Xprobe2

Xprobe2是一款远程主机系统探查工具，可通过ICMP协议来获取指纹等信息。

——by Ofir Arkin, Fyodor Yarochkin

一，帮助手册

Xprobe2 v.0.3 Copyright (c) 2002-2005 fyodor@o0o.nu, ofir@sys-security.com, meder@o0o.nu
Xprobe2 v.0.3版权所有（c）2002-2005 fyodor@o0o.nu，ofir@sys-security.com，meder@o0o.nu

usage: xprobe2 [options] target
使用：xprobe2[选项]目标

Options:

选项：

-v   Be verbose
-五

-r   Show route to target(traceroute)
-显示到目标的路由（traceroute）

-p proto:portnum:state Specify portnumber, protocol and state.
-pproto:portnum:state指定端口号、协议和状态。

Example: tcp:23:open, UDP:53:CLOSED
示例：tcp:23:打开，UDP:53:关闭

-c <configfile>   Specify config file to use.
-c <config file>指定要使用的配置文件。

-h   Print this help.
打印此帮助。

-o <\fname>   Use logfile to log everything.
-o <fname>使用日志文件记录所有内容。

-t <time_sec>   Set initial receive timeout or roundtrip time.
-t<time_sec>设置初始接收超时或往返时间。

-s <send_delay>   Set packsending delay (milseconds).
-s<send_delay>Set packsending delay（毫秒）。

-d <debuglv>   Specify debugging level.
-指定调试级别。

-D <modnum>   Disable module number <modnum>.
-D <modnum>禁用模块号 <modnum>。

-M <modnum>   Enable module number <modnum>.
-M<modnum>启用模块号<modnum>。

-L Display modules.
显示模块。

-m <numofmatches> Specify number of matches to print.
-m<numofmatches>指定要打印的匹配数。

-T <portspec> Enable TCP portscan for specified port(s).
-T<portspec>为指定端口启用TCP端口扫描。

Example: -T21-23,53,110
示例：-T21-23,53110

-U <portspec> Enable UDP portscan for specified port(s).
-U<portspec>为指定端口启用UDP端口扫描。

-f force fixed round-trip time (-t opt).
强制固定往返时间（-t opt）。

-F Generate signature (use -o to save to a file).
生成签名（使用-o保存到文件）。

-X Generate XML output and save it to logfile specified with -o.
-X生成XML输出并将其保存到用-o指定的日志文件中。

-B Options forces TCP handshake module to try to guess open TCP port
-B选项强制TCP握手模块尝试猜测打开的TCP端口

-A Perform analysis of sample packets gathered during portscan in
在中执行端口扫描期间收集的样本包分析

order to detect suspicious traffic (i.e. transparent proxies,
为了检测可疑流量（即透明代理，

firewalls/NIDSs resetting connections). Use with -T.
防火墙/NIDS重置连接）。与-T一起使用。

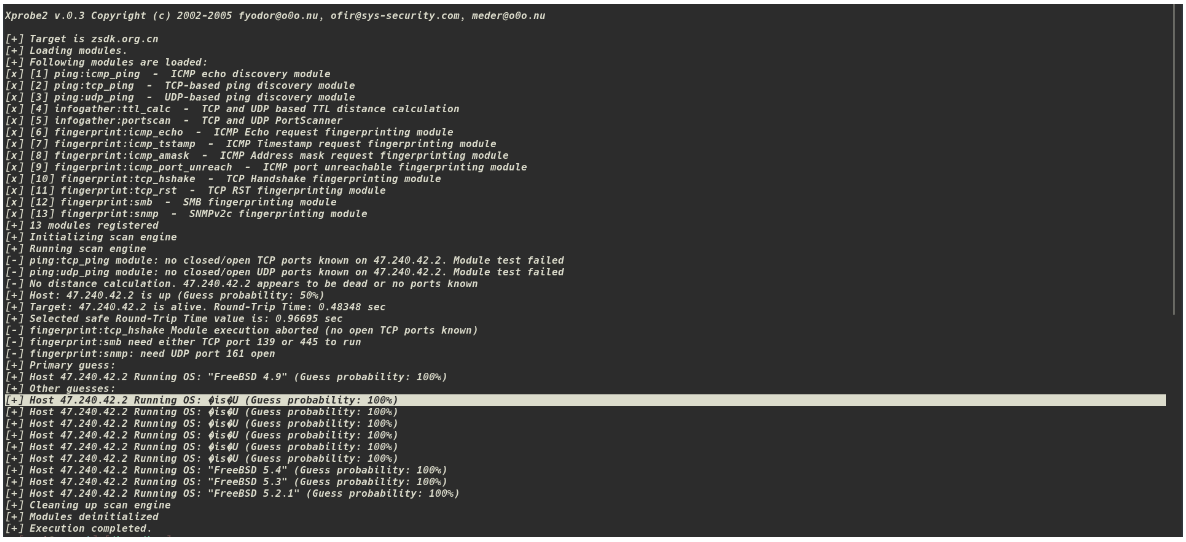
二，模块介绍

类型	EN	描述
PING	ICMP_ping	ICMP回声发现模块
PING	Tcp_ping	基于TCP PING的发现模块
PING	Udp_ping	基于UDP PING的发现模块
信息搜集(infogather)	Ttl_ping	基于TTL PING的TCP/UDP的TTL距离计算模块[^存疑]
信息搜集(infogather)	Portscan	TCP/UDP的端口扫描模块
指纹(fingerprint)	Icmp_echo	ICMP回声请求指纹模块
指纹(fingerprint)	Icmp_tstamp	ICMP时间戳请求模块
指纹(fingerprint)	Icmp_amask	ICMP地址掩码请求指纹模块
指纹(fingerprint)	Icmp_info	ICMP信息打印模块[^存疑]
指纹(fingerprint)	Icmp_port_unreach	ICMP端口无法到达时的指纹打印模块
指纹(fingerprint)	Tcp_hshake	TCP握手指纹模块
指纹(fingerprint)	Tcp_rst	TCP RST指纹模块
指纹(fingerprint)	Smb	SMB指纹模块
指纹(fingerprint)	Snmp	SNMPv2c指纹打印模块

