Teoria e Prática de Ataques de Segurança

2025/2026

André Baptista
andre.baptista@fc.up.pt

Miguel Regala
miguel.regala@fc.up.pt

https://tpas.alunos.dcc.fc.up.pt

FACULDADE DE CIÊNCIAS
UNIVERSIDADE DO PORTO

Class 5

Enumeration and passwords
Vulnerability scanning
Anonymization mechanisms

FACULDADE DE CIÊNCIAS
UNIVERSIDADE DO PORTO

Enumeration and passwords

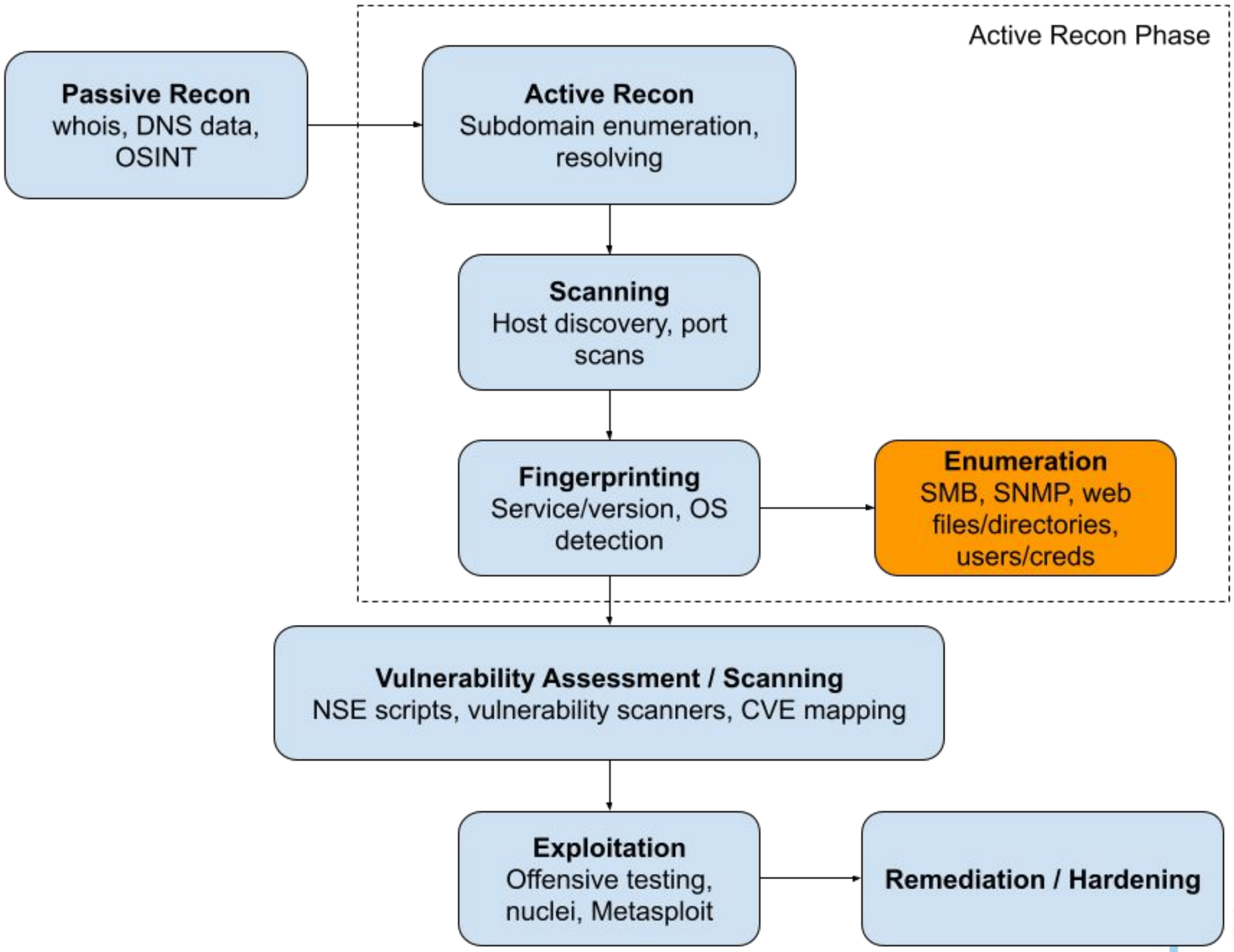
FACULDADE DE CIÊNCIAS
UNIVERSIDADE DO PORTO

Enumeration

- Scanning allowed us to identify alive hosts, IP addresses, machines, operating systems, and some potential vulnerabilities.

- However, we can perform **additional scanning techniques** to identify important information that can lead to multiple attack vectors:
  - Usernames, groups, passwords
  - Email addresses
  - Authentication domains and other providers (SSO)
  - Default credentials, bad permissions
  - SMB Shares, routing tables
- This is called **enumeration.**

Enumeration



Enumeration

- We can try to perform enumeration from multiple services (and others):
  - TCP 53: DNS
  - TCP 135: MS RPC endpoint
  - TCP 137: NetBIOS name service
  - TCP 139: NetBIOS session service
  - TCP 445: SMB over TCP
  - UDP 161: Simple Network Management Protocol (SNMP)
  - TCP/UDP 389: LDAP
  - TCP 25: Simple Mail Transfer Protocol

NetBIOS

- NetBIOS is a service/API that allows us to list resources available within a network.
    - Works over the session layer and provides naming services and messages.
- In Windows hosts, a NetBIOS service is usually active if "File/Printer Sharing" has been allowed.
- We can try to dump a list of available **resources**, information about **users** and **groups**.
- It's possible to list NetBIOS resources with multiple tools: `nmblookup`, `nbtscan`, SuperScan (old and Windows only)
- Other protocols may publish and reveal usernames without any protections within the network. NetBIOS is just one of them.

