listening on it.
- They can be helpful in showing that a host is up on an IP address (host discovery, or ping scanning), and as part of OS detection. Because closed ports are reachable, it may be worth scanning later in case some open up.

BASIC SCANNING

PORT SCAN STATE: FILTERED

- Nmap cannot determine whether the port is open because packet filtering prevents its probes from reaching the port. The filtering could be from a dedicated firewall device, router rules, or host-based firewall software.

- These ports frustrate attackers because they provide so little information. Sometimes they respond with ICMP error messages such as type 3 code 13 (destination unreachable: communication administratively prohibited), but filters that simply drop probes without responding are far more common. This forces Nmap to retry several times just in case the probe was dropped due to network congestion rather than filtering.

- This slows down the scan dramatically.

BASIC SCANNING

PORT SCAN STATE: FILTERED

```
root@kali:~# nmap -p21 192.168.176.159

Starting Nmap 7.01 ( https://nmap.org ) at 2016 07 27 03:13 EDT
Nmap scan report for 192.168.176.159
Host is up (0.00088s latency).
PORT   STATE SERVICE
21/tcp open  ftp
MAC Address: 00:0C:29:83:ED:59 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds
root@kali:~# nmap -p21 192.168.176.159

Starting Nmap 7.01 ( https://nmap.org ) at 2016 07 27 03:13 EDT
Nmap scan report for 192.168.176.159
Host is up (0.0011s latency).
PORT   STATE    SERVICE
21/tcp filtered ftp
MAC Address: 00:0C:29:83:ED:59 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.26 seconds
```

BASIC SCANNING

PORT SCAN STATE: UNFILTERED

- The unfiltered state means that a port is accessible, but Nmap is unable to determine whether it is open or closed.
- Only the ACK scan, which is used to map firewall rulesets, classifies ports into this state.
- Scanning unfiltered ports with other scan types such as Window scan, SYN scan, or FIN scan, may help resolve whether the port is open.

PORT SCANNING TECHNIQUES

PORT SCAN STATE: UNFILTERED

```
bash-3.2# nmap -sA -Pn 192.168.176.226

Starting Nmap 7.00 ( https://nmap.org ) at 2016-07-27 21:41 WIB
Nmap scan report for 192.168.176.226
Host is up (0.00010s latency).
All 1000 scanned ports on 192.168.176.226 are unfiltered
MAC Address: 00:0C:29:BA:E6:DD (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.24 seconds
bash-3.2#
```

BASIC SCANNING

PORT SCAN STATE: OPEN|FILTERED

- Nmap places ports in this state when it is unable to determine whether a port is open or filtered.
- This occurs for scan types in which open ports give no response. The lack of response could also mean that a packet filter dropped the probe or any response it elicited.
- So Nmap does not know for sure whether the port is open or being filtered. The UDP, IP protocol, FIN, NULL, and Xmas scans classify ports this way.

BASIC SCANNING

PORT SCAN STATE: OPEN|FILTERED

```
root@kali:~# nmap -p21 192.168.176.159

Starting Nmap 7.01 ( https://nmap.org ) at 2016 07 27 03:18 EDT
Nmap scan report for 192.168.176.159
Host is up (0.00088s latency).
PORT   STATE SERVICE
21/tcp open  ftp
MAC Address: 00:0C:29:83:ED:59 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds
root@kali:~# nmap -p21 192.168.176.159

Starting Nmap 7.01 ( https://nmap.org ) at 2016 07 27 03:18 EDT
Nmap scan report for 192.168.176.159
Host is up (0.0011s latency).
PORT   STATE    SERVICE
21/tcp filtered ftp
MAC Address: 00:0C:29:83:ED:59 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.26 seconds
root@kali:~# nmap -p21 -sX 192.168.176.159

Starting Nmap 7.01 ( https://nmap.org ) at 2016 07 27 03:19 EDT
Nmap scan report for 192.168.176.159
Host is up (0.0026s latency).
PORT   STATE         SERVICE
21/tcp open filtered ftp
MAC Address: 00:0C:29:83:ED:59 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.26 seconds
root@kali:~#
```

BASIC SCANNING

PORT SCAN STATE: CLOSED|FILTERED

- This state is used when Nmap is unable to determine whether a port is closed or filtered.
- It is only used for the IP ID idle scan.