三，命令实例

xprobe2 -b zsdk.org.cn

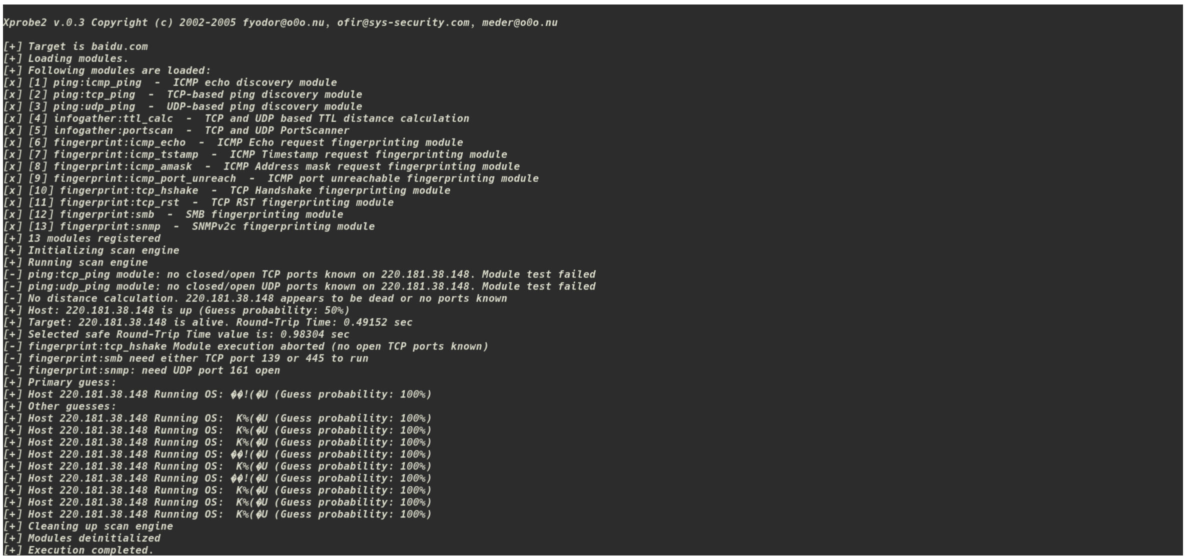
对目标进行详细的扫描



```
Xprobe2 v.0.3 Copyright (c) 2002-2005 fyodor@o0o.nu, ofir@sys-security.com, meder@o0o.nu

[+] Target is zsdk.org.cn
[+] Loading modules.
[+] Following modules are loaded:
[x] [1] ping:icmp_ping  -  ICMP echo discovery module
[x] [2] ping:tcp_ping  -  TCP-based ping discovery module
[x] [3] ping:udp_ping  -  UDP-based ping discovery module
[x] [4] infogather:ttl_calc  -  TCP and UDP based TTL distance calculation
[x] [5] infogather:portscan  -  TCP and UDP PortScanner
[x] [6] fingerprint:icmp_echo  -  ICMP Echo request fingerprinting module
[x] [7] fingerprint:icmp_tstamp  -  ICMP Timestamp request fingerprinting module
[x] [8] fingerprint:icmp_amask  -  ICMP Address mask request fingerprinting module
[x] [9] fingerprint:icmp_port_unreach  -  ICMP port unreachable fingerprinting module
[x] [10] fingerprint:tcp_hshake  -  TCP Handshake fingerprinting module
[x] [11] fingerprint:tcp_rst  -  TCP RST fingerprinting module
[x] [12] fingerprint:smb  -  SMB fingerprinting module
[x] [13] fingerprint:snmp  -  SNMPv2c fingerprinting module
[+] 13 modules registered
[+] Initializing scan engine
[+] Running scan engine
[-] ping:tcp_ping module: no closed/open TCP ports known on 47.240.42.2. Module test failed
[-] ping:udp_ping module: no closed/open UDP ports known on 47.240.42.2. Module test failed
[-] No distance calculation. 47.240.42.2 appears to be dead or no ports known
[+] Host: 47.240.42.2 is up (Guess probability: 50%)
[+] Target: 47.240.42.2 is alive. Round-Trip Time: 0.48348 sec
[+] Selected safe Round-Trip Time value is: 0.96695 sec
[-] fingerprint:tcp_hshake Module execution aborted (no open TCP ports known)
[-] fingerprint:smb need either TCP port 139 or 445 to run
[-] fingerprint:snmp: need UDP port 161 open
[+] Primary guess:
[+] Host 47.240.42.2 Running OS: "FreeBSD 4.9" (Guess probability: 100%)
[+] Other guesses:
[+] Host 47.240.42.2 Running OS: �is�U (Guess probability: 100%)
[+] Host 47.240.42.2 Running OS: �is�U (Guess probability: 100%)
[+] Host 47.240.42.2 Running OS: �is�U (Guess probability: 100%)
[+] Host 47.240.42.2 Running OS: �is�U (Guess probability: 100%)
[+] Host 47.240.42.2 Running OS: �is�U (Guess probability: 100%)
[+] Host 47.240.42.2 Running OS: �is�U (Guess probability: 100%)
[+] Host 47.240.42.2 Running OS: "FreeBSD 5.4" (Guess probability: 100%)
[+] Host 47.240.42.2 Running OS: "FreeBSD 5.3" (Guess probability: 100%)
[+] Host 47.240.42.2 Running OS: "FreeBSD 5.2.1" (Guess probability: 100%)
[+] Cleaning up scan engine
[+] Modules deinitialized
[+] Execution completed.
```