SNMP

- SNMP is used to manage network devices within a network.
- A device runs an agent that answers to requests:
  - Reading configurations (read-only password)
  - Changing configurations (read/write passwords)
- When these passwords are not changed, an attacker can leverage their default values to enumerate network configurations and create backdoors.

NTP

- Many organizations keep services centralized for clock synchronization and user directories.

- NTP (Network Time Protocol) allows a set of hosts to retrieve information about the time of a given host.

- The `ntp` toolbox (Linux) allows us to retrieve information, e.g. what hosts are synchronizing time from a specified **NTP server**.

LDAP

- LDAP (Lightweight Directory Access Protocol) allows centralizing operations of authentication of users and storage of attributes (and permissions).

- When available in a network, a misconfigured LDAP server allows us to read information about **users** and **resources** within a system (a similar example for Windows-based infrastructure is Active Directory)

Tooling

- The **`enum4linux`** tool tries to include a set of techniques from multiple, simpler tools available in Linux environments:
  - `smbclient, smbmap, rpcclient, net`
  - `nmblookup, nbtscan, ldapsearch`
- Since we can run multiple tools simultaneously, it’s an alternative to a more careful, manual research of information shared within a network.

SMTP

- Simple Mail Transfer Protocol is a protocol used for email delivery.
- An SMTP server answers to 3 user related types of commands:
  - VRFY - user validation
  - EXPN - can reveal real email addresses through mailing lists
  - RCPT TO - defines recipients for messages
- We can use these commands to understand if it’s possible to list users within an email system.
- Useful tool: https://github.com/cytopia/smtp-user-enum

DNS

- DNS servers accept **Zone Transfer** requests sometimes
- This feature is usually for DNS record propagation
- A proper query can reveal to a given client a set of DNS records (including internal records)
- `dig @ns1.example.com example.com AXFR`

Countermeasures

- Turn off SNMP agents or use recent versions that protect passwords and messages
- Block access to port 161 (SNMP)
- Don’t allow DNS zone transfers / whitelisting for secondary DNS servers only
- Configure SMTP servers to ignore messages from unauthenticated or invalid users
- Enforce authentication for LDAP
- **Turn off unnecessary shared services and enforce authentication**

Passwords

- Sometimes, the easiest way to penetrate a system is to find valid credentials of a legitimate user. There are a few shortcuts:
  - Default credentials for routers and other devices
  - Released password dumps
  - Password files (hash cracking, dictionary attacks)
  - Social engineering (including phishing)

Passwords

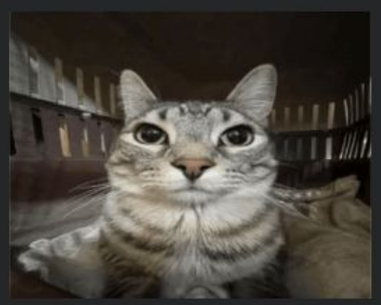
BreachForums › Leaks › Combolists › **ACESSO.GOV.PT 12K** Today's posts

Pages (3): 1 2 3 Next » New Reply

ACESSO.GOV.PT 12K

by BrotherArthur - Saturday August 10, 2024 at 09:11 PM

BrotherArthur



VIP User

VIP

Posts: 65

08-10-2024, 09:11 PM #1

AT autoridade tributária e aduaneira

Hey there **breachforums**!
I'm giving away this for free!
A combolist composed of login credentials for acesso.gov.pt/v2/login, a portuguese government website for tax purposes and much more, lots of juicy personal details from people there

The combolist is composed of 12470 lines

NAME:PASSWORD
(Name is their tax id number)

Default credentials

- There are multiple websites and databases on the internet that allow us to access default credential lists
  - Examples: https://open-sez.me/, https://www.routerpasswords.com/

- **Challenge:** search for a device that you own on the internet (router, etc). Did you change the default password?

Password dumps

- Many huge data leakages have been happening in the past years, including PII, emails, passwords, phones numbers, and more.

- Example:
  https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

- **Challenge:** try to find one of your passwords or hashes in one of these databases. Verify what an attacker could compromise.

- https://haveibeenpwned.com, https://dehashed.com/

- Mitigation: use password managers with strong, unique passwords.

Password attacks

- **Passive**
  - man in the middle, sniffing, replay attacks
- **Active**
  - password guessing (aka bruteforce)
  - trojans, spyware, keyloggers
  - phishing

Passwords - Linux

- Passwords are stored in `/etc/shadow`
- They are stored with salted hashes:
  - `salt, H(salt || password)`
- Currently: `H = sha512`
- Salting makes attacks against passwords harder. Otherwise, we could simply search in hash databases (rainbow tables).
- However, it's still possible to launch dictionary and bruteforce attacks.
- These are impossible to mitigate if an attacker retrieves hashes (one-way functions that transform passwords) [assuming secure hash function]

Passwords - Windows

- Windows systems store passwords in SAM (Security Accounts Manager) files.