BASIC SCANNING

PORT SCANNING TECHNIQUES

- Port scan techniques supported by Nmap
- Only one method may be used at a time, except that UDP scan (-sU) and any one of the SCTP scan types (-sY, -sZ) may be combined with any one of the TCP scan types.
- By default, Nmap performs a SYN Scan, though it substitutes a connect scan if the user does not have proper privileges to send raw packets (requires root access on Unix)

PORT SCANNING TECHNIQUES

SYN SCAN

- -sS, (TCP SYN scan)
- The TCP SYN scan is the default option for privileged users
- SYN scan is the default and most popular scan option for good reasons. It can be performed quickly, scanning thousands of ports per second on a fast network not hampered by restrictive firewalls.
- This technique is often referred to as half-open scanning, because you don't open a full TCP connection. You send a SYN packet, as if you are going to open a real connection and then wait for a response.
- A SYN/ACK indicates the port is listening (open), while a RST (reset) is indicative of a non-listener. If no response is received after several retransmissions, the port is marked as filtered.

PORT SCANNING TECHNIQUES

TCP SCAN

- -sT, (TCP Connect scan)
- TCP connect scan is the default TCP scan type when SYN scan is not an option. This is the case when a user does not have raw packet privileges.
- Nmap asks the underlying operating system to establish a connection with the target
- This scans take longer and require more packets to obtain the same information, but target machines are more likely to log the connection.

PORT SCANNING TECHNIQUES

SYN SCAN

```
raiser:~ ammar$ nmap -sS 192.168.176.159
You requested a scan type which requires root privileges.
QUITTING!
raiser:~ ammar$ nmap -sA 192.168.176.159
You requested a scan type which requires root privileges.
QUITTING!
raiser:~ ammar$ nmap -sT 192.168.176.159

Starting Nmap 7.00 ( https://nmap.org ) at 2016-07-27 21:21 WIB
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.08 seconds
raiser:~ ammar$ nmap -sT -Pn 192.168.176.159

Starting Nmap 7.00 ( https://nmap.org ) at 2016-07-27 21:22 WIB
Nmap scan report for 192.168.176.159
Host is up (0.00099s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE
2869/tcp open  icslap

Nmap done: 1 IP address (1 host up) scanned in 128.21 seconds
raiser:~ ammar$
```

PORT SCANNING TECHNIQUES

UDP SCAN

- -sU, (UDP scan)
- UDP scanning is generally slower and more difficult than TCP, but widely usage services are deployed using this protocol (DNS, SNMP, and DHCP)
- UDP scan works by sending a UDP packet to every targeted port.
- Occasionally, a service will respond with a UDP packet, proving that it is open. If no response is received after retransmissions, the port is classified as openlfiltered.

PORT SCANNING TECHNIQUES

UDP SCAN

```
raiser:~ ammar$ nmap -sU -Pn 192.168.176.159
You requested a scan type which requires root privileges.
QUITTING!
raiser:~ ammar$ sudo -s
Password:
bash-3.2# nmap -sU -Pn 192.168.176.159

Starting Nmap 7.00 ( https://nmap.org ) at 2016-07-27 21:29 WIB
Nmap scan report for 192.168.176.159
Host is up (0.00056s latency).
Not shown: 999 open|filtered ports
PORT    STATE SERVICE
137/udp open  netbios-ns
MAC Address: 00:0C:29:83:ED:69 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 28.33 seconds
bash-3.2#
```

PORT SCANNING TECHNIQUES

TCP NULL, FIN, AND XMAS SCANS

- -sN; -sF; -sX (TCP NULL, FIN, and Xmas scans)
- These three scan types (even more are possible with the --scanflags option described in the next section) exploit a subtle loophole in the TCP RFC to differentiate between open and closed ports.
- When scanning systems compliant with this RFC text, any packet not containing SYN, RST, or ACK bits will result in a returned RST if the port is closed and no response at all if the port is open. As long as none of those three bits are included, any combination of the other three (FIN, PSH, and URG) are OK.

PORT SCANNING TECHNIQUES

TCP ACK SCAN

- -sA (TCP ACK scan)
- This scan is different than the others discussed so far in that it never determines open (or even openlfiltered) ports. It is used to map out firewall rulesets, determining whether they are stateful or not and which ports are filtered.
- The ACK scan probe packet has only the ACK flag set (unless you use --scanflags). When scanning unfiltered systems, open and closed ports will both return a RST packet. Nmap then labels them as unfiltered, meaning that they are reachable by the ACK packet, but whether they are open or closed is undetermined. Ports that don't respond, or send certain ICMP error messages back (type 3, code 0, 1, 2, 3, 9, 10, or 13), are labeled filtered.