xprobe2 -r baidu.com

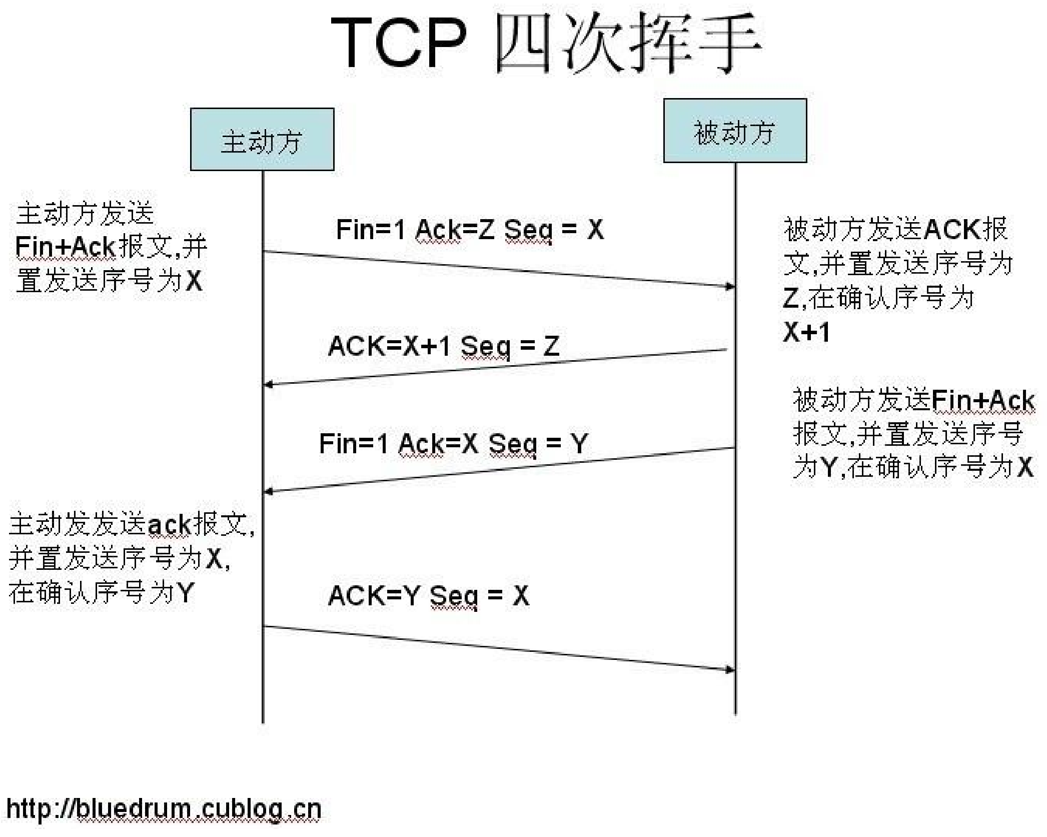
显示目标路径



```
Xprobe2 v.0.3 Copyright (c) 2002-2005 fyodor@o0o.nu, ofir@sys-security.com, meder@o0o.nu

[+] Target is baidu.com
[+] Loading modules.
[+] Following modules are loaded:
[x] [1] ping:icmp_ping  -  ICMP echo discovery module
[x] [2] ping:tcp_ping  -  TCP-based ping discovery module
[x] [3] ping:udp_ping  -  UDP-based ping discovery module
[x] [4] infogather:ttl_calc  -  TCP and UDP based TTL distance calculation
[x] [5] infogather:portscan  -  TCP and UDP PortScanner
[x] [6] fingerprint:icmp_echo  -  ICMP Echo request fingerprinting module
[x] [7] fingerprint:icmp_tstamp  -  ICMP Timestamp request fingerprinting module
[x] [8] fingerprint:icmp_amask  -  ICMP Address mask request fingerprinting module
[x] [9] fingerprint:icmp_port_unreach  -  ICMP port unreachable fingerprinting module
[x] [10] fingerprint:tcp_hshake  -  TCP Handshake fingerprinting module
[x] [11] fingerprint:tcp_rst  -  TCP RST fingerprinting module
[x] [12] fingerprint:smb  -  SMB fingerprinting module
[x] [13] fingerprint:snmp  -  SNMPv2c fingerprinting module
[+] 13 modules registered
[+] Initializing scan engine
[+] Running scan engine
[-] ping:tcp_ping module: no closed/open TCP ports known on 220.181.38.148. Module test failed
[-] ping:udp_ping module: no closed/open UDP ports known on 220.181.38.148. Module test failed
[-] No distance calculation. 220.181.38.148 appears to be dead or no ports known
[+] Host: 220.181.38.148 is up (Guess probability: 50%)
[+] Target: 220.181.38.148 is alive. Round-Trip Time: 0.49152 sec
[+] Selected safe Round-Trip Time value is: 0.98304 sec
[-] fingerprint:tcp_hshake Module execution aborted (no open TCP ports known)
[-] fingerprint:smb need either TCP port 139 or 445 to run
[-] fingerprint:snmp: need UDP port 161 open
[+] Primary guess:
[+] Host 220.181.38.148 Running OS: ��!(�U (Guess probability: 100%)
[+] Other guesses:
[+] Host 220.181.38.148 Running OS:  K%(�U (Guess probability: 100%)
[+] Host 220.181.38.148 Running OS:  K%(�U (Guess probability: 100%)
[+] Host 220.181.38.148 Running OS:  K%(�U (Guess probability: 100%)
[+] Host 220.181.38.148 Running OS: ��!(�U (Guess probability: 100%)
[+] Host 220.181.38.148 Running OS:  K%(�U (Guess probability: 100%)
[+] Host 220.181.38.148 Running OS: ��!(�U (Guess probability: 100%)
[+] Host 220.181.38.148 Running OS:  K%(�U (Guess probability: 100%)
[+] Host 220.181.38.148 Running OS:  K%(�U (Guess probability: 100%)
[+] Host 220.181.38.148 Running OS:  K%(�U (Guess probability: 100%)
[+] Cleaning up scan engine
[+] Modules deinitialized
[+] Execution completed.
```

xprobe2 -p tcp:80:open

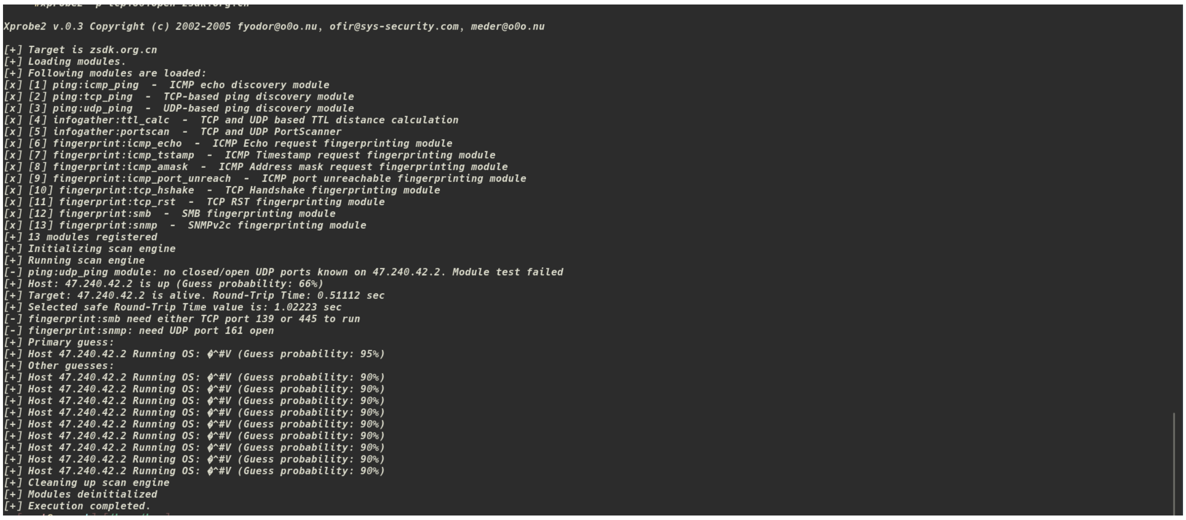
指定端口号为80,协议为TCP，状态为“OPEN打开”