- Mechanisms are in place for protecting these files against multiple attacks.

  - Kernel has an exclusive lock over files

  - Information is partially encrypted

- Passwords are stored in files with **hash values** LM/NTLM (MS proprietary)

Password cracking

- When we manage to access a login system, and we are sure about a username and/or if we manage to retrieve a file with password hashes, we can launch multiple attacks:
- Bruteforce
- Dictionary
- Hybrid or rule-based / mask
- Language-specific wordlists

Hashcat

- **hashcat** is a tool for password ~~recovery~~ cracking
- `$ hashcat --help` -> bring up all the options
- `$ hashcat -m 0 -a 3 -1 “?l” “0xhash” “?1?1?1?1?1?1”`

Vulnerability Scanning

Vulnerability scanning

- Vulnerability scanning identifies potential weaknesses and entry points in systems that we can try to exploit.

- Vulnerabilities come from:
  - Network topology
  - Operating system
  - Open ports and running services
  - Configuration errors in applications and services
  - Outdated applications and services (or properly updated - 0days)

Tools

- Vulnerability scanning takes time and relies on matching **known signatures** or **behaviors** stored in databases.

- Many tools automate these processes and are sold to organizations to help them identify attack vectors and mitigate vulnerabilities.

- However, these tools can also be used by attackers and external security researchers to identify (and exploit) vulnerabilities.

- Examples: Burp Suite Pro, Acunetix, Nessus - free trials available

- Other open-source tools exist: openVAS, nikto, nuclei, OWASP ZAP

- Static analysis: brakeman, flawfinder, nodejsscan, semgrep, LLMs

Finding vulnerabilities

- We can use automation and tools, but the most powerful testing is manual (human).

  - Our goal is to **understand the target** system (specific research, e.g. if we are dealing with compiled software, we should perform reverse engineering, if we're dealing with a webapp we should identify endpoints and APIs, etc).

  - Can user input trigger unwanted flows in a system?

  - For web applications, **manipulating HTTP requests** is essential for playing with user input.

  - Vulnerability research in 3rd party or open-source software and technologies used by a target can lead to unknown attack vectors and 0days.

Exploiting vulnerabilities

- When we find a vulnerability:
  - We should try to understand the exploitability, impact, and mitigations
  - If the vulnerability is known, are there any exploits available?
    - **Yes:** Exploit (run public exploits from exploit DB, metasploit, search for PoC code on GitHub, blog posts, CTF Writeups, etc)
    - **No:** Try to build an exploit. Research.
- Is this a new vulnerability or specific to the current target?
  - Build an exploit or a PoV (Proof of Vulnerability)

Metasploit

- Metasploit is a framework that allows us to run exploits and auxiliary modules.
  - Contains an exploit database with regular updates (`msfupdate`)
  - Provides payloads for command execution and fancy reverse shells with many features (e.g. `meterpreter > soundrecorder`, `screenshot`)
  - It makes running exploits easier against a given target
  - Generic `msfconsole` commands: `search [exploit]`, `use [exploit]`, `set RHOST [ip address, hostname]`, `set PAYLOAD [payload]`, `exploit`

Metasploit

- Basic Metasploit flow:

1. `search nginx` -> search modules for target software
2. `use nginx_mod_1` -> use that module
3. `show targets / SET target X` -> specify target (e.g. linux x86, linux ARM, etc)
4. `show payloads / SET payload X` -> what payloads are available for this module + target combination
5. `show options` -> current module + payload options
6. `SET RHOSTS target_ip` -> set target IP
7. … etc. Always check current options to see what needs to be set
8. **`exploit`**

```
[*] Command shell session 1 opened (100.89.47.82:4444 -> 100.101.228.35:35202)
```

Anonymization mechanisms

Proxies

- Proxies are widely used to control, route, and anonymize network traffic.
- Attackers use proxies to:
  - Avoid leaking real IP addresses to log files
  - Bypass authorization mechanisms as a trusted origin (firewall bypass)
  - Diversify the origin of scanning and exploitation and make tracking harder
  - Proxy **chaining** is a common technique:
    `User -> Proxy1 -> Proxy 2 -> Proxy … -> Proxy n -> Webpage`

Types of proxies

- HTTP and HTTPs proxies
  - HTTP based
- SOCKS4 and SOCKS5
  - TCP based
  - Better for non HTTP traffic
- Network based

How to use?

- `curl -x http://proxy:port https://example.com`

- `HTTP_PROXY=http://proxy:port HTTPS_PROXY= http://proxy:port curl https://example.com`

- Browser extensions, OS system settings

VPN - Virtual Private Network

- A VPN, makes a private network accessible from a public network. It allows users to send and receive packets as if they were directly connected to the private network.

- There are paid VPN services that allow users to change their IP address easily and access location-based forbidden content (e.g. hide.me, nordvpn.com, protonvpn.com).

