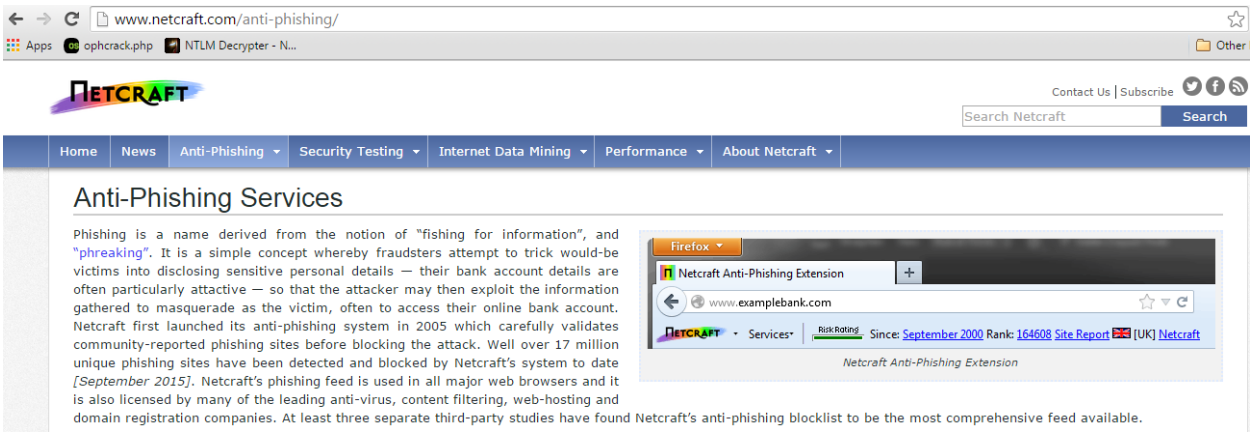
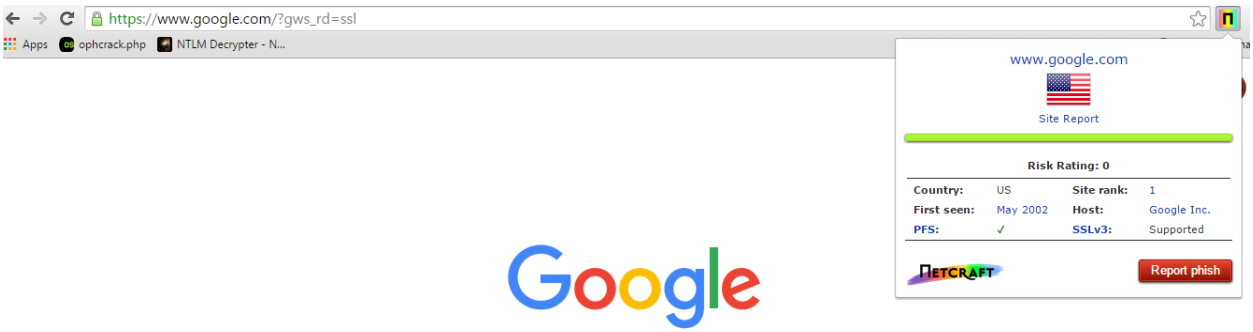
You can telnet to other commonly used ports with these commands:

- **SMTP: telnet ip_address 25**
- **HTTP: telnet ip_address 80**
- **POP3: telnet ip_address 110**

Netcraft Banner Grabbing

برای این منظور ابتدا بایستی وارد سایت www.netcraft.com شوید سپس باید وارد قسمت Anti-phishing Toolbar رفته وآن را برروی سیستم خود نصب کنیداین Toolbar برروی Firefox نصب می شودهمانطوری که در شکل زیر مشاهده میکنید:





Background

Site title	Google	**Date first seen**	May 2002
Site rank	1	**Primary language**	English
Description	*Not Present*		
Keywords	*Not Present*		

Network

Site	https://www.google.com	**Netblock Owner**	Google Inc.
Domain	google.com	**Nameserver**	ns1.google.com
IP address	216.58.208.68	**DNS admin**	dns-admin@google.com
IPv6 address	2a00:1450:4009:80a:0:0:0:2004	**Reverse DNS**	lhr14s27-in-f4.1e100.net
Domain registrar	markmonitor.com	**Nameserver organisation**	whois.markmonitor.com
Organisation	Google Inc., Please contact contact-admin@google.com, 1600 Amphitheatre Parkway, Mountain View, 94043, United States	**Hosting company**	Google

دستور پیشنهادی جهت اسکن یک Target به صورت زیر می باشد:

```
root@kali:~# nmap  -A  -v  -Pn  -f  -O  -sV  -sS  172.16.100.2
```

A– (برای تشخیص نوع سیستم عامل هدف و نسخه مربوط به آن می باشد و انجام عمل Trace به کار می رود)

v- (برای مشخص کردن پورتهای باز استفاده می شود)

Pn- (در اصطلاح یک اسکن خاموش می باشد)

f– (عملیات اسکن Fragment انجام می شود تا توسط فایروال شناسایی نشوند)

O- (برای تشخیص فقط نوع سیستم عامل می باشد)

sV- (برای شناسایی پورتهای باز و نسخه سرویس مربوط به آنها می باشد)

sS- (برای اجرای عملیات اسکن TCP Syn می باشد)

S- آدرس IP یک هکر را با یک آدرس جعلی در یک اسکن استفاده می کند.

Angry IP Scanner

هدف شناسایی سیستم های فعال در شبکه می باشد.

یکی از ابزارها برای این منظور نرم افزار Angry IP Scanner می باشد.

برای مثال ما قصد داریم تمامی مودم های ADSL یک ISP را که شامل پورت 80 می باشند را شناسایی کنیم. اکثر مودم های ADSL بر روی پورت TCP شماره 80 کار می کنند و شامل User name و Password پیش فرض می باشند.

Scan the ADSL Router:

Here is a detailed information on how to exploit the vulnerability of an ADSL router:

1. Go to whatismyipaddress.com. Once the page is loaded, you will find your IP address. Note it down.
2. Open Angry IP Scanner, here you will see an option called **IP Range:** where you need to enter the range of IP address to scan for.

   Suppose your IP is **117.192.195.101**, you can set the range something as **117.192.194.0 to 117.192.200.255** so that there exists at least 200-300 IP addresses in the range.