PORT SCANNING TECHNIQUES

TCP ACK SCAN

```
bash-3.2# nmap -sA -Pn 192.168.176.226

Starting Nmap 7.00 ( https://nmap.org ) at 2016-07-27 21:41 WIB
Nmap scan report for 192.168.176.226
Host is up (0.00010s latency).
All 1000 scanned ports on 192.168.176.226 are unfiltered
MAC Address: 00:0C:29:BA:E6:DD (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.24 seconds
bash-3.2#
```

PORT SCANNING TECHNIQUES

FTP BOUNCE SCAN

- -b FTP relay host (FTP bounce scan) .
- This scan is different than the others discussed so far in that it never determines open (or even openlfiltered) ports. It is used to map out firewall rulesets, determining whether they are stateful or not and which ports are filtered.
- The ACK scan probe packet has only the ACK flag set (unless you use --scanflags). When scanning unfiltered systems, open and closed ports will both return a RST packet. Nmap then labels them as unfiltered, meaning that they are reachable by the ACK packet, but whether they are open or closed is undetermined. Ports that don't respond, or send certain ICMP error messages back (type 3, code 0, 1, 2, 3, 9, 10, or 13), are labeled filtered.

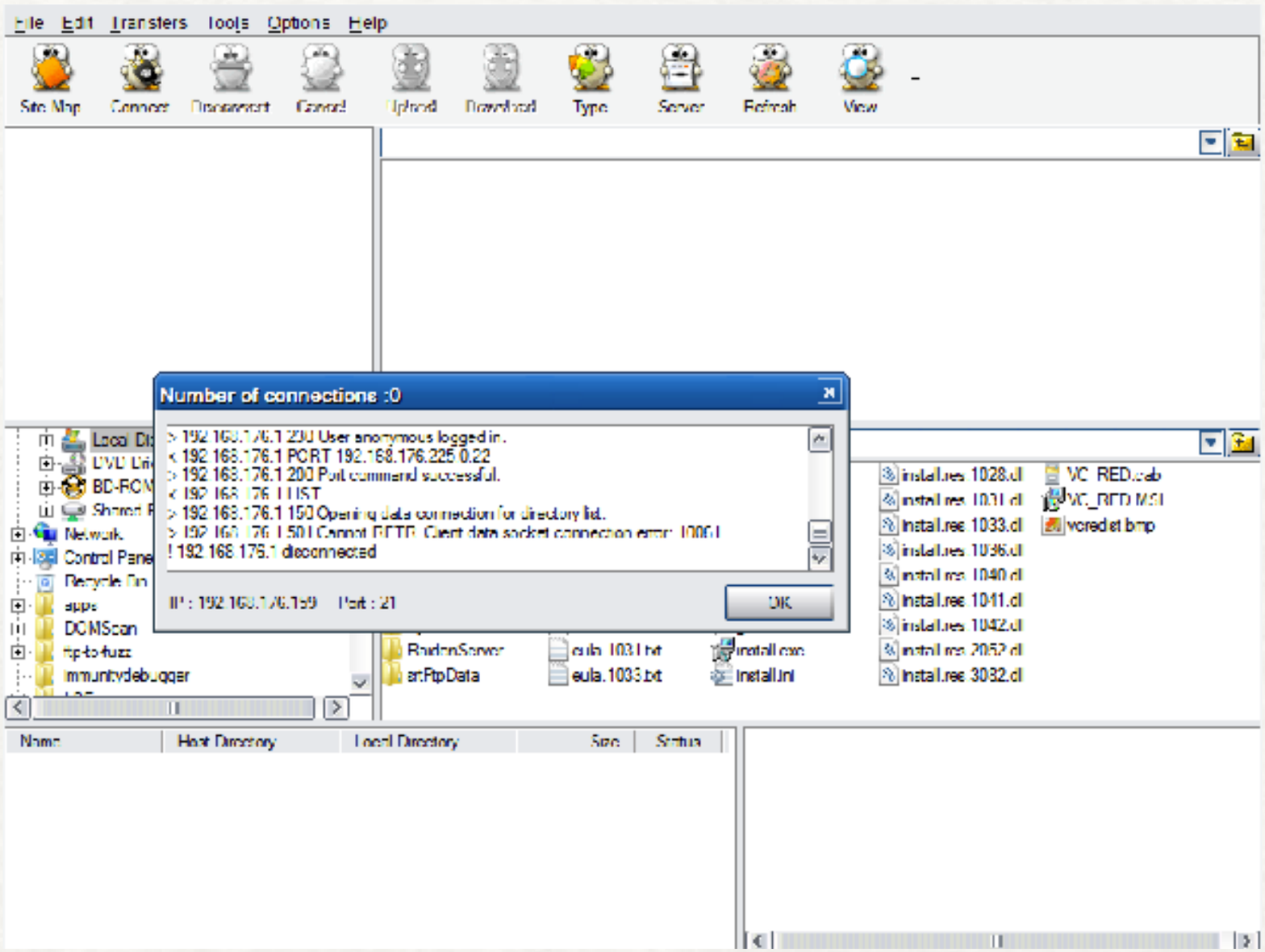
BASIC SCANNING

PORT SCANNING TECHNIQUES

```
bash-3.2# nmap -Pn -p21 -b anonymous:test@192.168.176.159 127.0.0.1

Starting Nmap 7.00 ( https://nmap.org ) at 2016-07-27 17:27 WIB
Nmap scan report for raiser (127.0.0.1)
Host is up.
PORT   STATE SERVICE
21/tcp open  ftp

Nmap done: 1 IP address (1 host up) scanned in 9.11 seconds
bash-3.2# nmap -Pn -p22 -b anonymous:test@192.168.176.159 192.168.176.225

Starting Nmap 7.00 ( https://nmap.org ) at 2016-07-27 17:27 WIB
Nmap scan report for 192.168.176.225
Host is up.
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 10.13 seconds
bash-3.2#
```

BASIC SCANNING

PORT SCANNING TECHNIQUES



BASIC SCANNING

PORT SPECIFICATION AND SCAN ORDER

- Nmap offers options for specifying which ports are scanned and whether the scan order is randomized or sequential.
- By default, Nmap scans the most common 1,000 ports for each protocol.

