

### Stealth Scanning Strategies

#### Risk = Discovery By The Target.

Camouflage tool signatures to avoid detection.  
Hide attack in legitimate traffic.  
Modify attack to hide source, type of traffic.  
Make attack invisible using non-standard traffic types & encryption.

### Adjust Source IP Stack & Tool ID - STEALTH 1

Disable Unnecessary Services:

**Disable DHCP** `chkconfig dhcpd off`

**Disable IPv6** `nano /etc/sysctl.conf`

`#disable ipv6`

`net.ipv6.conf.all.disable_ipv6 = 1`

`net.ipv6.conf.default.disable_ipv6`

`= 1`

`net.ipv6.conf.lo.disable = 1`

Tools often tag packets with an id sequence that can trigger IDS. Test tools against VM's and review system logs for the tool's name. Use **Wireshark** to capture traffic then search pcaps for keywords attributed to the testing tool.

**Set Metasploit UserAgent to Google**

**Indexing Spider:** [www.useragentstring.com](http://www.useragentstring.com)

`use`

`auxiliary/fuzzers/http/http_form_fi`

`eld`

`set UserAgent`

`set UserAgent Googlebot/2.1`

`(+http://www.google.com/bot.html)`

### Modify Packet Parameters - STEALTH 2

**Identify the goal before scanning** and send the minimum number of packets.

**Avoid scans that connect with target system** and leak data.

**Do not ping the target or use** synchronize (SYN) and nonconventional packet scans, such as acknowledge (ACK), finished (FIN), and reset (RST) packets.

**Randomize / spoof packet settings** source IP, port address, MAC address.

### Modify Packet Parameters - STEALTH 2 (cont)

**Adjust timing** to slow the arrival of packets at the target.

**Change packet size by fragmenting** packets or appending random data to confuse packet inspection devices.

**nmap** must be run as root

**nmap stealth** <http://nmap.org/book/man-bypass-firewalls-ids.html>

### Anonymity (Tor & Privoxy) - STEALTH 3

**Onion routing enables online anonymity** by encrypting user traffic and then transmitting it through a series of onion routers. At each router, a layer of encryption is removed to obtain routing information, and the message is then transmitted to the next node.

#### + Install Tor

`apt-get install tor`

`nano /etc/Proxychains.conf`

Disable `strict_chains`. Enable

`dynamic_chains`

Edit [ProxyList] and ensure `socks 5`

`127.0.0.1 9050` exists.

**Start Tor** service `tor start`

**Verify Tor** service `tor status`

**Verify Source IP** `iceweasel`

[www.whatismyip.com](http://www.whatismyip.com)

**Invoke Tor Routing with Proxychains**

`proxychains iceweasel`

[www.whatismyip.com](http://www.whatismyip.com)

**Whois** lookup the IP to confirm Tor is active.

**Tor Verify** <https://check.torproject.org>

**DNS Leak Test** [www.dnsleaktest.com](http://www.dnsleaktest.com)

#### ⚠ Note

**Owners of exit nodes can sniff traffic** and may be able to access credentials.

**Vulnerabilities in Tor Browser Bundle** can be used by law enforcement to exploit systems

**ProxyChains does not handle UDP**

### Anonymity (Tor & Privoxy) - STEALTH 3 (cont)

**Some applications will not run** - Metasploit, Nmap... Stealth SYN scan breaks out of proxychains and can leak information to the target.

**Browser applications can leak your IP**

(ActiveX, PDF, Flash, Java, RealPlay, QuickTime).

**Clear & block cookies before browsing.**

#### 👤 Tor-Buddy

Allows you to control how frequently the **Tor IP is refreshed**:

<http://sourceforge.net/projects/linuxscripts/files/Tor-Buddy/>

### Zenmap - STEP 1

#### 📖 Zenmap

<http://nmap.org/zenmap/>

The Official Nmap Security Scanner GUI.

Use this as an entry point and then use nmap scans to gather additional data.

### Maltego

Maltego 👤 [www.paterva.com](http://www.paterva.com) is an **open**

**source intelligence and forensics**

application for visualizing relationships among data that use data mining and link analysis.

### Identifying Network Infrastructure

📖 **traceroute** provides basic information on packet filtering abilities.