3. Go to **Tools->Preferences** and select the **Ports** tab. Under **Port selection** enter **80** (we need to scan for port 80). Now switch to the **Display** tab, select the option "**Hosts with open ports only**" and click on OK.

@Javangrpchannel

I have used Angry IP Scanner **v3.0 beta-4**. If you are using a different version, you need to Go to **Options** instead of **Tools**

4. Now click on **Start**. After a few minutes, the IP scanner will show a list of IPs with Port 80 open as shown in the below image:

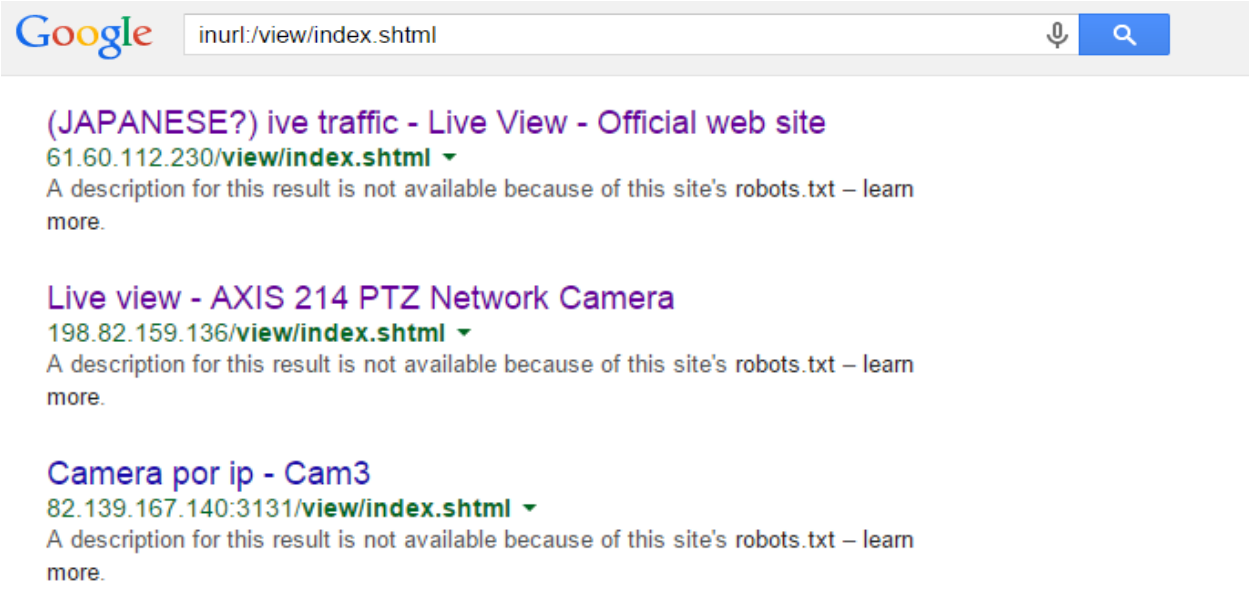
5.Now copy any of the IP from the list, paste it in your browser's address bar and hit enter. A window will popup asking for username and password. Since most users do not change the passwords, it should most likely work with the default username and password. For most routers the default **username-password** pair will be **admin-admin** or **admin-password**.

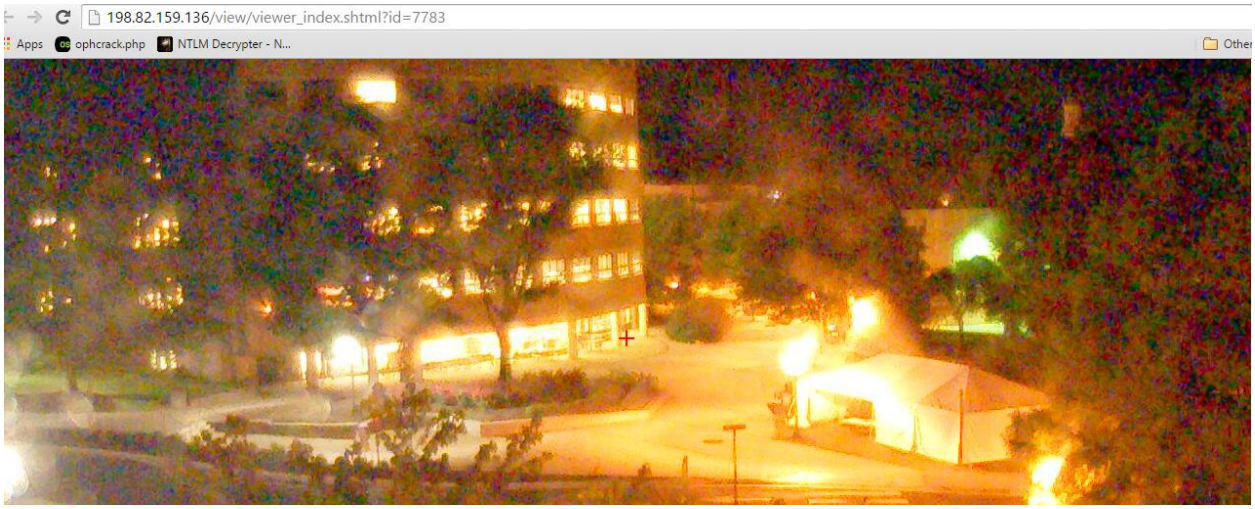
6.Just enter the username-password as specified above and hit enter. If you are lucky you should gain access to the router settings page where you can modify any of the router settings. The settings page can vary from router to router. A sample router settings page is shown below:

بعد از اسکن می توانیم بر روی Host هایی که alive هستند راست کلیک کرده و در قسمت open عملیاتی مانند Ftp و Telnet ، Ping و Traceroute ، Web Browser و غیره را انجام دهیم.

بعد از اینکه به مودم ADSl ، سیستم Target با Username ، password پیش فرض یعنی admin/admin وارد شدید در قسمت Remote management می توانید سرویس Telnet مودم را فعال کنید در web page مربوط به مودم ADSL معمولا User name شناسایی می شود ولی Password پنهان می باشد که با telnet به آن و اجرای دستور Show all می توانیم Password را هم ببینیم .