> open，全称“TCP open”其有意思为允许应用程序使用TCP/IP协议与客户端进行通讯。
>
> ---
>
> **四次挥手**
>
> 
>

TCP 四次挥手
> 主动方
> 被动方
> 主动方发送Fin+Ack报文,并置发送序号为X
> Fin=1 Ack=Z Seq = X
> 被动方发送ACK报文,并置发送序号为Z,在确认序号为X+1
> ACK=X+1 Seq = Z
> 被动方发送Fin+Ack报文,并置发送序号为Y,在确认序号为X
> Fin=1 Ack=X Seq = Y
> 主动发发送ack报文,并置发送序号为X,在确认序号为Y
> ACK=Y Seq = X
> http://bluedrum.cublog.cn
>
> TCP连接是双方的，因此需要逐个进行关闭，这原则是当一方完成他的数据发送任务后就可以发送FIN进行关闭这个方向的连接。
>
> 当收到了一个FIN则一味着这一方向的数据没有数据传输了，一个TCP连接在收到了一个FIN后仍然可以继续发送数据。首先关闭的一方将自执行主动挂比，而另一方则是被动关闭。

> 1. 客户端发送了一个FIN，用来关闭服务的请求
> 2. 服务端收到了这个FIN，他发送了一个ACK，表示我已经确认，此时的确认序列号为1，一个FI将占用1个序列号，此时也是和SYN的共同点，SYN也是占用一个序列号。
> 3. 服务端关闭了客户端的连接，发送了一个FIN给客户端
> 4. 客户端返回ACK报文，并将确认号设置为收到的序列号并加1。.
>
> **CLOSED**
>
> 用于表示初始状态
>
> **LISTED**
>
> 表示服务端的某一个SOCKET处于监听状态，告诉对方”我“可以接受连接
>
> **SYN_RCVD**
>
> 表示接受到了SYN报文，在正常的情况喜爱SOCKET在建立连接时的三次握手状态下的一个中间状态。当接收到了客户端的ACK报文后，他会进入到一个ESTABLISHED的状态
>
> **SYN_SENT**
>
> 与SYN_RCVD呼应，当客户端SOCKET执行CONNECTL连接时，首先会发出一个SYN报文，因此随即会进入SYN_SENT状态
>
> **ESTABLISHED**
>
> 用于表示已建立链接
>
> **FIN_WAIT_1**
>
> 等待对方的FIN报文，当SOCKET在ESTABLISHED状态时，想要主动关闭想对方发送了FIN报文，此时SOCKET即进入了FIN_WAIT_1状态
>
> **FIN_WAIT_2**
>
> 表示在FIN_WAIT_2状态下的SOCKET表示半连接，当有一方请求连接close时，告诉对方只是暂时的连接，稍后会关闭
>
> **TIME_WAIT**
>
> 表收收到对方的报文，并发送了ACK报文。之后等待2秒后回到CLOSED可用状态，
>
> 如果在FIN_WAIT_1状态下直接进入到TIME_WAIT状态

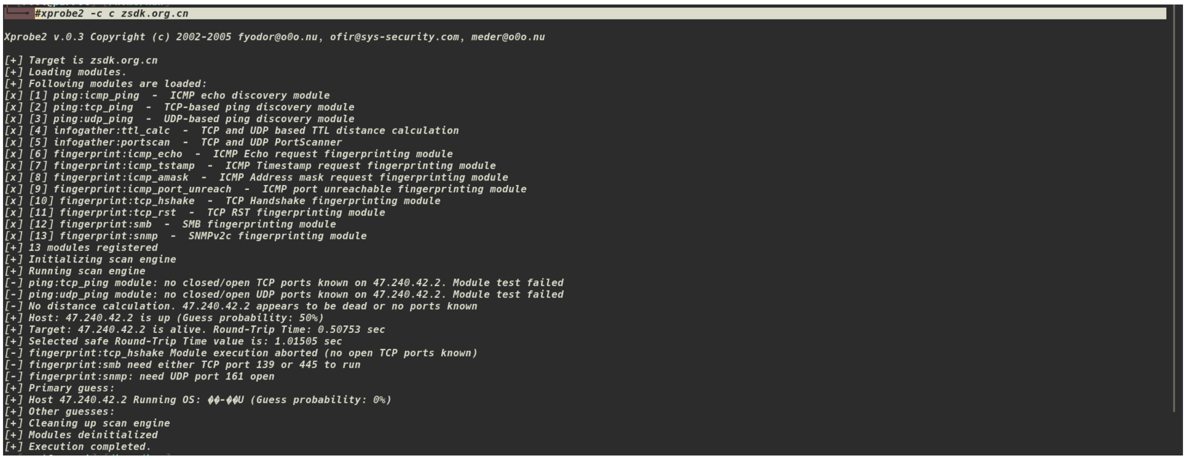
> **CLOSING**
>
> 表示双方都关闭SOCKE连接，双方在同时发送FIN报文的情况下会出现此状况[^双方同时处于CLOSING状状态下]。
>
> 在正常的环境中，发送FIN报文后因先收到对方的ACK报文，然后在发送FIN报文，但是在CLOSING环境下并没有发送ACK报文，但是对方却收到了FIN报文。
>
> **CLOSE_WAIT**
>
> 用于表示等待关闭，当对方关闭一个SOCKET后发送了一个FIN报文给自己，系统会好不留意的发送一个ACK报文给对方，此时会进入CLOSE_WAIT状态
>
> 此时如果没有数据要发送给对方的话，如果没有的话则可关闭这个SOCKET，发送FIN报文个对方也就是说直接关闭了链接，所以在CLOSE_WAIT模式下等待的是关闭链接。
>
> **LAS_ACK**
>
> 表示被动关闭了一方发送的FIN报文后，最后等待对方的ACK报文。当收到了ACK报文后，则可以进入CLOSED初始状态状态。
>
> ---
>
> close，全程“TCP close”即TCP终止，主要分为：
>
> > 半关闭（Half-close）\ 主动关闭（Active close）\ 被动关闭（Passive close）



```
Xprobe2 v.0.3 Copyright (c) 2002-2005 fyodor@o0o.nu, ofir@sys-security.com, meder@o0o.nu

[+] Target is zsdk.org.cn
[+] Loading modules.
[+] Following modules are loaded:
[x] [1] ping:icmp_ping  -  ICMP echo discovery module
[x] [2] ping:tcp_ping  -  TCP-based ping discovery module
[x] [3] ping:udp_ping  -  UDP-based ping discovery module
[x] [4] infogather:ttl_calc  -  TCP and UDP based TTL distance calculation
[x] [5] infogather:portscan  -  TCP and UDP PortScanner
[x] [6] fingerprint:icmp_echo  -  ICMP Echo request fingerprinting module
[x] [7] fingerprint:icmp_tstamp  -  ICMP Timestamp request fingerprinting module
[x] [8] fingerprint:icmp_amask  -  ICMP Address mask request fingerprinting module
[x] [9] fingerprint:icmp_port_unreach  -  ICMP port unreachable fingerprinting module
[x] [10] fingerprint:tcp_hshake  -  TCP Handshake fingerprinting module
[x] [11] fingerprint:tcp_rst  -  TCP RST fingerprinting module
[x] [12] fingerprint:smb  -  SMB fingerprinting module
[x] [13] fingerprint:snmp  -  SNMPv2c fingerprinting module
[+] 13 modules registered
[+] Initializing scan engine
[+] Running scan engine
[-] ping:udp_ping module: no closed/open UDP ports known on 47.240.42.2. Module test failed
[+] Host: 47.240.42.2 is up (Guess probability: 66%)
[+] Target: 47.240.42.2 is alive. Round-Trip Time: 0.51112 sec
[+] Selected safe Round-Trip Time value is: 1.02223 sec
[-] fingerprint:smb need either TCP port 139 or 445 to run
[-] fingerprint:snmp: need UDP port 161 open
[+] Primary guess:
[+] Host 47.240.42.2 Running OS: �^#V (Guess probability: 95%)
[+] Other guesses:
[+] Host 47.240.42.2 Running OS: �^#V (Guess probability: 90%)
[+] Host 47.240.42.2 Running OS: �^#V (Guess probability: 90%)
[+] Host 47.240.42.2 Running OS: �^#V (Guess probability: 90%)
[+] Host 47.240.42.2 Running OS: �^#V (Guess probability: 90%)
[+] Host 47.240.42.2 Running OS: �^#V (Guess probability: 90%)
[+] Host 47.240.42.2 Running OS: �^#V (Guess probability: 90%)
[+] Host 47.240.42.2 Running OS: �^#V (Guess probability: 90%)
[+] Host 47.240.42.2 Running OS: �^#V (Guess probability: 90%)
[+] Host 47.240.42.2 Running OS: �^#V (Guess probability: 90%)
[+] Cleaning up scan engine
[+] Modules deinitialized
[+] Execution completed.
```

