Ethical Student Hackers

Online Anonymity

SHEFFIELD Ethical Student Hackers

Breaking into security.

Welcome Back!

- Hope you all had a lovely break and managed to do something that wasn't revision related
- Today's session is all about online anonymity
  - How it can be 'achieved'
  - What limitations technologies have
  - How it can be compromised
- We'll be covering various technologies - VPNs, Tor and I2P
- We'll look at attacks on these anonymity solutions
- And we'll take you through setting up your own

SHEFFIELD Ethical Student Hackers
Breaking into security.

The Legal Bit

- The skills taught in these sessions allow identification and exploitation of security vulnerabilities in systems. We strive to give you a place to practice legally, and can point you to other places to practice. These skills should not be used on systems where you do not have explicit permission from the owner of the system. It is VERY easy to end up in breach of relevant laws, and we can accept no responsibility for anything you do with the skills learnt here.

- If we have reason to believe that you are utilising these skills against systems where you are not authorised you will be banned from our events, and if necessary the relevant authorities will be alerted.

- Remember, if you have any doubts as to if something is legal or authorised, just don't do it until you are able to confirm you are allowed to.

SHEFFIELD Ethical Student Hackers
Breaking into security.

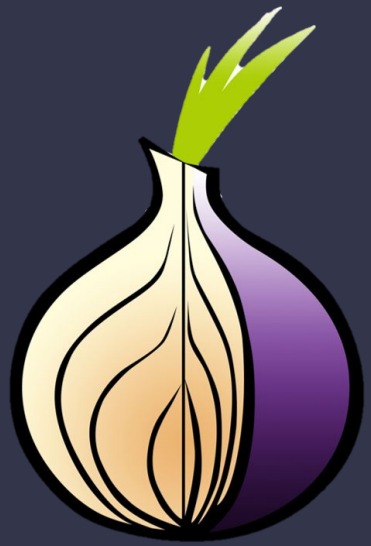
Code of Conduct

- Before proceeding past this point you must read and agree to our Code of Conduct - this is a requirement from the University for us to operate as a society.
- If you have any doubts or need anything clarified, please ask a member of the committee.
- Breaching the Code of Conduct = immediate ejection and further consequences.
- Code of Conduct can be found at https://shefesh.com/downloads/SESH%20Code%20of%20Conduct.pdf

SHEFFIELD Ethical Student Hackers
Breaking into security.

Anonymity Techs

And how to use them



Basics of Proxies

- Proxies create an indirect connection to their destination
  - Packets are routed towards a proxy server, and forwarded on
  - Some proxies mask the original source's IP address ('anonymous' proxies) and some preserve them ('transparent' proxies)

- SOCKS Proxies
  - Designed to route any kind of traffic at layer 5 (Session layer) or above
  - Often used for communicating over firewalls; also used by Tor (more on this later)
  - Doesn't interpret packets as they come through - just forwards them
  - Creates a TCP session - therefore supports authentication, and SSH tunneling

- HTTP
  - Creates a brand new, identical request, and sends this
  - May include an X-Forwarded-For header in a transparent proxy