How to Scan into live, public security cameras and web cams




198.82.159.136/view/viewer_index.shtml?id=7783
Apps
ophcrack.php
NTLM Decrypter - N...
Other


AXIS P7214 Video Encoder
Live View | Setup | Help
Stream profile
Motion JPEG
Video stream or PTZ preset
Quad Stream
Go
ID=029
ID=001
ID=001
HOLD
445
NO VIDEO

Scanning DNS Enumuration

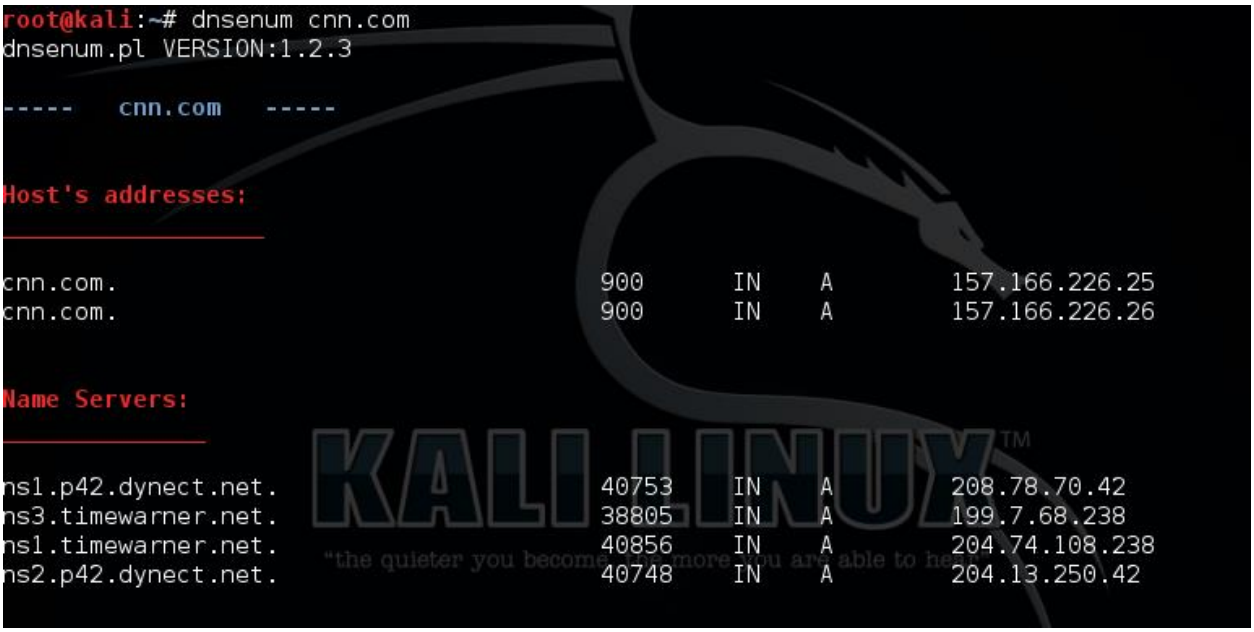
یک اسکریپت Perl می باشد که برای بدست آوردن اطلاعات DNS از یک Domain استفاده می شود.

با استفاده از DNS Enumuration شما می توانید اطلاعات زیر را در مورد یک Domain خاص بدست آورید:

```
1) Get the host's addresse (A record).

2) Get the namservers .

3) Get the MX record .
```



```
Mail (MX) Servers:
_____________________

ppsprmse.turner.com.                    1600     IN    A        157.166.157.26
ppsprmsa.turner.com.                    1600     IN    A        157.166.168.210
ppsprmsb.turner.com.                    1600     IN    A        157.166.168.213
ppsprmsd.turner.com.                    1600     IN    A        157.166.165.226
ppsprmsf.turner.com.                    1600     IN    A        157.166.157.27
ppsprmsg.turner.com.                    1600     IN    A        157.166.157.28
ppsprmsc.turner.com.                    1600     IN    A        157.166.165.224
```

HPing Scanning

HPing یک Free Packet Generator and Analyzer می باشد که برای تست

فایروال و شبکه استفاده می شود.

Hping براساس TCL Script نوشته شده است.

Anex A Hping3 Help

usage: hping3 host [options]
-h --help show this help
-v --version show version
-c --count packet count
-i --interval wait (uX for X microseconds, for example -i u1000)
--fast alias for -i u10000 (10 packets for second)
--faster alias for -i u1000 (100 packets for second)
--flood sent packets as fast as possible. Don't show replies.
-n --numeric numeric output
-q --quiet quiet
-I --interface interface name (otherwise default routing interface)
-V --verbose verbose mode
-D --debug debugging info
-z --bind bind ctrl+z to ttl (default to dst port)
-Z --unbind unbind ctrl+z
--beep beep for every matching packet received
Mode
default mode TCP
-0 --rawip RAW IP mode
-1 --icmp ICMP mode
-2 --udp UDP mode
-8 --scan SCAN mode.
Example: hping --scan 1-30,70-90 -S www.target.host
-9 --listen listen mode
IP
-a --spoof spoof source address
--rand-dest random destionation address mode. see the man.
--rand-source random source address mode. see the man.
-t --ttl ttl (default 64)
-N --id id (default random)

-W --winid use win* id byte ordering
-r --rel relativize id field (to estimate host traffic)
-f --frag split packets in more frag. (may pass weak acl)
-x --morefrag set more fragments flag
-y --dontfrag set dont fragment flag
-g --fragoff set the fragment offset
-m --mtu set virtual mtu, implies --frag if packet size > mtu
-o --tos type of service (default 0x00), try --tos help
-G --rroute includes RECORD_ROUTE option and display the route buffer
--lsrr loose source routing and record route
--ssrr strict source routing and record route
-H --ipproto set the IP protocol field, only in RAW IP mode

ICMP
-C --icmptype icmp type (default echo request)
-K --icmpcode icmp code (default 0)
--force-icmp send all icmp types (default send only supported types)
--icmp-gw set gateway address for ICMP redirect (default 0.0.0.0)
--icmp-ts Alias for --icmp --icmptype 13 (ICMP timestamp)
--icmp-addr Alias for --icmp --icmptype 17 (ICMP address subnet mask)
--icmp-help display help for others icmp options