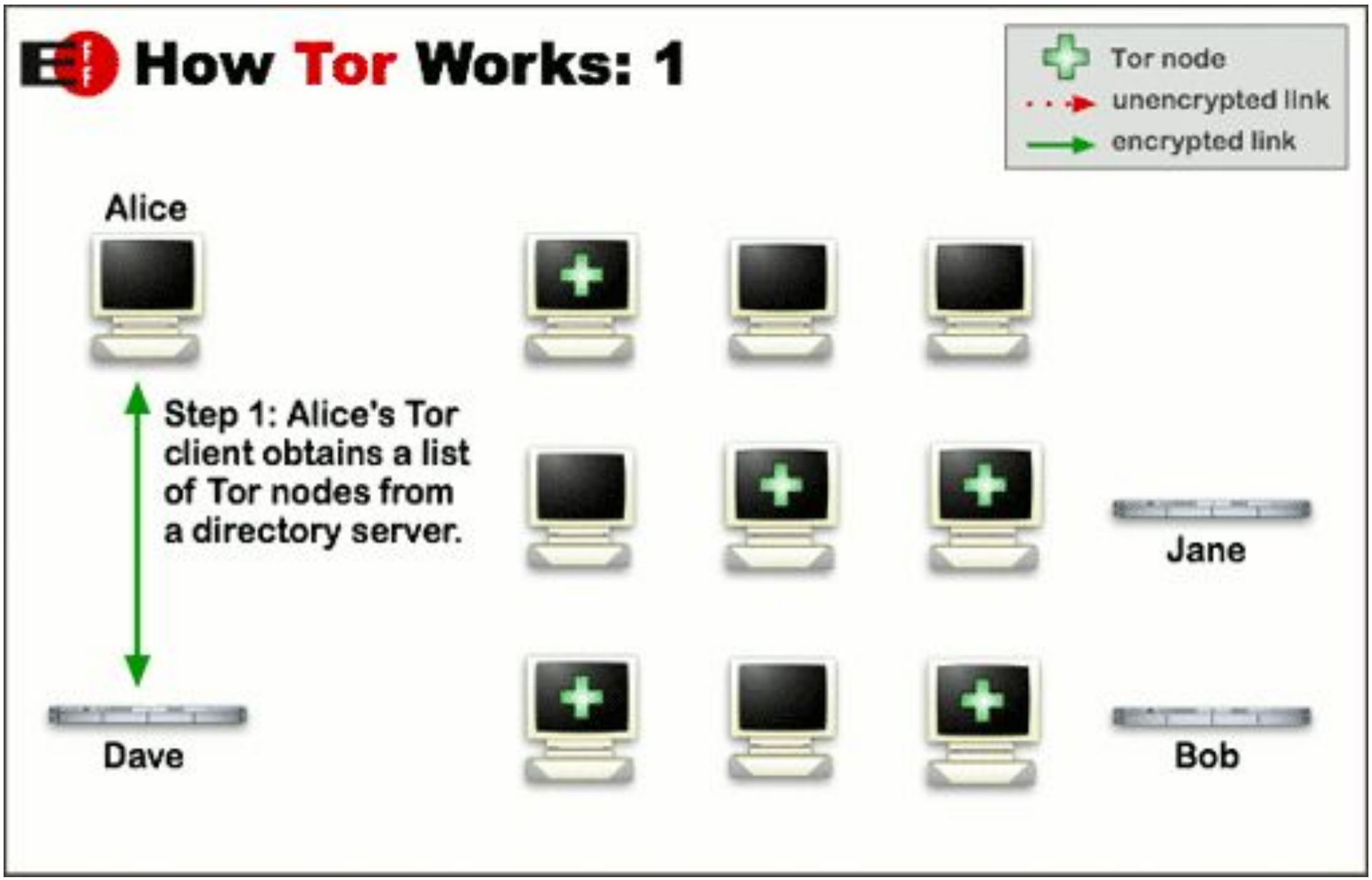
- Attackers also use VPN services to launch attacks from different locations.

- Some VPN providers don’t store logs (but most do).