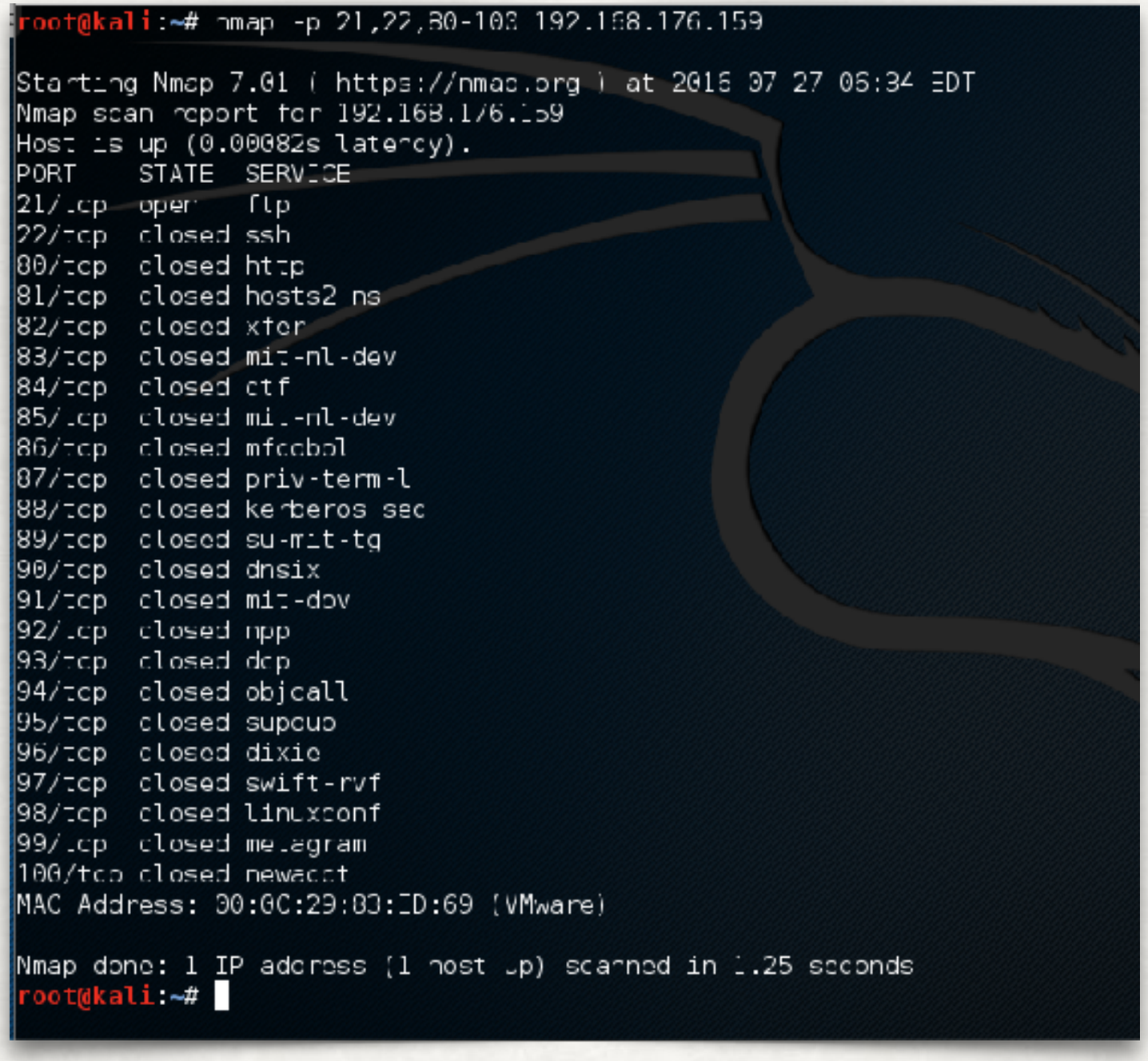
BASIC SCANNING

PORT SPECIFICATION AND SCAN ORDER

- -p [port]/[ranges] - Only scan specified ports
  - nmap -p 21,22,80-100 192.168.176.159

BASIC SCANNING

PORT SPECIFICATION AND SCAN ORDER



BASIC SCANNING

PORT SPECIFICATION AND SCAN ORDER

- When scanning a combination of protocols (e.g. TCP and UDP), you can specify a particular protocol by preceding the port numbers by T: for TCP, U: for UDP, S: for SCTP, or P: for IP Protocol.

  - nmap -sU -sS -p T:21,22,80-100,U:53,161 192.168.176.159

BASIC SCANNING

PORT SPECIFICATION AND SCAN ORDER

```
root@kali:~# nmap -sU -sS  -p T:21,22,80-100,U:53,161 192.168.176.226

Starting Nmap 7.01 ( https://nmap.org ) at 2016-07-27 09:04 EDT
Nmap scan report for 192.168.176.226
Host is up (0.00027s latency).
PORT    STATE  SERVICE
21/tcp  open   ftp
22/tcp  open   ssh
80/tcp  open   http
81/tcp  closed hosts2-ns
82/tcp  closed xfer
83/tcp  closed mit-ml-dev
84/tcp  closed ctf
85/tcp  closed mit ml dev
86/tcp  closed mfcobol
87/tcp  closed priv-term-l
88/tcp  closed kerberos-sec
89/tcp  closed su-mit-tg
90/tcp  closed crsix
91/tcp  closed mit-dov
92/tcp  closed rpp
93/tcp  closed ccp
94/tcp  closed objcall
95/tcp  closed supdup
96/tcp  closed dixie
97/tcp  closed swift-rvf
98/tcp  closed linuxconf
99/tcp  closed metagram
100/tcp closed newacct