UDP/TCP
-s --baseport base source port (default random)
-p --destport [+][+]<port> destination port(default 0) ctrl+z inc/dec
-k --keep keep still source port
-w --win winsize (default 64)
-O --tcpoff set fake tcp data offset (instead of tcphdrlen / 4)
-Q --seqnum shows only tcp sequence number
-b --badcksum (try to) send packets with a bad IP checksum many systems will fix the IP checksum sending the packet so you'll get bad UDP/TCP checksum instead.
-M --setseq set TCP sequence number
-L --setack set TCP ack
-F --fin set FIN flag
-S --syn set SYN flag
-R --rst set RST flag
-P --push set PUSH flag
-A --ack set ACK flag
-U --urg set URG flag
-X --xmas set X unused flag (0x40)
-Y --ymas set Y unused flag (0x80)
--tcpexitcode use last tcp->th_flags as exit code
--tcp-timestamp enable the TCP timestamp option to guess the HZ/uptime

Common
-d --data data size (default is 0)
-E --file data from file
-e --sign add 'signature'
-j --dump dump packets in hex
-J --print dump printable characters
-B --safe enable 'safe' protocol
-u --end tell you when --file reached EOF and prevent rewind
-T --traceroute traceroute mode (implies --bind and --ttl 1)
--tr-stop Exit when receive the first not ICMP in traceroute mode
--tr-keep-ttl Keep the source TTL fixed, useful to monitor just one hop
--tr-no-rtt Don't calculate/show RTT information in traceroute mode

ARS packet description (new, unstable)
--apd-send Send the packet described with APD (see docs/APD.txt)

@Javangrpchannel

1. Testing ICMP: In this example hping3 will behave like a normal ping utility, sending ICMP-echo und receiving ICMP-reply

```
hping3 -1 0daysecurity.com
```

2. Traceroute using ICMP: This example is similar to famous utilities like tracert (windows) or traceroute (linux) who uses ICMP packets increasing every time in 1 its TTL value.

```
hping3 --traceroute -V -1 0daysecurity.com
```

3. Checking port: Here hping3 will send a Syn packet to a specified port (80 in our example). We can control also from which local port will start the scan (5050).

```
hping3 -V -S -p 80 -s 5050 0daysecurity.com
```

4. Traceroute to a determined port: A nice feature from Hping3 is that you can do a traceroute to a specified port watching where your packet is blocked. It can just be done by adding --traceroute to the last command.

```
hping3 --traceroute -V -S -p 80 -s 5050 0daysecurity.com
```

5. Other types of ICMP: This example sends a ICMP address mask request (Type 17).

```
hping3 -c 1 -V -1 -C 17 0daysecurity.com
```

6. Other types of Port Scanning: First type we will try is the FIN scan. In a TCP connection the FIN flag is used to start the connection closing routine. If we do not receive a reply, that means the port is open. Normally firewalls send a RST+ACK packet back to signal that the port is closed..

```
hping3 -c 1 -V -p 80 -s 5050 -F 0daysecurity.com
```

7. Ack Scan: This scan can be used to see if a host is alive (when Ping is blocked for example). This should send a RST response back if the port is open.

```
hping3 -c 1 -V -p 80 -s 5050 -A 0daysecurity.com
```

8. Xmas Scan: This scan sets the sequence number to zero and set the URG + PSH + FIN flags in the packet. If the target device's TCP port is closed, the target device sends a TCP RST packet in reply. If the target device's TCP port is open, the target discards the TCP Xmas scan, sending no reply.

```
hping3 -c 1 -V -p 80 -s 5050 -M 0 -UPF 0daysecurity.com
```

9. Null Scan: This scan sets the sequence number to zero and have no flags set in the packet. If the target device's TCP port is closed, the target device sends a TCP RST packet in reply. If the target device's TCP port is open, the target discards the TCP NULL scan, sending no reply.

```
hping3 -c 1 -V -p 80 -s 5050 -Y 0daysecurity.com
```

10. Smurf Attack: This is a type of denial-of-service attack that floods a target system via spoofed broadcast ping messages.

```
hping3 -1 --flood -a VICTIM_IP BROADCAST_ADDRESS
```

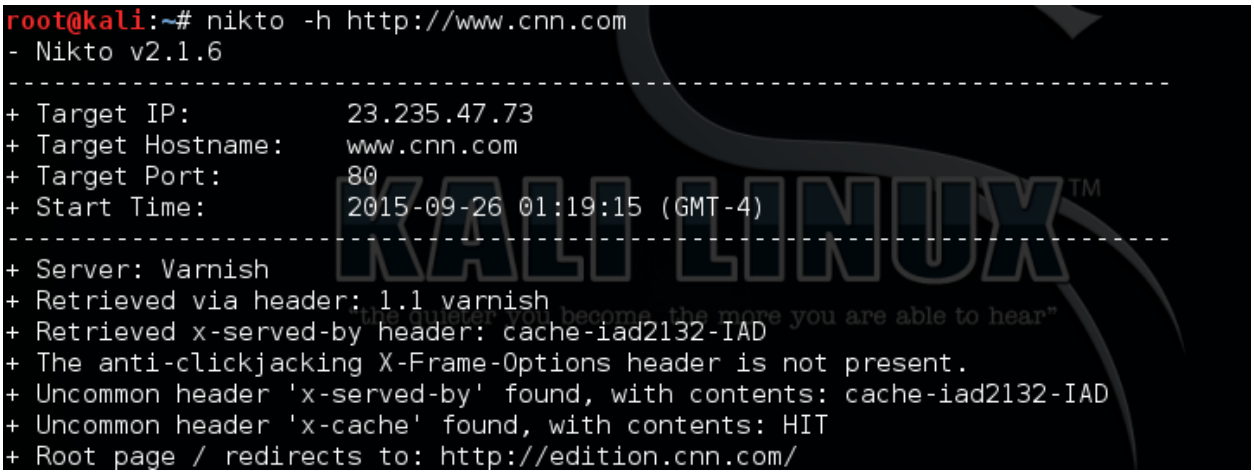
11. DOS Land Attack:

```
hping3 -V -c 1000000 -d 120 -S -w 64 -p 445 -s 445 --flood --rand-source VICTIM_IP
```

- --flood: sent packets as fast as possible. Don't show replies.
- --rand-dest: random destionation address mode. see the man.
- -V <-- Verbose
- -c --count: packet count
- -d --data: data size
- -S --syn: set SYN flag
- -w --win: winsize (default 64)
- -p --destport [+][+]<port> destination port(default 0) ctrl+z inc/dec
- -s --baseport: base source port (default random)