TOR

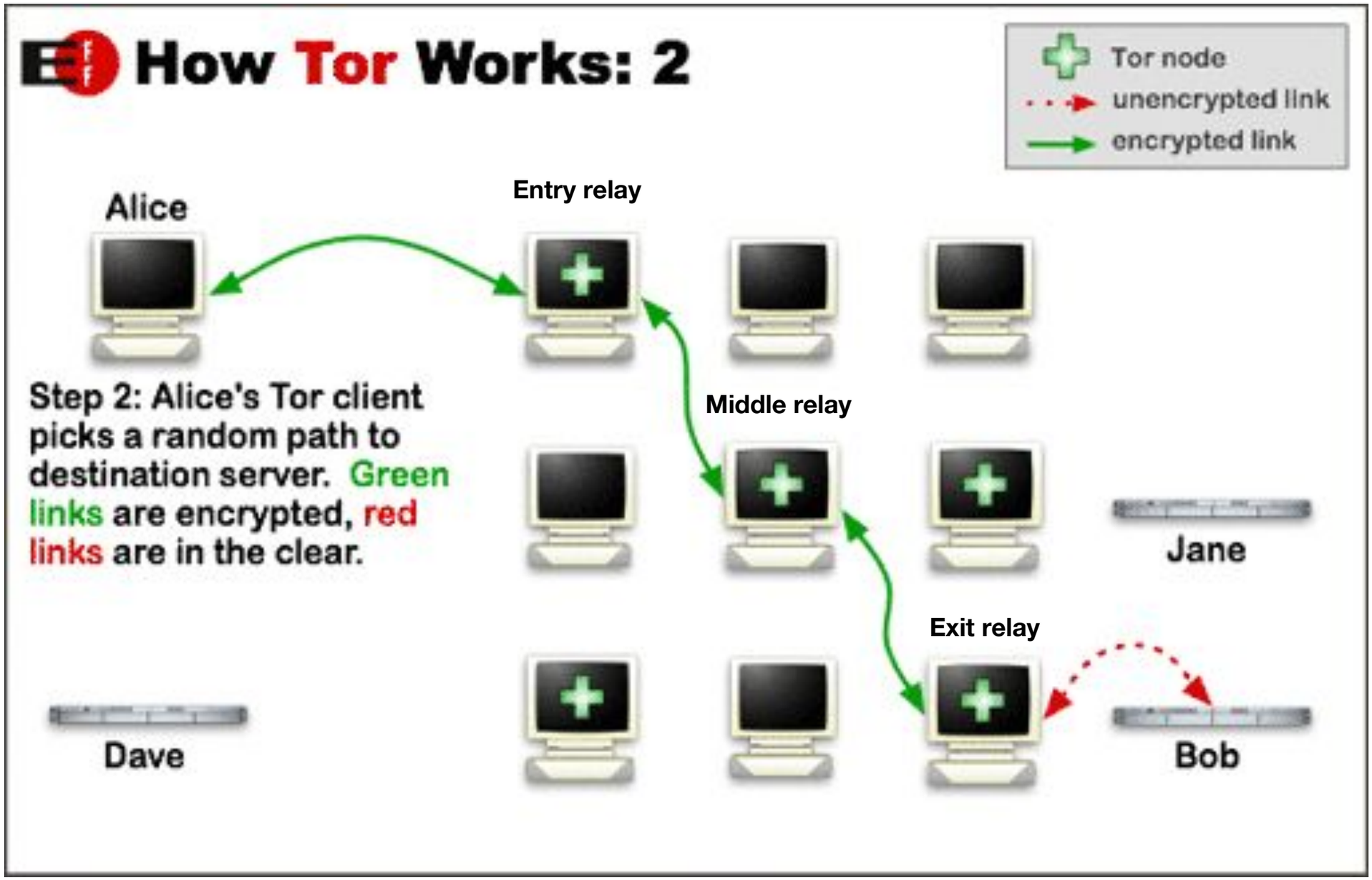
- Network composed of volunteer nodes.
- Allows anonymization of users and servers.
- The goal is to protect the privacy of the users for a free internet.
- However, TOR has been used by attackers or hacktivists to launch attacks, sell exploits, and other sensitive content (PII, credentials, etc).
- Deep/dark web (.onion) -> Silk road, dumps…
- We can route all network traffic through TOR: torctl, proxychains

TOR - How it works?



