TOR

19 lezione 23/02/2021

Tor: the onion router

↳ 2nd generation low-latency anonymity network of onion routers that enables users to communicate ANONYMOUSLY across the Internet.

↳ Uses a TCP connections

Tor network users must run a onion proxy on their system, which allows them to communicate to the TOR NETWORK and negotiate a virtual circuit.

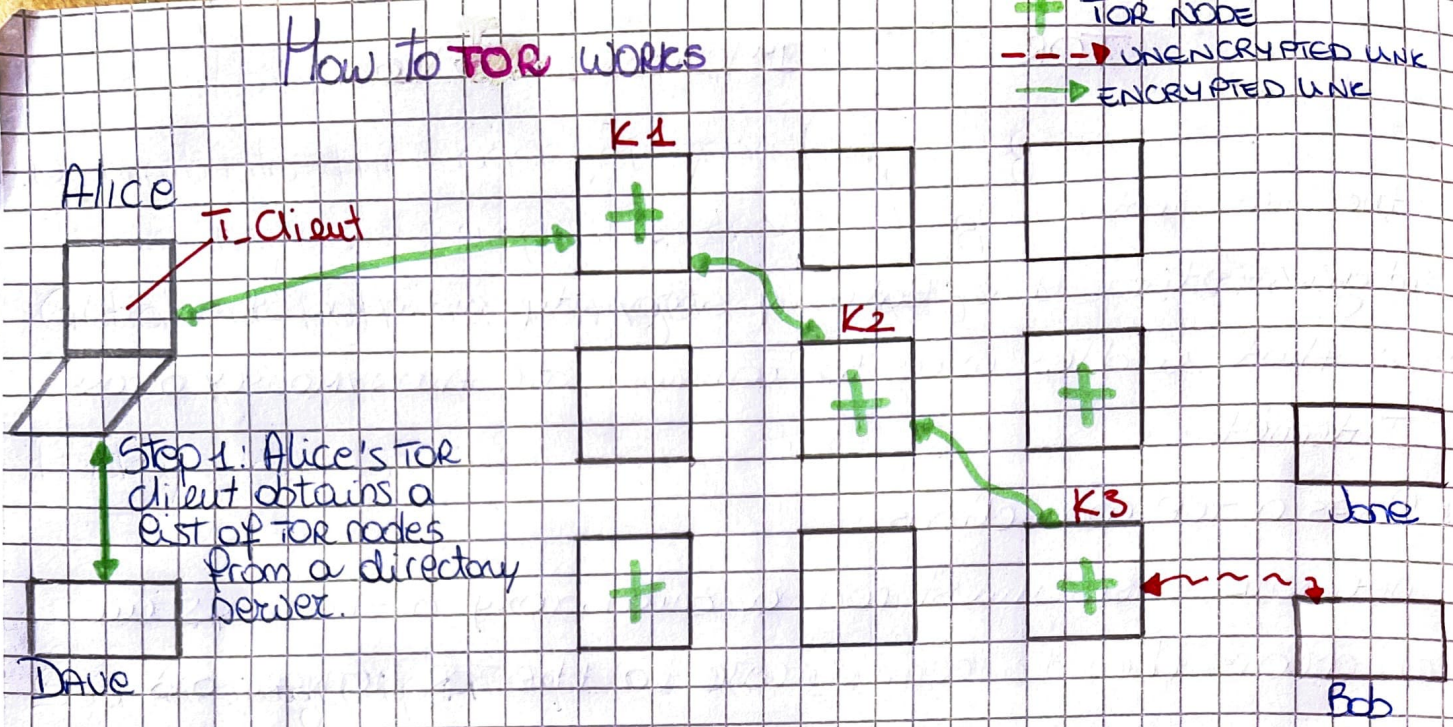
- VIDALIA: GUI for Tor (interfaccia). START/STOP, VIEW THE STATUS of TOR
- PRIVOXY: web filtering proxy. Funzionalità di filtro x la protezione della privacy. MANIPOLA ANCHE COOKIES, MODIFYING WEB PAGE DATA and HTTP headers.
- Tor Resolve: script to connect to a SOCKS proxy that knows about the SOCKS RESOLVE command, hand it a hostname, and return an IP address
- Proxychains: to force connections through TOR
- Scoat: to relay persistently and connections among servers.