Scanning Nikto

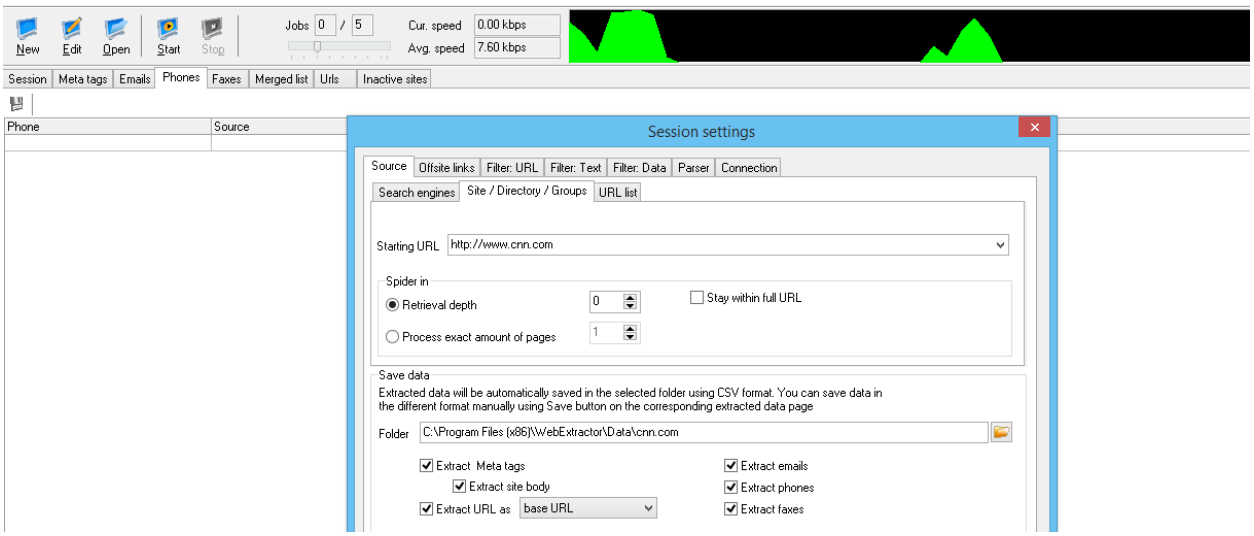
یک web Server Scanner می باشد که برای شناسایی مشکلاتی که برروی وب سرورها وجود دارد استفاده می شود از طرف دیگر می تواند نوع وب سرور را هم مشخص کند.

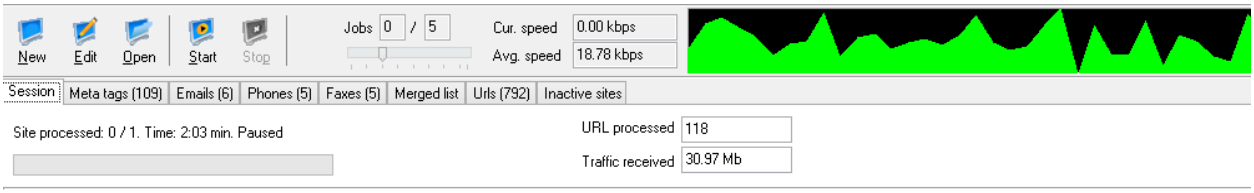


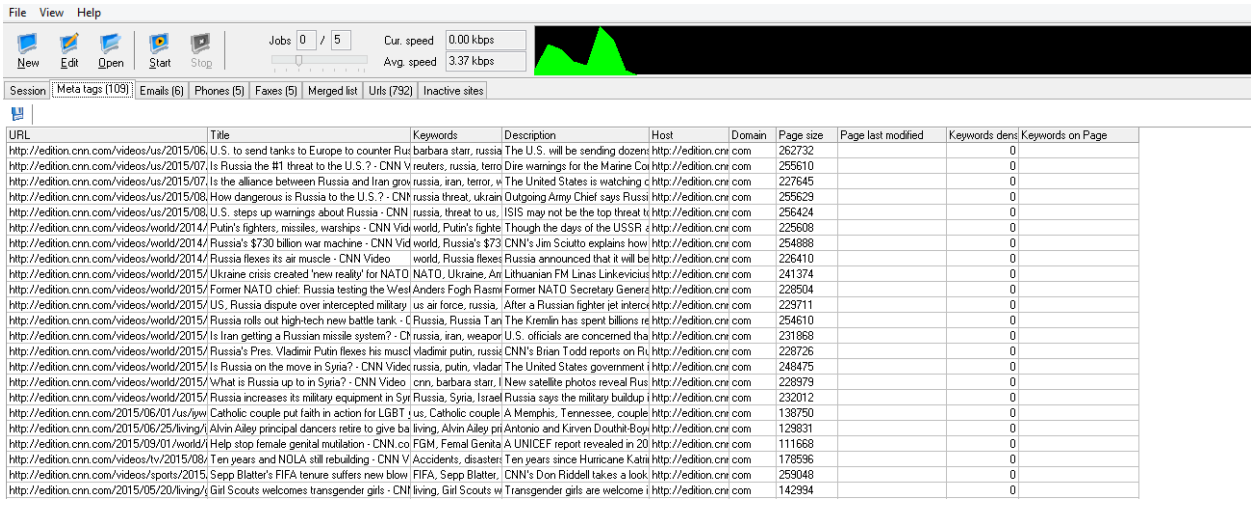
Scanning with web Data Extractor

با استفاده از این اسکنر شما می توانید اطلاعات مهمی مانند ایمیل آدرس ها و شماره تلفن و آدرس وب سایت های مرتبط به آن و کد های مهمی که در یک وب سایت وجود دارد را بدست آورید.