xprobe2 -c zsdk.org.cn

使用配置文件对目标进行扫描



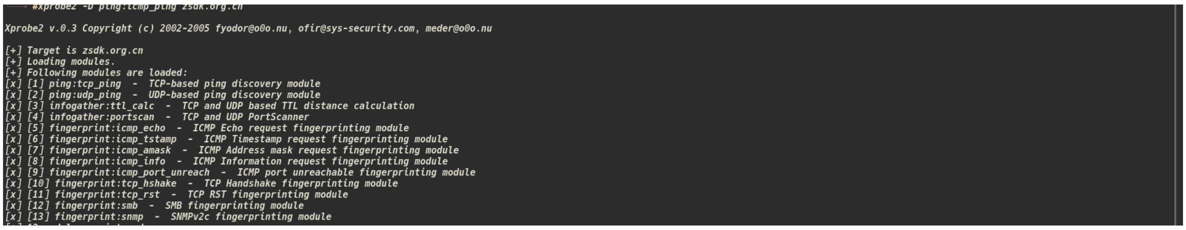
```
#xprobe2 -c c zsdk.org.cn

Xprobe2 v.0.3 Copyright (c) 2002-2005 fyodor@o0o.nu, ofir@sys-security.com, meder@o0o.nu

[+] Target is zsdk.org.cn
[+] Loading modules.
[+] Following modules are loaded:
[x] [1] ping:icmp_ping  -  ICMP echo discovery module
[x] [2] ping:tcp_ping  -  TCP-based ping discovery module
[x] [3] ping:udp_ping  -  UDP-based ping discovery module
[x] [4] infogather:ttl_calc  -  TCP and UDP based TTL distance calculation
[x] [5] infogather:portscan  -  TCP and UDP PortScanner
[x] [6] fingerprint:icmp_echo  -  ICMP Echo request fingerprinting module
[x] [7] fingerprint:icmp_tstamp  -  ICMP Timestamp request fingerprinting module
[x] [8] fingerprint:icmp_amask  -  ICMP Address mask request fingerprinting module
[x] [9] fingerprint:icmp_port_unreach  -  ICMP port unreachable fingerprinting module
[x] [10] fingerprint:tcp_hshake  -  TCP Handshake fingerprinting module
[x] [11] fingerprint:tcp_rst  -  TCP RST fingerprinting module
[x] [12] fingerprint:smb  -  SMB fingerprinting module
[x] [13] fingerprint:snmp  -  SNMPv2c fingerprinting module
[+] 13 modules registered
[+] Initializing scan engine
[+] Running scan engine
[-] ping:tcp_ping module: no closed/open TCP ports known on 47.240.42.2. Module test failed
[-] ping:udp_ping module: no closed/open UDP ports known on 47.240.42.2. Module test failed
[-] No distance calculation. 47.240.42.2 appears to be dead or no ports known
[+] Host: 47.240.42.2 is up (Guess probability: 50%)
[+] Target: 47.240.42.2 is alive. Round-Trip Time: 0.50753 sec
[+] Selected safe Round-Trip Time value is: 1.01505 sec
[-] fingerprint:tcp_hshake Module execution aborted (no open TCP ports known)
[-] fingerprint:smb need either TCP port 139 or 445 to run
[-] fingerprint:snmp: need UDP port 161 open
[+] Primary guess:
[+] Host 47.240.42.2 Running OS: ��-��U (Guess probability: 0%)
[+] Other guesses:
[+] Cleaning up scan engine
[+] Modules deinitialized
[+] Execution completed.
```

