

Forum:[Hack Forums](#)

Thread: [How To perform Anonymous Port scanning using Nmap and Tor](#)

Unixroot™ - June 10, 2010, 4:42 am

Tor is a network of virtual tunnels that allows people and groups to improve their privacy and security on the Web. It also permits developers / researchers to generate new communication tools with built-in privacy features. Tor provides the foundation for a range of applications that permit organizations and individuals to share information over public networks without compromising their privacy

The Onion Router [TOR] is an excellent work towards defending online privacy. As of with every debate about exploitation frameworks, security tools, vulnerability disclosures such projects have also been victim of criticism, and debates of potential abuse that they may cause and the dangers of teaching individuals a dangerous and potentially illegal craft and a 'secure' channel to hide their online presence. But lets face it, the bad guys already know about it (that is the reason they're bad 'eh). However although these channels of misuse and abuse do exist and they cannot be ignored, still the merits of it will always outweigh the harm black community may cause.

Regrettably in the country I live in even most of the senior know-how people I meet / see / have a chance to work with, don't even have a clue of online privacy or security of their information.

Privacy is every individuals right, and is as important as any other basic human need. You will seldom require somebody tracking your IP, spywares tracing your network activity, and the next time you try to experiment with something, you receive a disagreeable small e mail from an ISP admin that you were doing so-and-so. I am by no way TEMPTING you to do something wrong. Its all about your morale and motivation :) , the small how-to below is a kick starter for getting started with TOR and experimenting with some stuff securely. Interested ? move on, but don't go about emailing me that this stuff like this is illegal to be posted and ought to be removed.

The problem

A basic issue for the privacy minded is that the recipient of your communication / conversation or even otherwise can see that you sent it by taking a look at the IP headers, or worse trace the whole path. And so can authorized intermediaries like ISPs, govt. organizations etc, and sometimes unauthorized intermediaries as well. A very simple type of network traffic analysis might involve sitting somewhere between sender and recipient on the network (man-in-the-middle), taking a look at headers.

But there's also more powerful kinds of packet analysis. Some attackers spy on multiple parts of the Web and use sophisticated statistical techniques to track the communications patterns of plenty of different organizations and individuals. Encryption does not help against these attackers, since it only hides the content of Web traffic, not the headers (VPN ? duh!!) .

The solution:

A distributed, anonymous, secure network

To reduce the risks of both simple and sophisticated traffic analysis by distributing your web traffic over several places / servers, so no single point can link you to your location helps defending your privacy. Its like taking a zig-zag random, hard to follow path to deceive somebody who is tracing you (what the heroes usually do against the villain in action films :)) , then periodically erasing your footprints. In lieu of taking a direct route from source to location, information packets on TOR take a random pathway through several servers that cover your tracks so no observer at any single point can tell where the information came from or where it is going.

TOR incrementally builds a circuit of encrypted connections through servers on the network which is extended one hop at a time, and each server along the way knows only which server gave it information and which server it is giving information to. No individual server ever knows the whole path that a knowledge packet has taken. The client negotiates a separate set of encryption keys for each hop along the circuit to make positive that each hop cannot trace these connections as they pass through.

Two times a circuit has been established any information can be exchanged and because each server sees no over one hop in the circuit, neither an eavesdropper nor a compromised server can use traffic analysis to link the connection's source and location.

Tor only works for TCP streams and can be used by any application with SOCKS support.

to experiment and write this small how-to, I setup a server on the Web that I desired to scan from my home network using Nmap, Nessus, and metasploit from my backtrack suite installed in a VM. Here are the steps I followed to launch the scan / exploitation method by Tor:

A. Installing TOR: Detailed instructions can be viewed on the net site.

B) Download socat .This gizmo is an excellent multipurpose relay and will permit to setup a local TCP listener that will tunnel my connections by the Tor SOCKS server (listening on 9050).

Unfortunately socat comes only on bsd and *nix systems. To make use of TOR on windows I would recommend using Privoxy, or better installing the whole TorCP bundle.

Let us assume that the IP address of the host I desired to scan was

Code 202.163.97.20I invoked socat:

Code [talha@localhost#] ./socat TCP4-LISTEN:8080,fork SOCKS4:127.0.0.1: 202.163.97.20:80,socksport=9050

The above command causes socat to listen on port 8080, and tunnel all incoming connections to 202.163.97.20 (port 80) by the Tor SOCKS server.

For using on windows you will need to:

1. Install privoxy
2. permit HTTP CONNECT requests by 80 through your firewall
3. Browse to <http://config.privoxy.org/show-status>

C. I assume Nmap, Nessus and metasploit are already installed and running. If not you can find the detailed instructions on respective website.