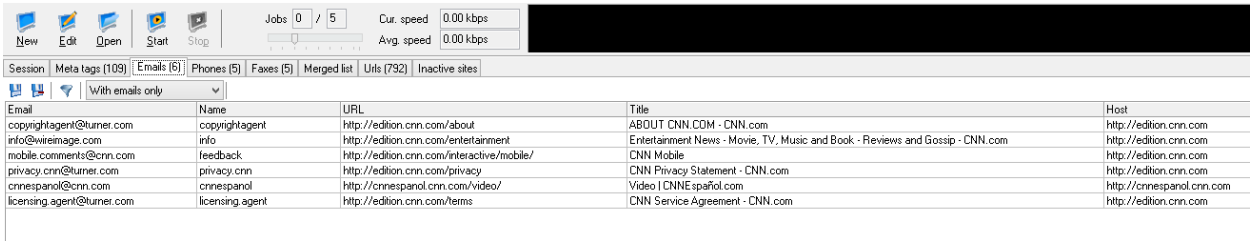
@Javangrpchannel







@Javangrpchannel

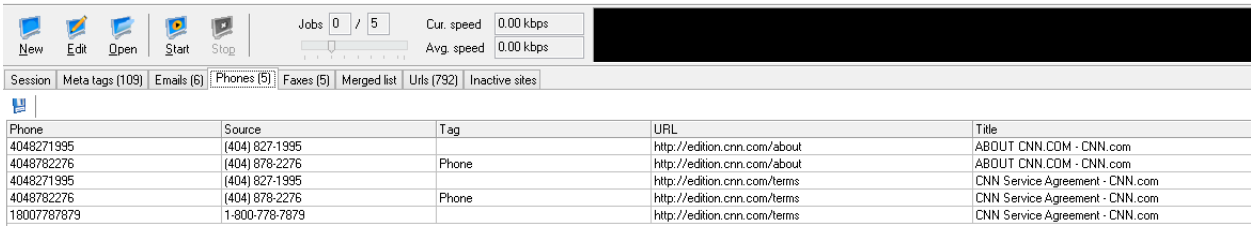


New Edit Open Start Stop Jobs 0 / 5 Cur. speed 0.00 kbps Avg. speed 0.00 kbps

Session | Meta tags (109) | Emails (6) | Phones (5) | Faxes (5) | Merged list | Urls (792) | Inactive sites

With emails only

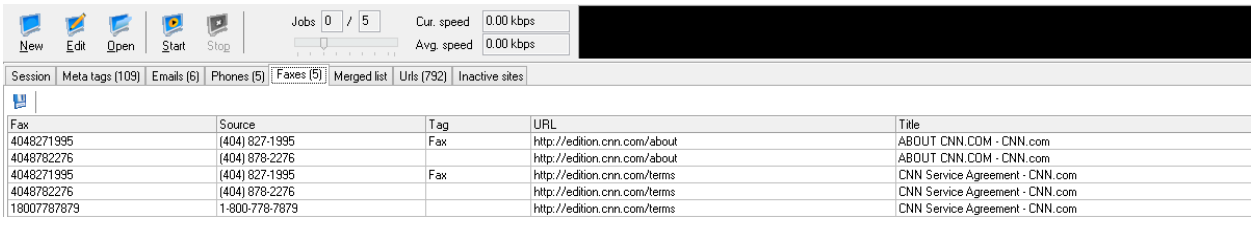
Email	Name	URL	Title	Host
copyrightagent@turner.com	copyrightagent	http://edition.cnn.com/about	ABOUT CNN.COM - CNN.com	http://edition.cnn.com
info@wireimage.com	info	http://edition.cnn.com/entertainment	Entertainment News - Movie, TV, Music and Book - Reviews and Gossip - CNN.com	http://edition.cnn.com
mobile.comments@cnn.com	feedback	http://edition.cnn.com/interactive/mobile/	CNN Mobile	http://edition.cnn.com
privacy.cnn@turner.com	privacy.cnn	http://edition.cnn.com/privacy	CNN Privacy Statement - CNN.com	http://edition.cnn.com
cnnespanol@cnn.com	cnnespanol	http://cnnespanol.cnn.com/video/	Video	CNNEspañol.com	http://cnnespanol.cnn.com
licensing.agent@turner.com	licensing.agent	http://edition.cnn.com/terms	CNN Service Agreement - CNN.com	http://edition.cnn.com



New Edit Open Start Stop Jobs 0 / 5 Cur. speed 0.00 kbps Avg. speed 0.00 kbps

Session | Meta tags (109) | Emails (6) | Phones (5) | Faxes (5) | Merged list | Urls (792) | Inactive sites

Phone	Source	Tag	URL	Title
4048271995	(404) 827-1995		http://edition.cnn.com/about	ABOUT CNN.COM - CNN.com
4048782276	(404) 878-2276	Phone	http://edition.cnn.com/about	ABOUT CNN.COM - CNN.com
4048271995	(404) 827-1995		http://edition.cnn.com/terms	CNN Service Agreement - CNN.com
4048782276	(404) 878-2276	Phone	http://edition.cnn.com/terms	CNN Service Agreement - CNN.com
18007787879	1-800-778-7879		http://edition.cnn.com/terms	CNN Service Agreement - CNN.com