> xprobe2 -o zsdk zsdk.org.cn
>
> 使用日志文件zsdk 记录一切

> xprobe2 -t 10 zsdk.org.cn
>
> 设置初始接收或接受超时的时间
>
> xprobe2 -s 10 zsdk.org.cn
>
> 设置发送包延迟为10
>
> xprobe2 -d 3 zsdk.org.cn
>
> 设置一个调试级别
>
> xprobe2 -m 5 zsdk.org.cn
>
> 设置一个匹配数为“5
>
> > 比如你将匹配数设置为 “1”那么xprobe2只在终端回显一行数据
>
> xprobe2 -f 1 zsdk.org.cn
>
> 强制固定往返时间为1分钟
>
> xprobe2 -B zsdk.org.cn
>
> 强制使用TCP握手模块猜测目标打开的端口

xprobe2 -D ping:icmp_ping zsdk.org.cn

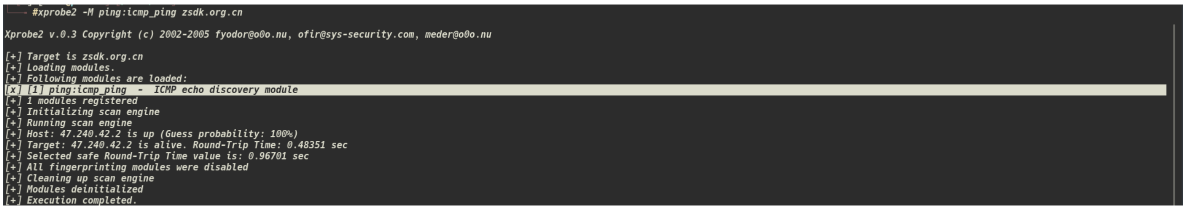
禁止ping:icmp_ping模块



```
#xprobe2 -D ping:icmp_ping zsdk.org.cn

Xprobe2 v.0.3 Copyright (c) 2002-2005 fyodor@o0o.nu, ofir@sys-security.com, meder@o0o.nu

[+] Target is zsdk.org.cn
[+] Loading modules.
[+] Following modules are loaded:
[x] [1] ping:tcp_ping  -  TCP-based ping discovery module
[x] [2] ping:udp_ping  -  UDP-based ping discovery module
[x] [3] infogather:ttl_calc  -  TCP and UDP based TTL distance calculation
[x] [4] infogather:portscan  -  TCP and UDP PortScanner
[x] [5] fingerprint:icmp_echo  -  ICMP Echo request fingerprinting module
[x] [6] fingerprint:icmp_tstamp  -  ICMP Timestamp request fingerprinting module
[x] [7] fingerprint:icmp_amask  -  ICMP Address mask request fingerprinting module
[x] [8] fingerprint:icmp_info  -  ICMP Information request fingerprinting module
[x] [9] fingerprint:icmp_port_unreach  -  ICMP port unreachable fingerprinting module
[x] [10] fingerprint:tcp_hshake  -  TCP Handshake fingerprinting module
[x] [11] fingerprint:tcp_rst  -  TCP RST fingerprinting module
[x] [12] fingerprint:smb  -  SMB fingerprinting module
[x] [13] fingerprint:snmp  -  SNMPv2c fingerprinting module
```

xprobe2 -M ping:icmp_ping zsdk.org.cn

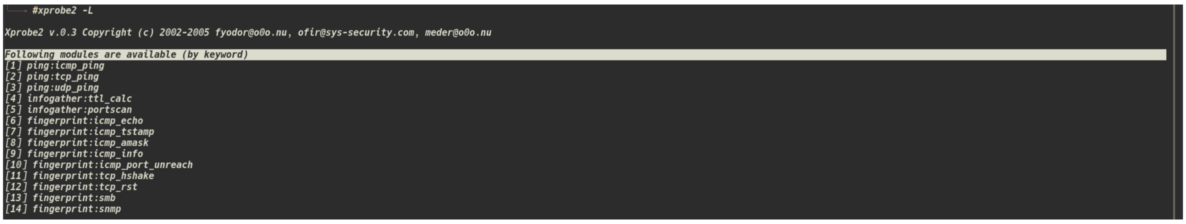
只启用ping:icmp_ping模块对目标进行扫描



```
#xprobe2 -M ping:icmp_ping zsdk.org.cn

Xprobe2 v.0.3 Copyright (c) 2002-2005 fyodor@o0o.nu, ofir@sys-security.com, meder@o0o.nu

[+] Target is zsdk.org.cn
[+] Loading modules.
[+] Following modules are loaded:
[x] [1] ping:icmp_ping  -  ICMP echo discovery module
[+] 1 modules registered
[+] Initializing scan engine
[+] Running scan engine
[+] Host: 47.240.42.2 is up (Guess probability: 100%)
[+] Target: 47.240.42.2 is alive. Round-Trip Time: 0.48351 sec
[+] Selected safe Round-Trip Time value is: 0.96701 sec
[+] All fingerprinting modules were disabled
[+] Cleaning up scan engine
[+] Modules deinitialized
[+] Execution completed.
```

xprobe2 -L

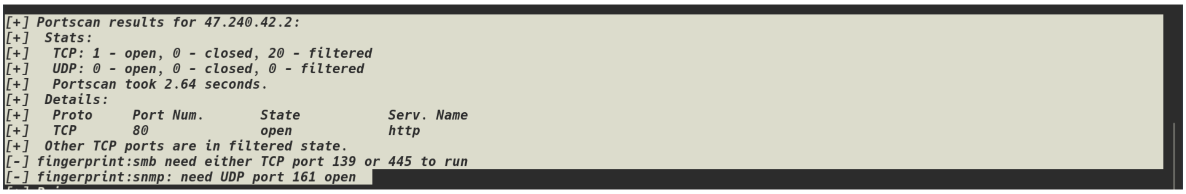
显示所有模块



```
#xprobe2 -L

Xprobe2 v.0.3 Copyright (c) 2002-2005 fyodor@o0o.nu, ofir@sys-security.com, meder@o0o.nu

Following modules are available (by keyword)
[1] ping:icmp_ping
[2] ping:tcp_ping
[3] ping:udp_ping
[4] infogather:ttl_calc
[5] infogather:portscan
[6] fingerprint:icmp_echo
[7] fingerprint:icmp_tstamp
[8] fingerprint:icmp_amask
[9] fingerprint:icmp_info
[10] fingerprint:icmp_port_unreach
[11] fingerprint:tcp_hshake
[12] fingerprint:tcp_rst
[13] fingerprint:smb
[14] fingerprint:snmp
```