D. Launch an nmap connect or nessus scan against 127.0.0.1 port 8080. Configure Nessus to limit the scan to port 8080 in the "Scan Options" tab.

Here are a quantity of the entries in my Apache log that were a result of the scan:

Code 212.9.32.5 - - [10/Jul/2005:17:29:56 -0700] "GET /Agents/ HTTP/1.1" 404 205 "-"

"Mozilla/4.75 [en] (X11, U; Nessus)"

212.9.32.5 - - [10/Jul/2005:17:29:56 -0700] "GET

/cgi-bin/viewpic.php?id=7&conversation_id=&btopage=0 HTTP/1.1" 404 217 "-" "Mozilla/4.75 [en] (X11, U; Nessus)"

212.9.32.5 - - [10/Jul/2005:17:29:57 -0700] "GET /index.php?err=3&email= HTTP/1.1" 404 207 "-"

"Mozilla/4.75 [en] (X11, U; Nessus)"

212.9.32.5 - - [10/Jul/2005:17:29:57 -0700] "GET

/scripts/fom/fom.cgi?cmd=&file=1&keywords=nessus HTTP/1.1" 404 217 "-" "Mozilla/4.75 [en] (X11, U; Nessus)"

212.9.32.5 - - [10/Jul/2005:17:29:58 -0700] "GET

/scripts/viewpic.php?id=7&conversation_id=&btopage=0 HTTP/1.1" 404 217 "-" "Mozilla/4.75 [en] (X11, U; Nessus)"

212.9.32.5 - - [10/Jul/2005:17:29:58 -0700] "GET /Album/ HTTP/1.1" 404 204 "-" "Mozilla/4.75 [en] (X11, U; Nessus)"

212.9.32.5 - - [10/Jul/2005:17:29:59 -0700] "GET /fom/fom.cgi?cmd=&file=1&keywords=nessus HTTP/1.1" 404 209 "-" "Mozilla/4.75 [en] (X11, U; Nessus)"

212.9.32.5 - - [10/Jul/2005:17:29:59 -0700] "GET /cgi-bin/wiki.pl? HTTP/1.1" 404 213 "-"

"Mozilla/4.75 [en] (X11, U; Nessus)"

The 212.9.32.5 IP address represents the host that is the last onion router in the random circuit that was setup by the Tor program

Similarly two times you discover a vuln in a remote technique, setup another instance of socat: Say for simplicity you are exploiting a webserver (port 80).

[talha@localhost#] ./socat TCP4-LISTEN:1234,fork SOCKS4:127.0.0.1: 202.163.97.20:80,

In metasploit when launching the exploit, set the target IP to 127.0.0.1 and remote port to 1234. Its that simple eh.

The above instructions may even be used to exploit program flaws in order to anonymously execute arbitrary commands on vulnerable hosts.

Some pieces of advice:

1. Nmap makes use of something that generates packets by the raw packet interface so the packets connect directly to the target, not by Tor. For example:

Doing a connect() scan (TCP) will work with Tor but using something like -sS connects directly to the target, revealing your true address.

2. Nmap & Nessus will often ping a target so see if it is up before doing a port scan. This is usually completed by raw ICMP packet's, ICMP won't traverse the Tor network (since its not TCP) and will reveal your true address.

In the usage of socat, socks4 does client side DNS. So you resolve a target host name by DNS from your machine not by the Tor network proxies.

Hence it is impossible to leak your source IP because you tell your scanner to make use of 127.0.0.1 as the target IP . Therefore, nmap / nessus has no host name to resolve, and in case you do forget to tell your scanner not to bother with ICMP pings, you will finish up pinging yourself – not the target directly.

Staying anonymous

Tor cannot solve all anonymity issues. It focuses only on defending the transport of information.

You will need to make use of protocol-specific support program in case you don't require the sites you visit to see your identifying information. For example, you can use web proxies such as Privoxy and open relays while web browsing to block cookies and withhold information about your browser type ident.

Be clever. Don't provide your name or other revealing information in web forms. Be aware that, like all anonymizing networks that are fast for web browsing, Tor does not provide protection against end-to-end timing assaults: If your attacker can watch the traffic coming out of your computer, and also the traffic arriving at your selected location, they can use statistical analysis to discover that they are part of the same circuit.

The Electronic Privacy Information Centre (EPIC) lists down a comprehensive list which servers as a sampling of best available privacy enhancing tools.

tipledown - June 10, 2010, 8:19 am

all copy pasted :D