📖 **Ibd** Uses two DNS- and HTTP-based techniques to detect load balancers

📖 **miranda.py** Identifies universal plug-and-play and UPNP devices

📖 **nmap** Detects devices and determines the operating systems and their version



`nmap -sSV -A -p- -T5`



`192.168.56.101`





**Shodan** search engine identifies devices connected to the Internet, including those with default passwords, known misconfigurations, and vulnerabilities

### Live Host Discovery

Run **ping sweeps** against a target address space and look for responses that indicate a particular target is live. (TCP, UDP, ICMP, ARP)

 **alive6**  **detect-new-ip6** - IPv6 host detection. detect-new-ip6 runs on a scripted basis and identifies new IPv6 devices when added.

 **dnmap**  **nmap** - nmap is the standard network enumeration tool. dnmap is a distributed client-server implementation of the nmap scanner. PBNJ stores nmap results in a database, and then conducts historical analyses to identify new hosts.

 **fping**  **hping2**  **hping3**  **nping** - Packet crafters that respond to targets in various ways to identify live hosts

### Port Scanning

<http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml>

**Nmap port discovery is very noisy** and will be logged by network security devices.

**Only test necessary ports.**

**Port scanning can impact a network** and old equipment might lock.

### Determining Active Services

**Identify default ports and services.**

**Banner Grabbing**

 **netcat**  **nmap**  **telnet**


**Review Default Web Pages:** Some applications install with default administration, error, or other pages.

**Review Source Code:** Poorly configured web-based applications may respond to certain HTTP requests such as HEAD or OPTIONS with a response that includes the web server software version, and possibly, the base operating system or the scripting environment in use.

### Fingerprinting the OS

**Active:** The attacker sends normal and malformed packets to the target and records its response pattern (fingerprint) which is compared to the database to determine the OS

**Passive:** The attacker sniffs, or records and analyses the packet stream to determine the characteristics of the packets.

 **xprobe2** uses different TCP, UDP, ICMP packets **to bypass firewalls and avoid detection by IDS / IPS systems.**

### Nmap Scripting Engine (NSE)

<http://nmap.org/nsedoc/>

Scripts are written in **LUA**

**Recon of IPv4 & IPv6 DNS data**

**Identify web application firewalls, IDS, IPS**

**Test firewall rulesets** (via firewalk) and attempting to bypass the firewall

**Harvesting user names** from target and online sites

**Brute-force guessing of passwords**


**Crawling the target network** to identify network shares

**Extract EXIF metadata** from images in a defined website

**Geographical localization of IP's**


Network attacks such as IPv6 packet flooding

**Fuzzing and SQL injection testing**

 **Screenshot Web Services**

(wkhtmltoimage)

<http://wkhtmltopdf.googlecode.com>

 **Screenshot NSE Script**

[https://github.com/SpiderLabs/Nmap-](https://github.com/SpiderLabs/Nmap-Tools/blob/master/NSE/http-screenshot.nse)

[Tools/blob/master/NSE/http-screenshot.nse](https://github.com/SpiderLabs/Nmap-Tools/blob/master/NSE/http-screenshot.nse)

### Recon-ng

 **recon-ng**

Modules are written in python.

**show** available modules.

**search** available modules.

**info** information on how the module works.

**show options** options that can be set.

**set** sets the options.

**run** to execute.

**Harvest contacts** (whois, jigsaw, linkedin, twitter)(use the mangle module to extract and present e-mail data)

**Identify hosts**

**Identify geographical locations** of hosts and individuals using hostop, ipinfodb, maxmind, uniapple, wigle

**Identify host information** using netcraft and related modules

**Identify account and password information** that has previously been compromised and leaked onto the Internet (the pwnedlist modules, wascompanyhacked, xssed, and punkspider)

### Vulnerability Scanning

**Loud and easily detected**

**Usually signature based** and can only detect known vulnerabilities with recognition signatures.

**Falsepositive results with a rate as high as 70%**

**Network Scanning Watch List** for devices known to fail when scanned [www.digininja.org](http://www.digininja.org)

 **Scanning may breach laws** in some countries

In Kali, found in Vulnerability Analysis submenu and Web Vulnerability Scanners menu.

**OpenVAS** Open Vulnerability Assessment System

**Nexpose** [www.rapid7.com](http://www.rapid7.com)

**Nessus** [www.nessus.org](http://www.nessus.org)



By **fred**

[cheatography.com/fred/](http://cheatography.com/fred/)

Published 30th July, 2015.

Last updated 12th May, 2016.

Page 2 of 2.

Sponsored by **CrosswordCheats.com**

Learn to solve cryptic crosswords!

<http://crosswordcheats.com>