More important tools:

- NMap: to scan for open services
  - nmap -sT: used to specify a full connection, rather than a SYN scan
  - nmap -n: used to ensure no DNS requests are performed outside of the Tor
  - nmap -sV: used to perform service & version detection on each open port.
  - nmap -p: used with a common set of ports to probe
  - nmap -PN: used to skip host discovery since he's sure the host is online
- nc (netcat): to send request to servers (check server version) (EXPLOIT VULNERABILITIES TO OWN).

→ To relay informations among different hosts

How to TOR works



Step 2: Alice's TOR client picks a random path to dst server.
Green links are encrypted,
red links are in the clear.

- Alice wants to communicate anonymously with BOB. Alice obtains a list of TOR nodes from a directory server.

TOR node definition - - - -

Alice's TOR client picks a random path to dst server in a path encrypted among some TOR nodes.

Alice $\xrightarrow{msg}$ BOB, the msg m is encrypted several times (ONION)

3 TOR NODES: K1, K2, K3

$E_{K1}(E_{K2}(E_{K3}(m)))$ → 3 times encryption

There's the anonimate because if eavesdropper intercept the clear msg, he see only that the msg is delivered by K3 and Bob, he can't see that who deliver msg is Alice.

TOR directory server → TOR expects certain trusted nodes to act as directory servers providing a list of known routers and their status.

The clear web where is Bob can't see the dark web in TOR.

FOOTPRINTING → IS NECESSARY BECAUSE IT GIVES YOU A PICTURE OF WHAT THE HACKER SEES.
↳ se sappiamo cosa vede un hacker, possiamo proteggerci.

What's footprinting?

The footprinting is the fine art of GATHERING INFORMATION.
↳ generally refers to one of the pre-attack phases; tasks performed before doing the actual attack.
↳ Is the technique used for gathering info about computer systems and the entities they belong to.
↳ Thanks to the use of various tools, attackers can take an unknown entity and reduce it to a specific range of domain names, network blocks, subnets, routers and an individual IP add of systems directly connected to the internet, as well as many other details.

Most important tools:

- TRACEROUTE
- Nmap
- nslookup
- Sam Spade

Step 1:

Determinate the scope of your footprinting activities.

Step 2: Layers 8 & 9: politics and funding

Get proper Authorization; get-out-of-jail-free card

Step 3:

Publicly Available information

Nmap (comandi + usati)

TARGET SELECTION:

Scan: a single ip: nmap 192.168.1.1

a host: nmap www.testhosthome.com

a range of IPs: nmap 192.168.1.1-120

a subnet: nmap 192.168.1.0/24

target from a text file: nmap -iL list-of-ips.txt

PORT SELECTION:

Scan a: single port: nmap -p 22 192.168.1.1

range of ports: nmap -p 1-100 192.168.1.1

100 most common ports: nmap -F 192.168.1.1

dee 65535 ports: nmap -p- 192.168.1.1

SOCAT

opens a proxy listening on localhost:8080 and forwards dee requests through Tor to the target 10.10.10.100:80

bt~# socat TCP4-LISTEN:8080,fork

SOCKS4a:127.0.0.1:10.10.10.100:80,socksport=9050 &

Company web pages

Many times, a website provides excessive amounts of information that can aid attackers. We have actually seen organizations list security configuration details & detailed asset inventory spreadsheets directly on their Internet web server.

- Try reviewing the HTML source code for comments.

  Wget (unix) — Teleport Pro (windows)

- Things buried in comment tags: <, !, --

- Discovery sometimes requires brute-force techniques to enumerate "hidden" files and directories on a website.

  OWASP's DirBuster
  - attempts to enumerate hidden files and directories RECURSIVELY
    - ci restituisce un report con tutte le varie info.

- Easy to be detected: proxy through privoxy

- Remote access to internal resources via browser
- Microsoft Exchange server: proxy to internal server.

- Look for other sites beyond the main
  - VPN sites
  - www1, www2, web, test, ect.

Un hacker può fingersi un impiegato ed ottenere molte info, chiamando l'assistenza x le VPN ad esempio.

Related Organizations

CSS files just recently, indicating that the target's web development was outsourced
↳ partner company → aren't as security-minded
is now a potential
target for attack too.