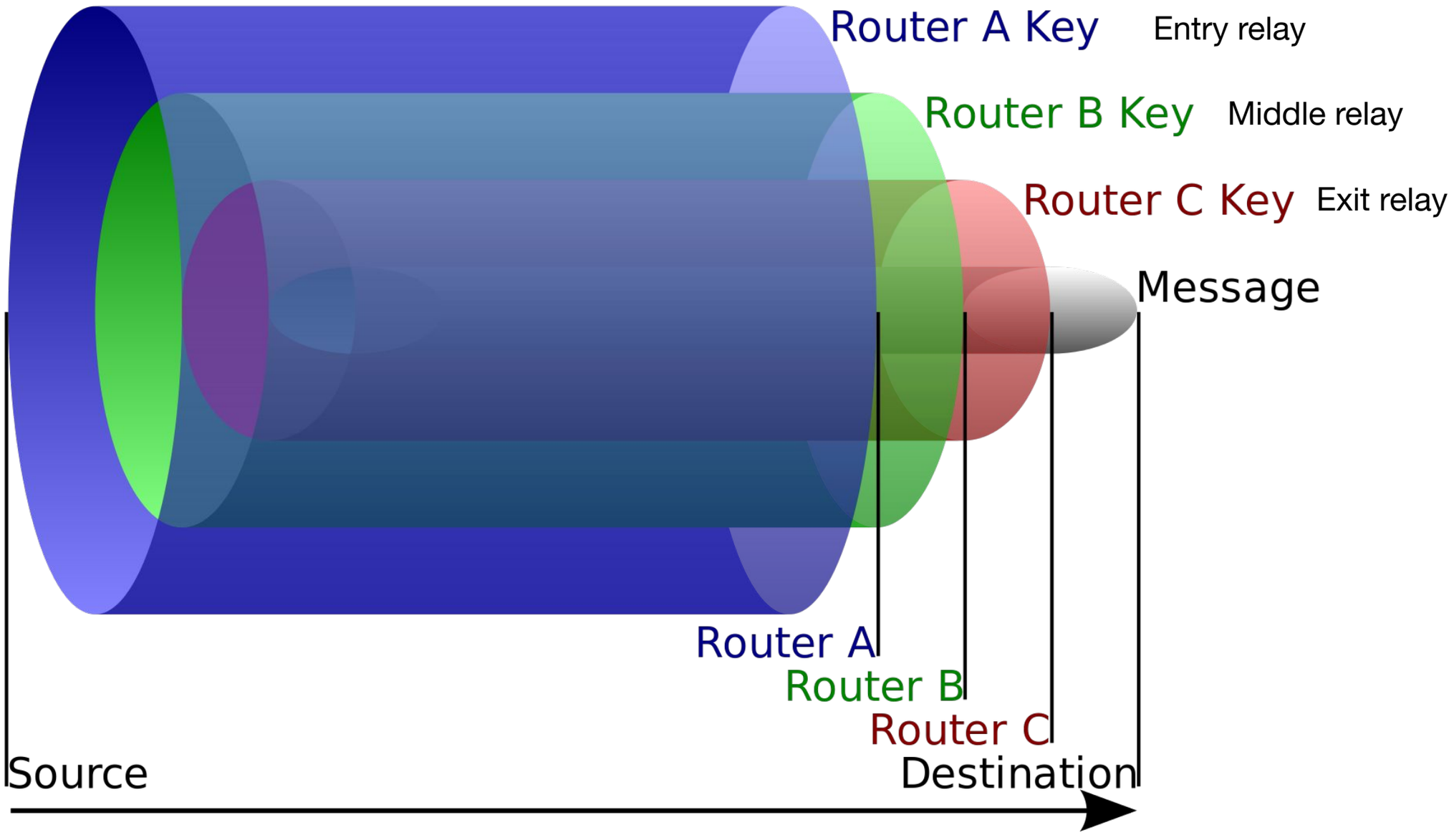
From: torproject.org

TOR - How it works?

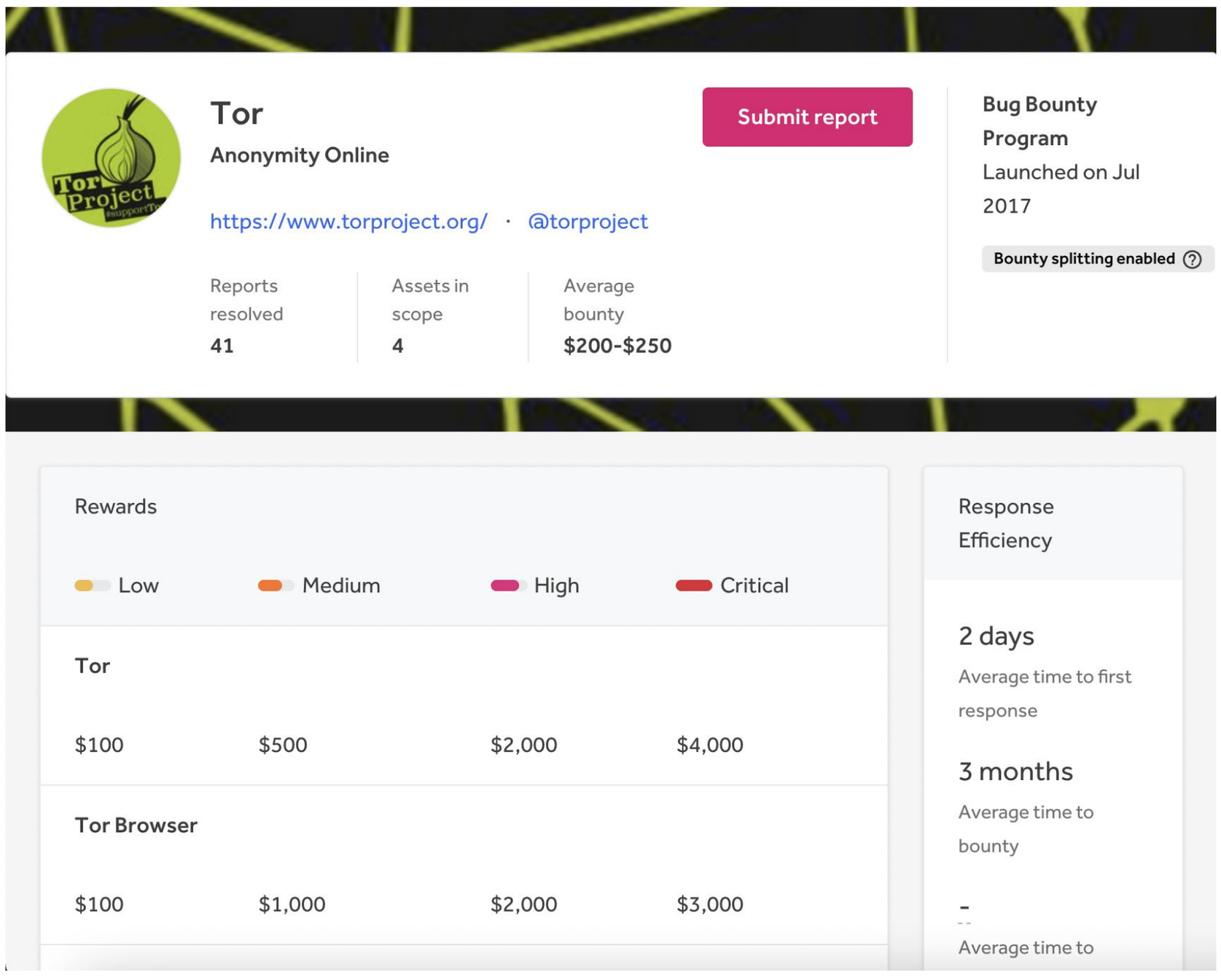


From: torproject.org

TOR - Onion routing



TOR - Bug Bounties



From: HackerOne

TOR - “Bug Bounties”