New Edit Open Start Stop Jobs 0 / 5 Cur. speed 0.00 kbps Avg. speed 0.00 kbps

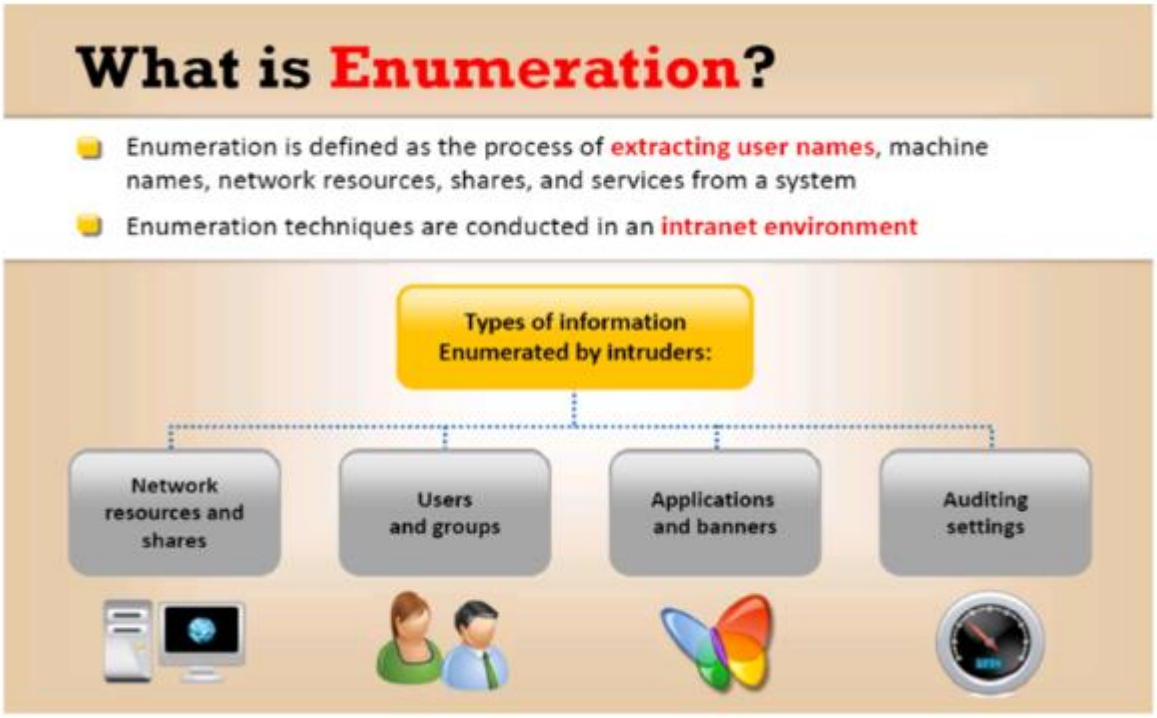
Session | Meta tags (109) | Emails (6) | Phones (5) | Faxes (5) | Merged list | Urls (792) | Inactive sites

Fax	Source	Tag	URL	Title
4048271995	(404) 827-1995	Fax	http://edition.cnn.com/about	ABOUT CNN.COM - CNN.com
4048782276	(404) 878-2276		http://edition.cnn.com/about	ABOUT CNN.COM - CNN.com
4048271995	(404) 827-1995	Fax	http://edition.cnn.com/terms	CNN Service Agreement - CNN.com
4048782276	(404) 878-2276		http://edition.cnn.com/terms	CNN Service Agreement - CNN.com
18007787879	1-800-778-7879		http://edition.cnn.com/terms	CNN Service Agreement - CNN.com

@Javangrpchannel

Module 04 Enumeration

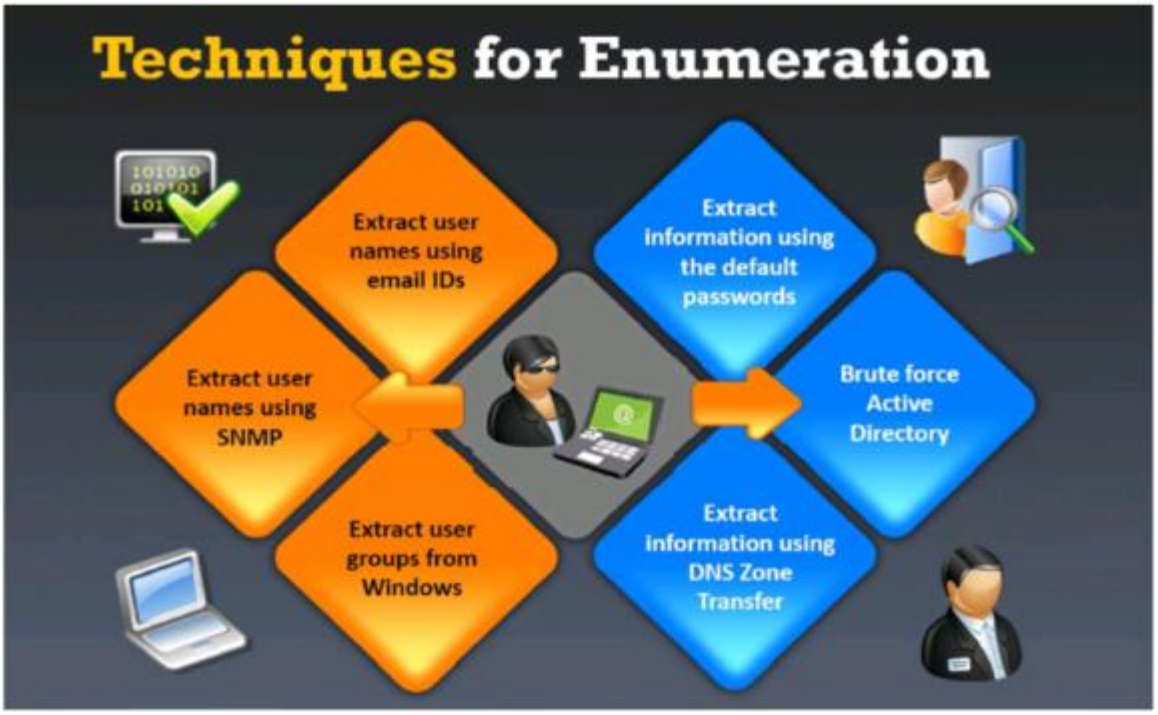
@Javangrpchannel



به معنی جز به جز شمردن می باشد و فقط برروی شبکه LAN قابل پیاده سازی می باشد.

با استفاده از این روش می توان اطلاعات دقیقتری درباره یک سیستم بدست آورد.

@Javangrpchannel



با استفاده از پروتکل های زیر می توان عملیات Enumretaion انجام داد:

- ✓ **پورت 445**
- ✓ **پورت 137**
- ✓ **پورت 138**
- ✓ **پورت 139**
- ✓ **پورت 161**
- ✓ **پورت 123**

برای انجام Enumration نیاز به یک Session باز با سیستم مقصد می باشد.