xprobe2 -T 80-100 zsdk.org.cn

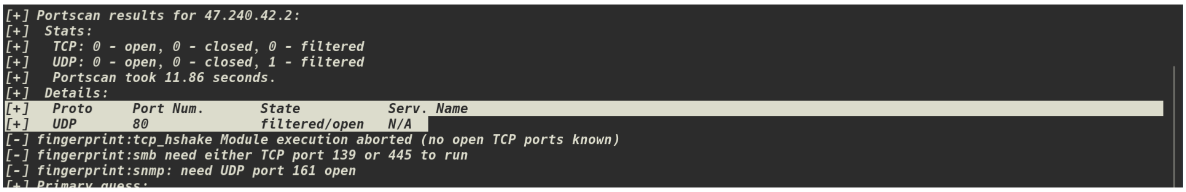
为指定的端口进行TCP端口扫描



```
[+] Portscan results for 47.240.42.2:
[+]  Stats:
[+]   TCP: 1 - open, 0 - closed, 20 - filtered
[+]   UDP: 0 - open, 0 - closed, 0 - filtered
[+]   Portscan took 2.64 seconds.
[+]  Details:
[+]   Proto     Port Num.       State           Serv. Name
[+]   TCP       80              open            http
[+]  Other TCP ports are in filtered state.
[-] fingerprint:smb need either TCP port 139 or 445 to run
[-] fingerprint:snmp: need UDP port 161 open
```

xprobe2 -U 80 zsdk.org.cn

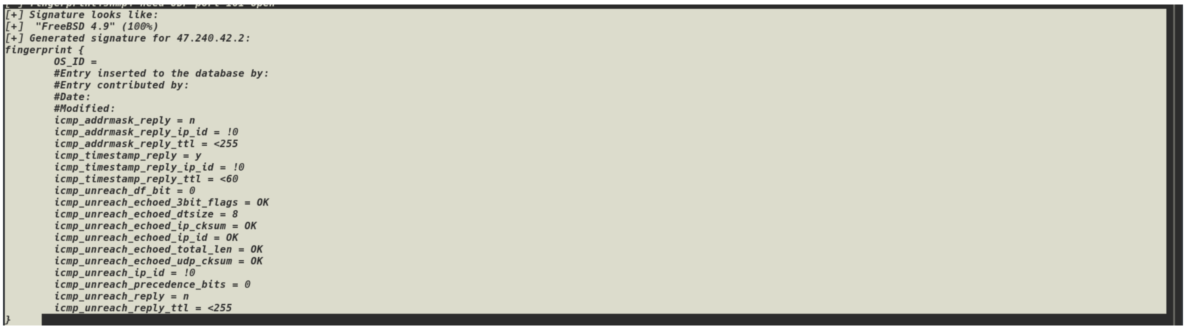
为指定的端口进行UDP扫描



```
[+] Portscan results for 47.240.42.2:
[+]  Stats:
[+]   TCP: 0 - open, 0 - closed, 0 - filtered
[+]   UDP: 0 - open, 0 - closed, 1 - filtered
[+]   Portscan took 11.86 seconds.
[+]  Details:
[+]   Proto     Port Num.       State           Serv. Name
[+]   UDP       80              filtered/open   N/A
[-] fingerprint:tcp_hshake Module execution aborted (no open TCP ports known)
[-] fingerprint:smb need either TCP port 139 or 445 to run
[-] fingerprint:snmp: need UDP port 161 open
```

xprobe2 -F zsdk.org.cn

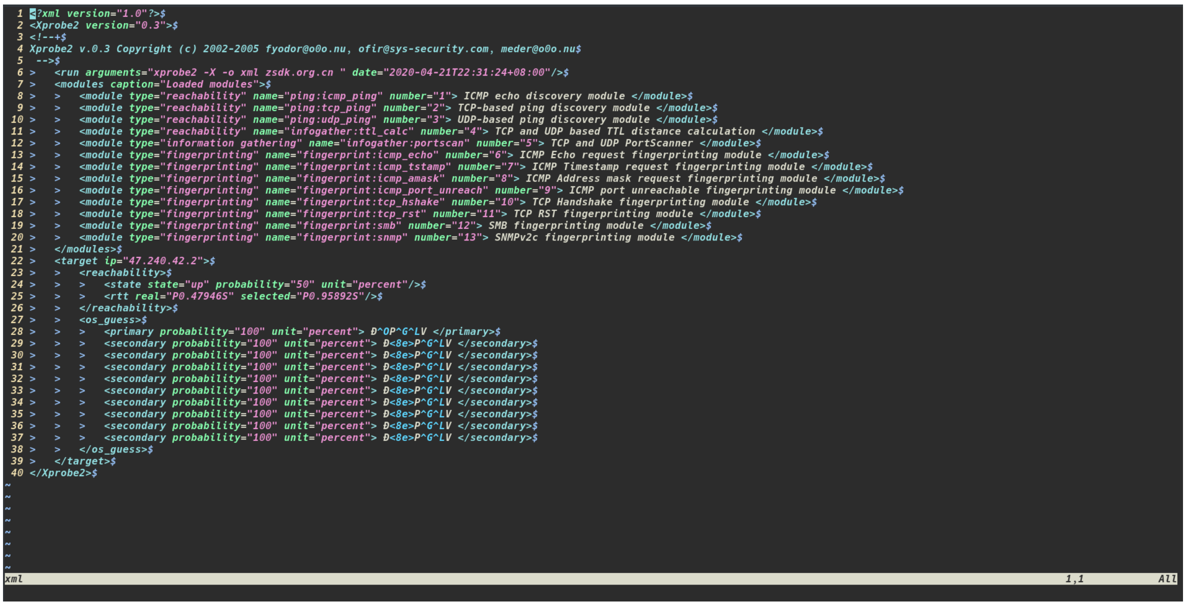
生成签名和指纹[^可配合 "-o"参数进行使用]



```
[-] fingerprint:snmp: need UDP port 161 open
[+] Signature looks like:
[+]  "FreeBSD 4.9" (100%)
[+] Generated signature for 47.240.42.2:
fingerprint {
        OS_ID =
        #Entry inserted to the database by:
        #Entry contributed by:
        #Date:
        #Modified:
        icmp_addrmask_reply = n
        icmp_addrmask_reply_ip_id = !0
        icmp_addrmask_reply_ttl = <255
        icmp_timestamp_reply = y
        icmp_timestamp_reply_ip_id = !0
        icmp_timestamp_reply_ttl = <60
        icmp_unreach_df_bit = 0
        icmp_unreach_echoed_3bit_flags = OK
        icmp_unreach_echoed_dtsize = 8
        icmp_unreach_echoed_ip_cksum = OK
        icmp_unreach_echoed_ip_id = OK
        icmp_unreach_echoed_total_len = OK
        icmp_unreach_echoed_udp_cksum = OK
        icmp_unreach_ip_id = !0
        icmp_unreach_precedence_bits = 0
        icmp_unreach_reply = n
        icmp_unreach_reply_ttl = <255
}
```