Table expired (2021). For a limited time, they paid up to 1M USD per exploit

Software / OS	JavaScript Blocked (Security Settings: HIGH) RCE+LPE to Root/SYSTEM	JavaScript Blocked (Security Settings: HIGH) RCE Only (No LPE)	JavaScript Allowed (Default) (Security Settings: Low) RCE+LPE to Root/SYSTEM	JavaScript Allowed (Default) (Security Settings: Low) RCE Only (No LPE)
Tor Browser on Tails 3.x (64bit) **AND** on Windows 10 RS3/RS2 (64bit)	$250,000	$185,000	$125,000	$85,000
Tor Browser on Tails 3.x (64bit) **OR** on Windows 10 RS3/RS2 (64bit)	$200,000	$175,000	$100,000	$75,000

From: Zerodium

TOR vs Proxies vs VPN

Tor Pros:

+ Anonymity is guaranteed, masking the true origin of traffic
+ Traffic is encrypted in the network
+ Can be combined with a VPN as an extra layer

Tor Cons:

- There is no way to understand who controls the nodes that are being used by us
- There are suspicions that NSA has been controlling several nodes within the network
- DNS leaks: https://torguard.net/vpn-dns-leak-test.php

TOR vs **Proxies** vs VPN

Proxy Pros:

+ Public proxies are free
+ Many are sufficient for basic web browsing
+ They can unlock content restricted to a given location (country, etc)
+ They can help bypassing network restrictions
+ Multiple protocols: HTTP, HTTPS, SOCKS (additional security)

Proxy Cons:

- Many don’t provide encrypted channels (HTTP proxies - traffic can be sniffed)
- Who’s making the proxy available? Sometimes is hard to tell.
- Public proxies are unstable and unpredictable

TOR vs Proxies vs **VPN**

VPN Pros:

+ We can trust some VPN providers
+ Strong cryptography protocols are used on connections
+ VPNs can work pretty much as a proxy for connections
+ DNS leak protections, private DNS, firewalls
+ We can choose our geolocation
+ There are providers with different log policies

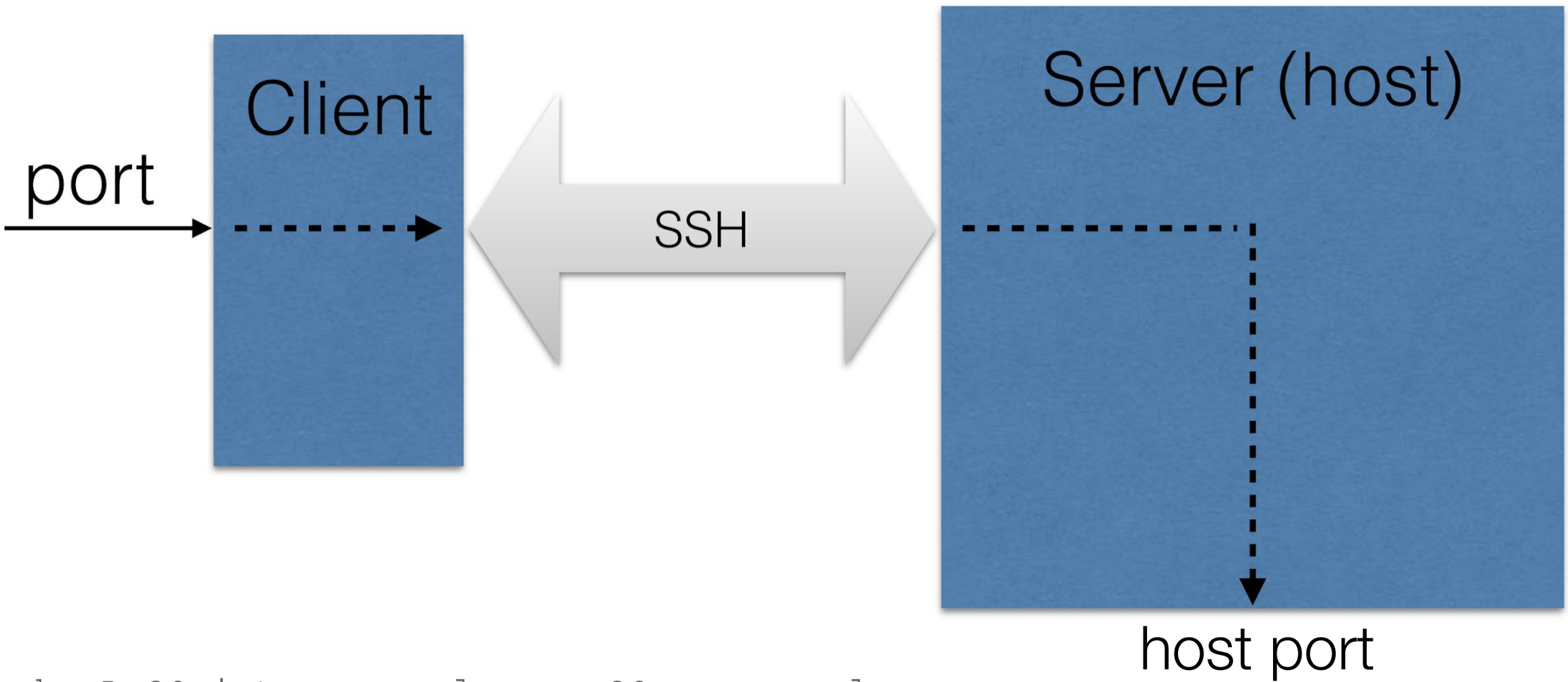
VPN Cons:

- The best VPNs are not free
- Using a VPN adds a little bit more CPU and memory overhead
- VPN companies routinely log and hand over your information to government when asked/compelled (e.g. ProtonVPN)

HTTP/SSH tunneling

- HTTP(S) ports (80, 443) are not usually blocked for outgoing traffic in firewalls.
- This allows us to create communication channels that look like HTTP(S) traffic.
- These channels are tunnels for other types of network traffic and allow us to reach other ports.
- They allow network traffic, including protocols using encryption through firewalls.
- Example: http://http-tunnel.sourceforge.net/
- Other protocol example: https://github.com/DhavalKapil/icmptunnel
- SSH tunnels are other way to mask addresses and bypass firewalls.

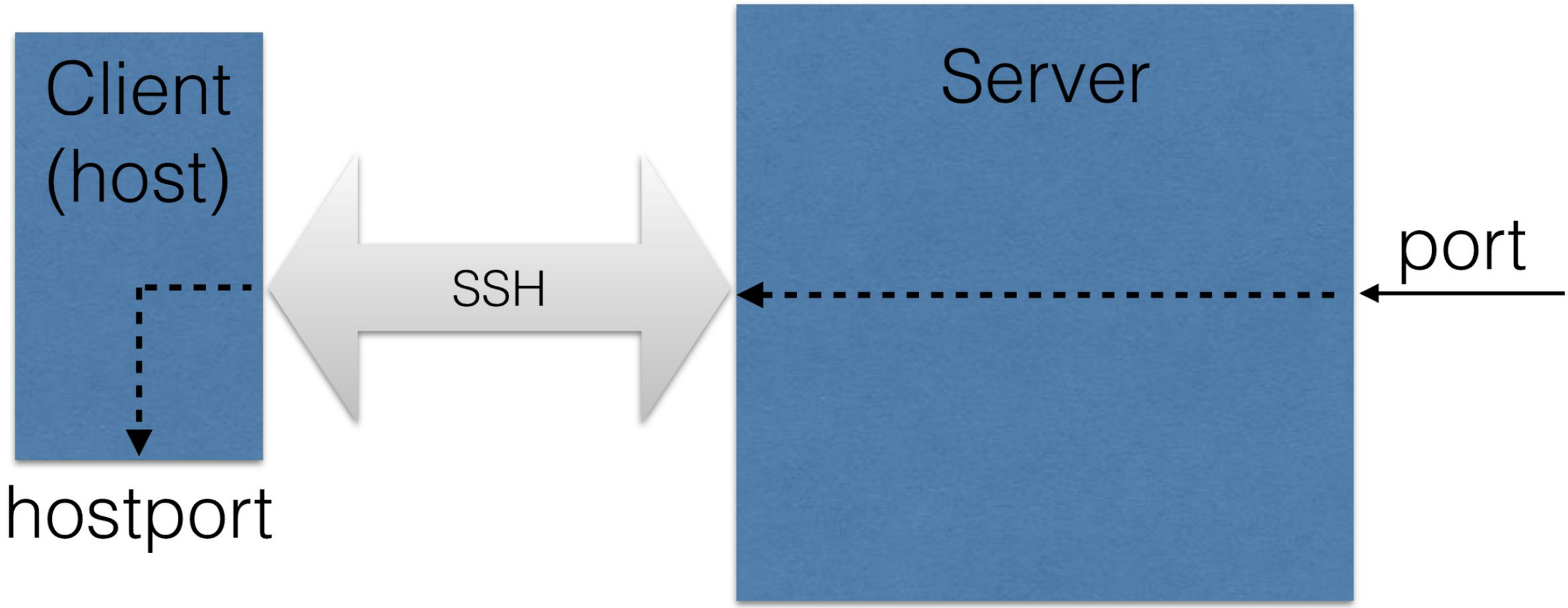
SSH: Local to Remote (-L)




```
ssh -L 80:intra.example.com:80 gw.example.com
```

This example opens a connection to the `gw.example.com` jump server, and forwards any connection to port 80 on the local machine to port 80 on `intra.example.com`

SSH: Remote to Local (-R)




```
ssh -R 8080:localhost:80 public.example.com
```

This allows anyone on the remote server to connect to TCP port 8080 on the remote server. The connection will then be tunneled back to the client host, and the client then makes a TCP connection to port 80 on `localhost`. Any other reachable hostname or IP address could be used instead of `localhost` to specify the host to connect to.

SSH: Socks proxy

- `ssh -D 8080 username@sshd_server`

- Configure the browser to use a socks5 proxy:
  `127.0.0.1:8080`

- Proxychains is also useful

Laboratório

- Testar o TOR, verificar o IP público, fazer DNS leak test
- Instalar e explorar o metasploit (`msfconsole`)
- Resolver o desafio lab 03 no https://tpas-desafios.dcc.fc.up.pt
- Implementar o exploit numa linguagem de programação à escolha para 50 pontos extra