53/udp  open   domain
161/udp closed snmp
MAC Address: 00:0C:29:BA:E6:DD (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.17 seconds
root@kali:~#
```

BASIC SCANNING

PORT SPECIFICATION AND SCAN ORDER

- --exclude-ports port ranges (Exclude the specified ports from scanning) .
  - This option specifies which ports you do want Nmap to exclude from scanning.

BASIC SCANNING

PORT SPECIFICATION AND SCAN ORDER

```
root@kali:~# nmap -p20-100 --exclude-ports 80 192.168.176.226

Starting Nmap 7.01 ( https://nmap.org ) at 2016-07-27 10:58 EDT
Nmap scan report for 192.168.176.226
Host is up (0.00011s latency).
Not shown: 75 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
23/tcp open  telnet
25/tcp open  smtp
53/tcp open  domain
MAC Address: 00:0C:29:BA:E6:DD (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.08 seconds
root@kali:~# nmap -p80 192.168.176.226

Starting Nmap 7.01 ( https://nmap.org ) at 2016-07-27 10:59 EDT
Nmap scan report for 192.168.176.226
Host is up (0.00036s latency).
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 00:0C:29:BA:E6:DD (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.06 seconds
root@kali:~#
```

BASIC SCANNING

PORT SPECIFICATION AND SCAN ORDER

- -F (Fast (limited port) scan)

Normally Nmap scans the most common 1,000 ports for each scanned protocol. With -F, this is reduced to 100.