xprobe2 -X -o xml zsdk.org.cn

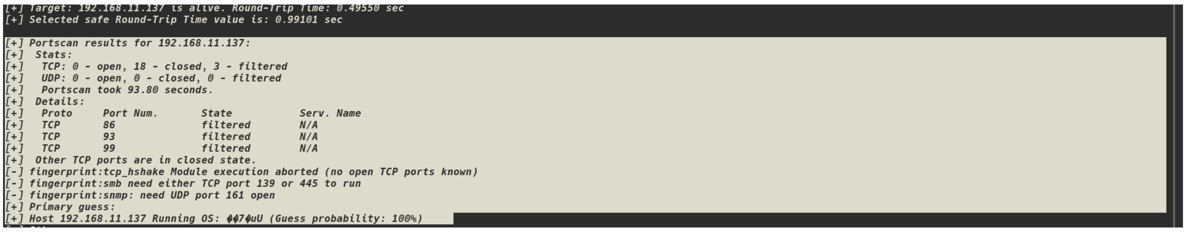
将最终回显结果以XML形式输出到xml文件之中



```
<?xml version="1.0"?>$
<Xprobe2 version="0.3">$
<!--+$
Xprobe2 v.0.3 Copyright (c) 2002-2005 fyodor@o0o.nu, ofir@sys-security.com, meder@o0o.nu$
 -->$
>   <run arguments="xprobe2 -X -o xml zsdk.org.cn " date="2020-04-21T22:31:24+08:00"/>$
>   <modules caption="Loaded modules">$
>   >   <module type="reachability" name="ping:icmp_ping" number="1"> ICMP echo discovery module </module>$
>   >   <module type="reachability" name="ping:tcp_ping" number="2"> TCP-based ping discovery module </module>$
>   >   <module type="reachability" name="ping:udp_ping" number="3"> UDP-based ping discovery module </module>$
>   >   <module type="reachability" name="infogather:ttl_calc" number="4"> TCP and UDP based TTL distance calculation </module>$
>   >   <module type="information gathering" name="infogather:portscan" number="5"> TCP and UDP PortScanner </module>$
>   >   <module type="fingerprinting" name="fingerprint:icmp_echo" number="6"> ICMP Echo request fingerprinting module </module>$
>   >   <module type="fingerprinting" name="fingerprint:icmp_tstamp" number="7"> ICMP Timestamp request fingerprinting module </module>$
>   >   <module type="fingerprinting" name="fingerprint:icmp_amask" number="8"> ICMP Address mask request fingerprinting module </module>$
>   >   <module type="fingerprinting" name="fingerprint:icmp_port_unreach" number="9"> ICMP port unreachable fingerprinting module </module>$
>   >   <module type="fingerprinting" name="fingerprint:tcp_hshake" number="10"> TCP Handshake fingerprinting module </module>$
>   >   <module type="fingerprinting" name="fingerprint:tcp_rst" number="11"> TCP RST fingerprinting module </module>$
>   >   <module type="fingerprinting" name="fingerprint:smb" number="12"> SMB fingerprinting module </module>$
>   >   <module type="fingerprinting" name="fingerprint:snmp" number="13"> SNMPv2c fingerprinting module </module>$
>   </modules>$
>   <target ip="47.240.42.2">$
>   >   <reachability>$
>   >   >   <state state="up" probability="50" unit="percent"/>$
>   >   >   <rtt real="P0.47946S" selected="P0.95892S"/>$
>   >   </reachability>$
>   >   <os_guess>$
>   >   >   <primary probability="100" unit="percent"> Ð^OP^G^LV </primary>$
>   >   >   <secondary probability="100" unit="percent"> Ð<8e>P^G^LV </secondary>$
>   >   >   <secondary probability="100" unit="percent"> Ð<8e>P^G^LV </secondary>$
>   >   >   <secondary probability="100" unit="percent"> Ð<8e>P^G^LV </secondary>$
>   >   >   <secondary probability="100" unit="percent"> Ð<8e>P^G^LV </secondary>$
>   >   >   <secondary probability="100" unit="percent"> Ð<8e>P^G^LV </secondary>$
>   >   >   <secondary probability="100" unit="percent"> Ð<8e>P^G^LV </secondary>$
>   >   >   <secondary probability="100" unit="percent"> Ð<8e>P^G^LV </secondary>$
>   >   >   <secondary probability="100" unit="percent"> Ð<8e>P^G^LV </secondary>$
>   >   >   <secondary probability="100" unit="percent"> Ð<8e>P^G^LV </secondary>$
>   >   </os_guess>$
>   </target>$
</Xprobe2>$
~
~
~
~
~
~
~
~
xml                                                                                                   1,1            All
```

xprobe2 -T 80-100 -A 192.168.11.137

对目标进行端口扫描，并从端口扫描的期间内对收集的数据包进行分析。



```
[+] Target: 192.168.11.137 is alive. Round-Trip Time: 0.49550 sec
[+] Selected safe Round-Trip Time value is: 0.99101 sec

[+] Portscan results for 192.168.11.137:
[+]  Stats:
[+]   TCP: 0 - open, 18 - closed, 3 - filtered
[+]   UDP: 0 - open, 0 - closed, 0 - filtered
[+]   Portscan took 93.80 seconds.
[+]  Details:
[+]   Proto     Port Num.       State           Serv. Name
[+]   TCP       86              filtered        N/A
[+]   TCP       93              filtered        N/A
[+]   TCP       99              filtered        N/A
[+]  Other TCP ports are in closed state.
[-] fingerprint:tcp_hshake Module execution aborted (no open TCP ports known)
[-] fingerprint:smb need either TCP port 139 or 445 to run
[-] fingerprint:snmp: need UDP port 161 open
[+] Primary guess:
[+] Host 192.168.11.137 Running OS: ��7�uU (Guess probability: 100%)
```