Location Details

A physical address can prove a very useful to determined attacker.
↳ dumpster-diving,
surveillance,
social engineering
and other attack.

GOOGLE EARTH
↳ which can be found
at earth.google.com

→ you can see addresses with amazing clarity and detail via a well-designed client app.

STREET VIEW: "drive-by" series of images so you can familiarize yourself with the building, its surroundings, the street, and traffic of the area.

Google street it's also tracking any wi-fi networks and their associated MAC addresses that it encounters along the way. (Google location and skyhook)

Employee Information

Most organizations use some derivative of the employee's name for their username and email add.
Have a username → access to the system resources.

Attackers may also use your phone number to help them target their war-dialing ranges, or to launch social engineering attacks to gain additional info and/or access.

▸ peoplesearch.com
gives hacker personal details ranging from homephone numbers and addresses to social security numbers, credit histories, criminal records, etc...

The website you should frequent in your footprinting searches include social and info networking sites, professional networking sites, career management sites and family ancestry sites.

Employee directories can be purchased through business directory services such JigSaw.com.
↳ these sites used by sales teams who pay for prospective client contact information for the purposes of cold-call introductions.

More business directory sites also institute a reward system to incentivize their members to keep contact records current.
↳ the centralization and currency of this info is very helpful for the attacker.
↳ social engineering and phishing attacks.

Data-mining tools like MAITEGO are available for sifting through the burgeoning number of information sources and drawing relationship maps between the data points collected.
An attacker can also obtain information from job advertisements posted by companies.
→ monster.com, careerbuilder.com

Attackers can be disgruntled or ex-employees and they can take advantage of sites that provide info about the internal organization.

Current Events
One of the first things to happen after a merger or acquisition is a blending of the organizations' networks.
If a company is a publicly traded company, information about current events is widely available on the internet.
↳ They are required to file certain periodic reports to the Securities and Exchange Commission (SEC) on regular basis; these reports provide a wealth of information.

10-Q (quarterly)
&
10-K (annual) reports
↳ EDGAR database sec.gov to see them.

Business info and stock trading sites such Yahoo! Finance message boards, can provide similar data. An attacker can use this info to target weak points in the organization.

PRIVACY OR SECURITY POLICIES AND TECHNICAL DETAILS INDICATING THE TYPES OF SECURITY MECHANISMS IN PLACE.

→ hardware and software protection

Archived Information

Be aware that there are sites on the Internet where you can retrieve archived copies of info that may no longer be available from the original source.

↳ WayBack Machine at archive.org

Search Information and Data Relationships

The search engines available today are fantastic. Within seconds, you can find just about anything you could ever want to know. Many of today's popular search engines provide for advance searching capabilities that can help you hone in on that tidbit of info that makes the difference.

↳ google.com, bing.com, yahoo.com, dogpile.com

If you search Google for allinurl:tsweb/default.htm Google reveals Microsoft Windows servers with Remote Desktop Web Connection exposed. See GHDB.

Tools like FOCA are designed to identify and analyze the METADATA stored within a file. Foca utilizes some of the same search engine hacking techniques described earlier to identify common document extensions such as: .pdf, .doc(x), .xsl(x) and .ppt(x). Once analyzed, the tool categorizes the metadata results into summary information. One feature integrated

uto Foca, and worth exploring on its own, is the use of the Sentient Hyper-Optimized Data Access Network (SHODAN). SHODAN is a search engine that's designed to find Internet-facing systems and devices using potentially insecure mechanisms for authentication & authorization.
For example, a simple search for "pix firewall config help" yields hundreds of posting from people requesting help with their CISCO PIX firewall configurations.
Some of these postings actually include CUT and PASTED copies of their production configuration, including IP addr, ACLs, PSW hashes, NAT mapping, etc... If the person in need of help knows to not post configuration details to a public forum like this

↳ people might still pray to a SOCIAL ENGINEERING ATTACK.

MALTEGO have been created to data mine and link relevant pieces of info on a particular object.
It provides the ability to aggregate and correlate info and correlate info and then display those relationships to the user in an easy-to-understand graphical representation.

PUBLIC DATABASE SECURITY COUNTERMEASURES

The Site Security Handbook (RFC 2196) is a wonderful resource for many policy-related issues.