BASIC SCANNING

PORT SPECIFICATION AND SCAN ORDER

```
Nmap done: 1 IP address (1 host up) scanned in 13.16 seconds
root@kali:~# nmap -F 192.168.1.1

Starting Nmap 7.01 ( https://nmap.org ) at 2016-07-27 18:28 EDT
Nmap scan report for 192.168.1.1
Host is up (0.018s latency).
Not shown: 97 filtered ports
PORT   STATE SERVICE
21/tcp open  ftp
23/tcp open  telnet
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 7.12 seconds
root@kali:~#
```

```
root@kali:~# nmap 192.168.1.1

Starting Nmap 7.01 ( https://nmap.org ) at 2016-07-27 18:27 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0019s latency).
Not shown: 997 filtered ports
PORT   STATE SERVICE
21/tcp open  ftp
23/tcp open  telnet
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 17.03 seconds
root@kali:~#
```

BASIC SCANNING

PORT SPECIFICATION AND SCAN ORDER

- -r (Don't randomize ports)

By default, Nmap randomizes the scanned port order (except that certain commonly accessible ports are moved near the beginning for efficiency reasons). This randomization is normally desirable, but you can specify -r for sequential (sorted from lowest to highest) port scanning instead.

BASIC SCANNING

PORT SPECIFICATION AND SCAN ORDER

```
root@kali:~# nmap -r 192.168.1.1

Starting Nmap 7.01 ( https://nmap.org ) at 2016-07-27 18:48 EDT
Nmap scan report for 192.168.1.1
Host is up (0.059s latency).
Not shown: 997 filtered ports
PORT   STATE SERVICE
21/tcp open  ftp
23/tcp open  telnet
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 21.67 seconds
root@kali:~#
 File  Edit  View  Search  Terminal  Help
```

BASIC SCANNING

PORT SPECIFICATION AND SCAN ORDER

- --top-ports n

Scans the n highest-ratio ports found in nmap-services file after excluding all ports specified by --exclude-ports. n must be 1 or greater.

BASIC SCANNING

PORT SPECIFICATION AND SCAN ORDER

```
root@kali:~# nmap --top-ports 10 192.168.176.226

Starting Nmap 7.01 ( https://nmap.org ) at 2016-07-27 20:05 EDT
Nmap scan report for 192.168.176.226
Host is up (0.0011s latency).
PORT     STATE  SERVICE
21/tcp   open   ftp
22/tcp   open   ssh
23/tcp   open   telnet
25/tcp   open   smtp
80/tcp   open   http
110/tcp  closed pop3
139/tcp  open   netbios-ssn
443/tcp  closed https
445/tcp  open   microsoft-ds
3389/tcp closed ms-wbt-server
MAC Address: 00:0C:29:BA:E6:DD (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.13 seconds
root@kali:~#
```

BASIC SCANNING

SERVICE AND VERSION DETECTION

- Even if Nmap is right, and the hypothetical server above is running SMTP, HTTP, and DNS servers, that is not a lot of information. Having an accurate version number helps dramatically in determining which exploits a server is vulnerable to.

- Version detection helps to obtain service and version information.

BASIC SCANNING

SERVICE AND VERSION DETECTION

- After TCP and/or UDP ports are discovered using one of the other scan methods, version detection interrogates those ports to determine more about what is actually running.

- The nmap-service-probes, database contains probes for querying various services and match expressions to recognize and parse responses. Nmap tries to determine the service protocol (e.g. FTP, SSH, Telnet, HTTP), the application name (e.g. ISC BIND, Apache httpd, Solaris telnetd), the version number, hostname, device type (e.g. printer, router), the OS family (e.g. Windows, Linux).

BASIC SCANNING

SERVICE AND VERSION DETECTION

- -sV (Version detection) .

Enables version detection, as discussed above. Alternatively, you can use -A, which enables version detection among other things.

--allports (Don't exclude any ports from version detection) .

By default, Nmap version detection skips TCP port 9100 because some printers simply print anything sent to that port, leading to dozens of pages of HTTP GET requests, binary SSL session requests, etc. This behavior can be changed by modifying or removing the Exclude directive in nmap-service-probes, or you can specify --allports to scan all ports regardless of any Exclude directive.

BASIC SCANNING

PORT SPECIFICATION AND SCAN ORDER

```
root@kali:~# nmap -sV 192.168.176.226

Starting Nmap 7.01 ( https://nmap.org ) at 2016-07-27 20:19 EDT
Nmap scan report for 192.168.176.226
Host is up (0.00015s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell       Netkit rshd
1099/tcp open  rmiregistry GNU Classpath grmiregistry
1524/tcp open  shell       Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:BA:C6:DD (VMware)
Service Info: Hosts:  metasploitable.localdomain, localhost, irc.Metasploitable.LAN; OSs: Unix, Linux;
CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 32.33 seconds
root@kali:~#
```

BASIC SCANNING

OS DETECTION

- One of Nmap's best-known features is remote OS detection using TCP/IP stack fingerprinting.
- Nmap sends a series of TCP and UDP packets to the remote host and examines practically every bit in the responses. After performing dozens of tests such as TCP ISN sampling, TCP options support and ordering, IP ID sampling, and the initial window size check, Nmap compares the results to its nmap-os-db.