برای مثال

\\x.x.x.x

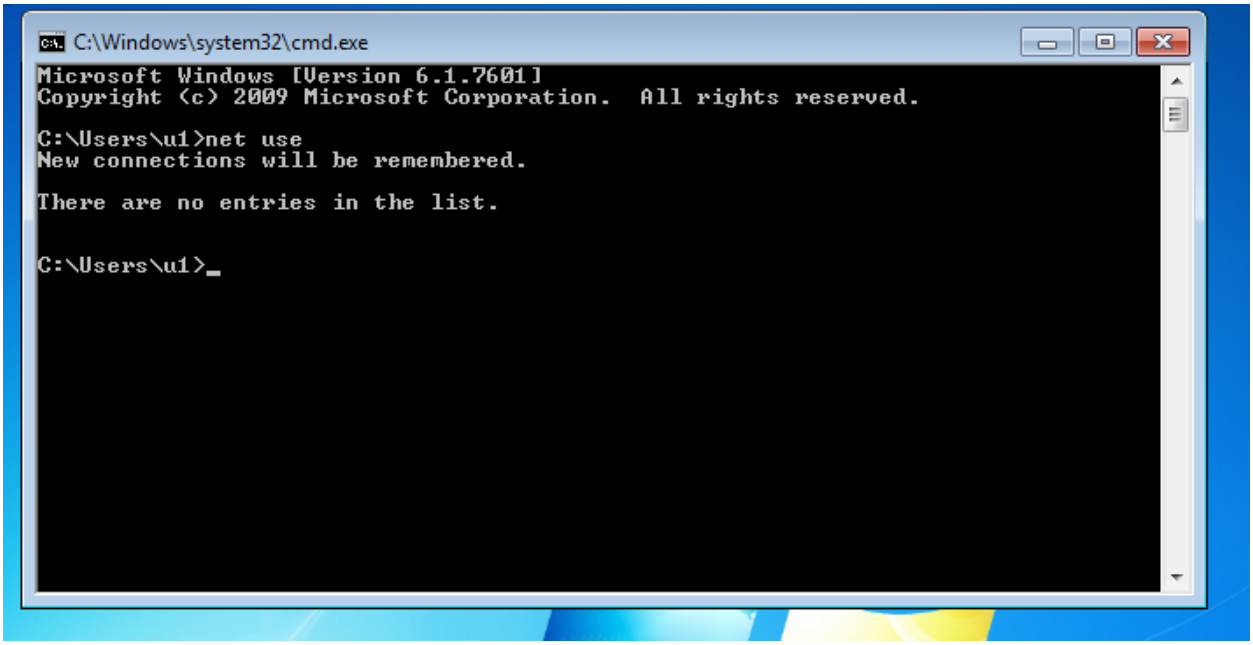
Session باز فقط برروی پروتکل های TCP و UDP شکل می گیرد.

@Javangrpchannel

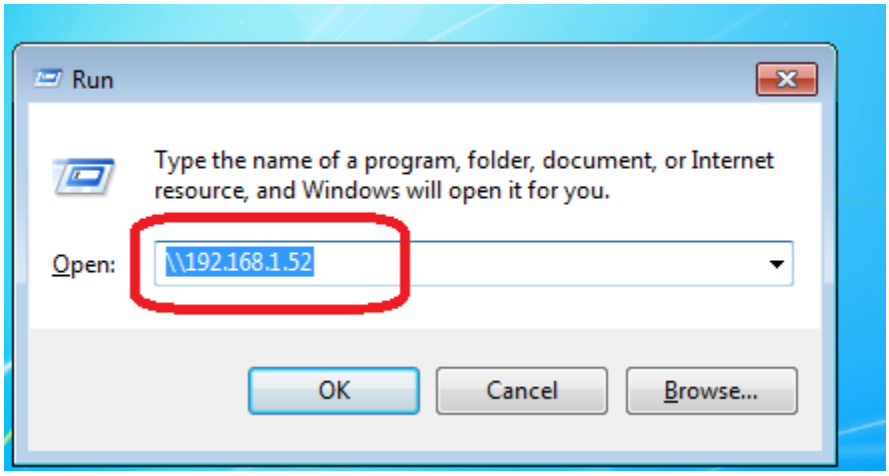
تفاوت شبکه های Domain و Workgroup

Enumration در شبکه های Domain راحتر می باشد.

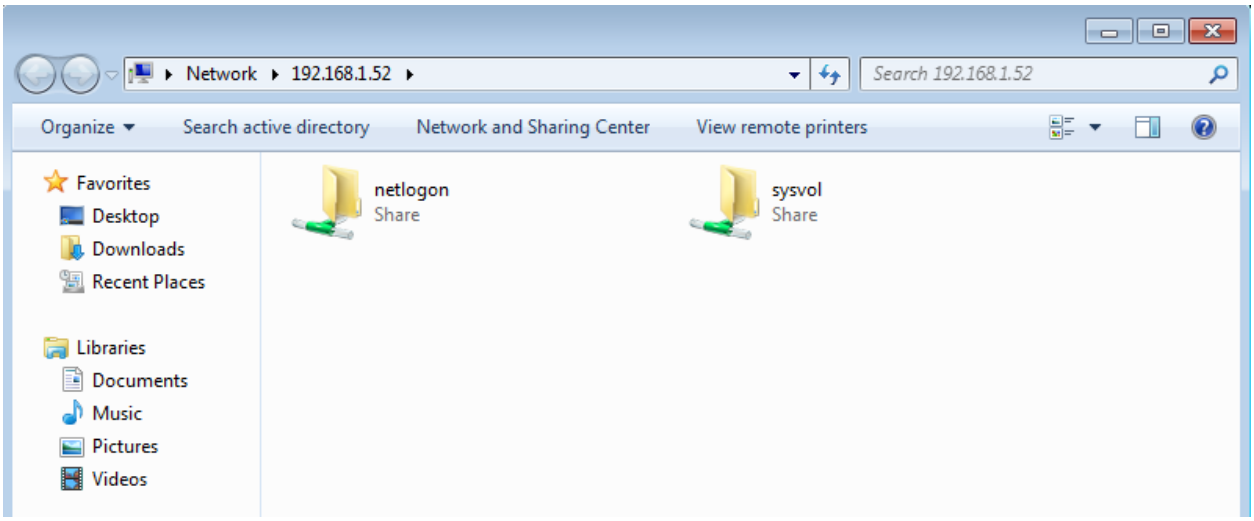
برای مشاهده Session های باز برروی یک سیستم از دستور زیر استفاده می شود:



برای باز کردن یک Session باز بر روی سیستم مقصد از دستور زیر استفاده می شود:



@Javangrpchannel



در شبکه های **Domain** برای باز کردن **Session** باز نیازی به **Username** و **Password** نیست

به همین دلیل **Enumeration** برروی شبکه های **Domain** راحتر می باشد و از لحاظ امنیتی نسبت به شبکه های **workstation** ضعیفتر می باشند.

یکی از ابزارهایی که برای **Enumeration** استفاده می شود **Hyena** می باشد.