BASIC SCANNING

OS DETECTION

```
root@kali:~# head -n 50 /usr/share/nmap/nmap-os-db
# Nmap OS Fingerprinting 2nd Generation DB. -*- mode: fundamental; -*-
# $Id: nmap-os-db 35497 2015-11-20 04:26:25Z dmiller $
#
# Contributions to this database are welcome.  If Nmap obtains a new
# fingerprint (and test conditions are favorable), it will print out a
# URL you can use to submit the fingerprint.  If Nmap guesses wrong,
# please see https://nmap.org/submit/ .
#
# By submitting fingerprints you are transfering any and all copyright
# interest in the data to Insecure.Com LLC so it can be modified,
# incorporated into Nmap, relicensed, etc.
#
# This collection of fingerprint data is (C) 1996-2010 by Insecure.Com
# LLC.  It is distributed under the Nmap Oper Source license as
# provided in the COPYING file of the source distribution or at
# https://nmap.org/data/COPYING .  Note that this license
# requires you to license your own work under a compatible open source
# license.  If you wish to embed Nmap technology into proprietary
# software, we sell alternative licenses (contact sales@insecure.com).
# Dozens of software vendors already license Nmap technology such as
# host discovery, port scanning, OS detection, and version detection.
# For more details, see https://nmap.org/book/man-legal.html
#
# For a complete description of Nmap OS detection and the format of
# fingerprints in this file, see https://nmap.org/book/osdetect.html.

# This first element provides the number of points every fingerprint
# test is worth.  Tests like TTL or Don't fragment are worth less
# (individually) because there are so many of them and the values are
# often correlated with each other.  Meanwhile, elements such as IS
# (TCP timestamp) which are only used once, get more points.  Points
# are used when there are no perfect matches to determine which OS
# fingerprint matches a target machine most closely.
MatchPoints
SEQ(SP=25%GCD=75%ISR=25%TI=100%CI=50%II=100%SS=80%TS=100)
OPS(O1=20%O2=20%O3=20%O4=20%O5=20%O6=20)
WIN(W1=15%W2=15%W3=15%W4=15%W5=15%W6=15)
```

BASIC SCANNING

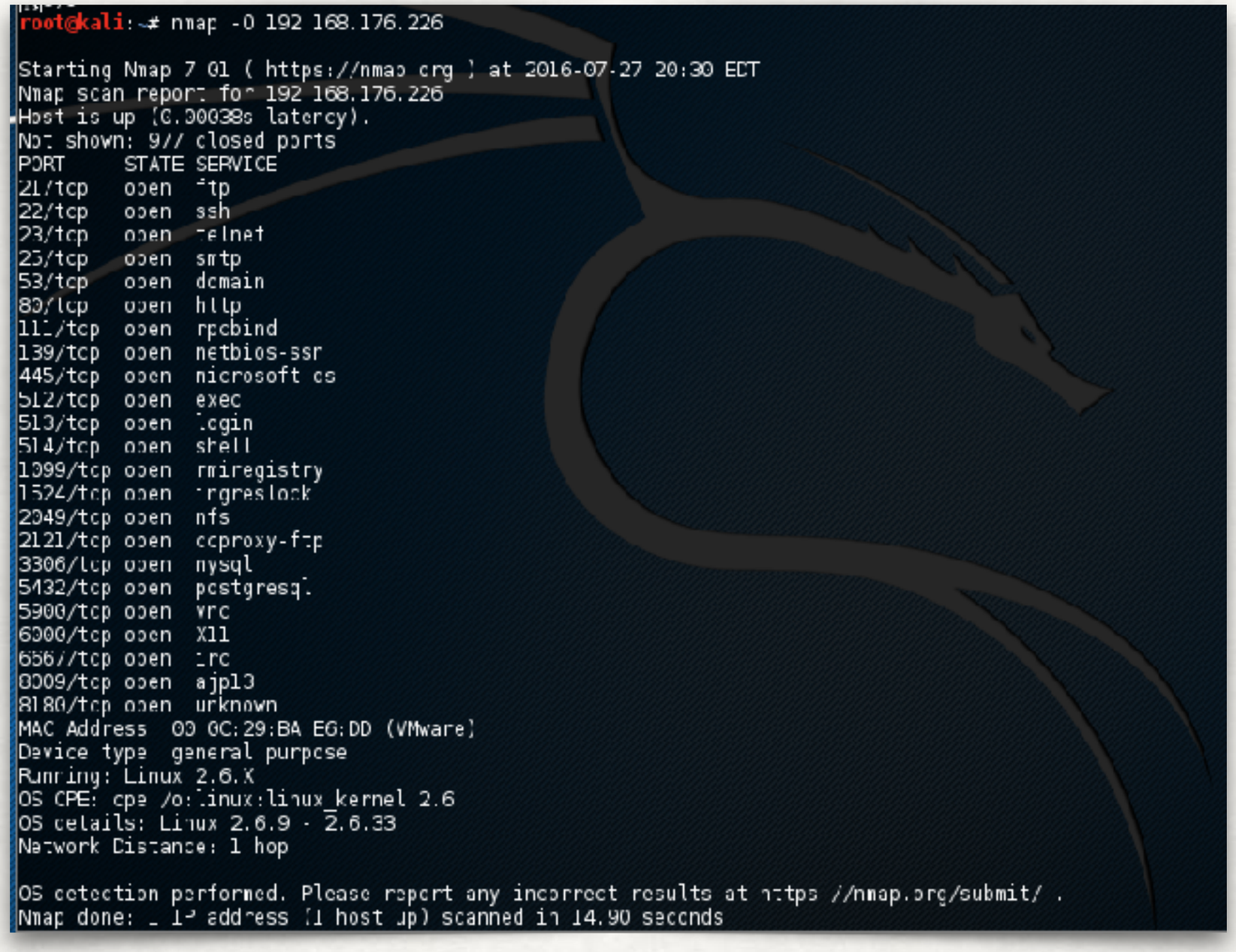
OS DETECTION

- -O (Enable OS detection) .

Enables OS detection, as discussed above. Alternatively, you can use -A to enable OS detection along with other things.

BASIC SCANNING

OS DETECTION



BASIC SCANNING

OS DETECTION

```
root@kali:~# nmap -O 192.168.176.159

Starting Nmap 7.01 ( https://nmap.org ) at 2016-07-27 20:33 EDT
Nmap scan report for 192.168.176.159
Host is up (0.00068s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE
2869/tcp open  icslap
MAC Address: 00:0C:29:83:ED:69 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1
 closed port
Device type: general purpose|specialized|phone
Running: Microsoft Windows 2008|7|Phone|Vista
OS CPE: cpe:/o:microsoft:windows_server_2008::beta3 cpe:/o:microsoft:windows_server_2008
cpe:/o:microsoft:windows_7::-:professional cpe:/o:microsoft:windows_8 cpe:/o:microsoft:wi
ndows_7 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windo
ws_vista::sp1
OS details: Microsoft Windows Server 2008 or 2008 Beta 3, Windows Server 2008 R2, Microso
ft Windows 7 Professional or Windows 8, Microsoft Windows Embedded Standard 7, Microsoft
Windows Phone 7.5 or 8.0, Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or
 Windows 7, Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 38.84 seconds
```

BASIC SCANNING

OS DETECTION

--osscan-limit (Limit OS detection to promising targets) .

OS detection is far more effective if at least one open and one closed TCP port are found. Set this option and Nmap will not even try OS detection against hosts that do not meet this criteria. This can save substantial time, particularly on -Pn scans against many hosts. It only matters when OS detection is requested with -O or -A.

--osscan-guess; --fuzzy (Guess OS detection results) .

When Nmap is unable to detect a perfect OS match, it sometimes offers up near-matches as possibilities. The match has to be very close for Nmap to do this by default. Either of these (equivalent) options make Nmap guess more aggressively. Nmap will still tell you when an imperfect match is printed and display its confidence level (percentage) for each guess.

BASIC SCANNING

OS DETECTION

```
root@kali:~# nmap -O 192.168.176.159 --osscan-limit

Starting Nmap 7.01 ( https://nmap.org ) at 2016-07-27 23:37 EDT
Nmap scan report for 192.168.176.159
Host is up (0.0020s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE
2869/tcp open  icslap
MAC Address: 00:0C:29:83:ED:69 (VMware)

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 29.74 seconds
root@kali:~# nmap -O 192.168.176.159 --osscan-guess

Starting Nmap 7.01 ( https://nmap.org ) at 2016-07-27 23:38 EDT
Nmap scan report for 192.168.176.159
Host is up (0.013s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE
2869/tcp open  icslap
MAC Address: 00:0C:29:83:ED:69 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1
 closed port
Device type: general purpose
Running: Microsoft Windows Vista
OS CPE: cpe:/o:microsoft:windows_vista::sp1:home_premium
OS details: Microsoft Windows Vista Home Premium SP1
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 42.35 seconds
root@kali:~#
```

REFERENCE

- NMAP Manual
- NMAP Online book (free content) - https://nmap.org/book/