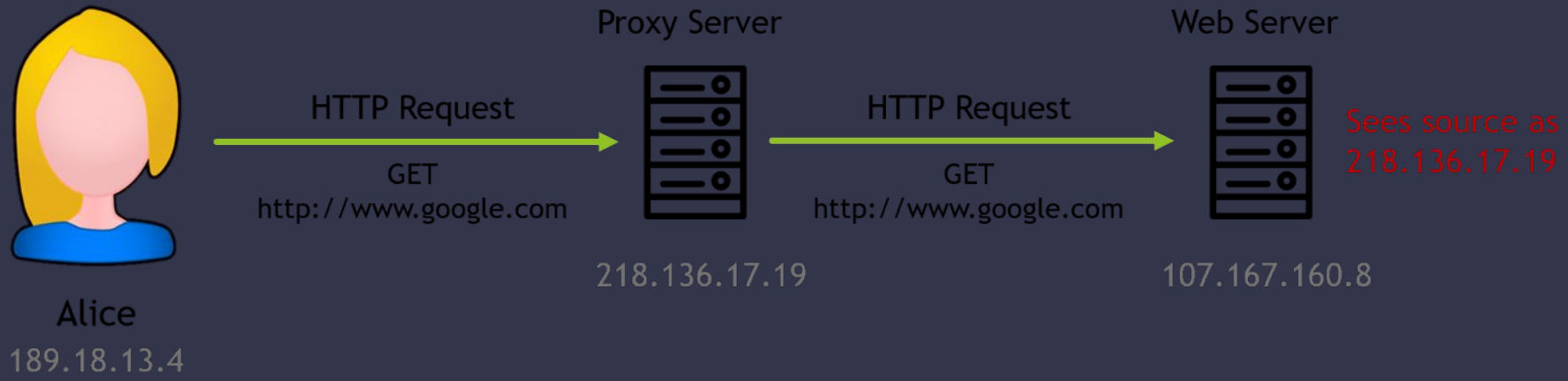
SHEFFIELD Ethical Student Hackers
Breaking into security.

Uses of Proxies

- Bypassing geolocation filters & IP bans (in theory)
- Load Balancing & Firewalls
  - Allows packet inspection
  - Allows separation from internal network
- HTTPS proxies are possible using the CONNECT HTTP verb
- Many common tools allow a proxying option, for example to pass traffic to Burp Suite
  - Curl: -x, --proxy <[protocol://][user:password@]proxyhost[:port]>
  - WFUZZ: -p localhost:8080 or -p localhost:2222:SOCKS5
  - SQLMap: --proxy=http://127.0.0.1:8080
  - Gobuster: -p http://127.0.0.1:8080

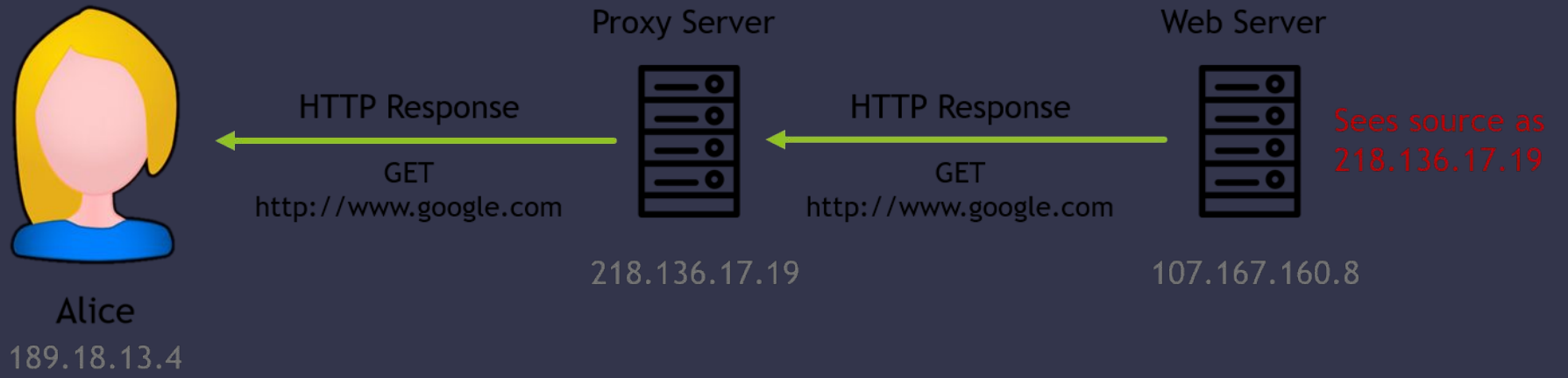
SHEFFIELD Ethical Student Hackers
Breaking into security.

Proxies



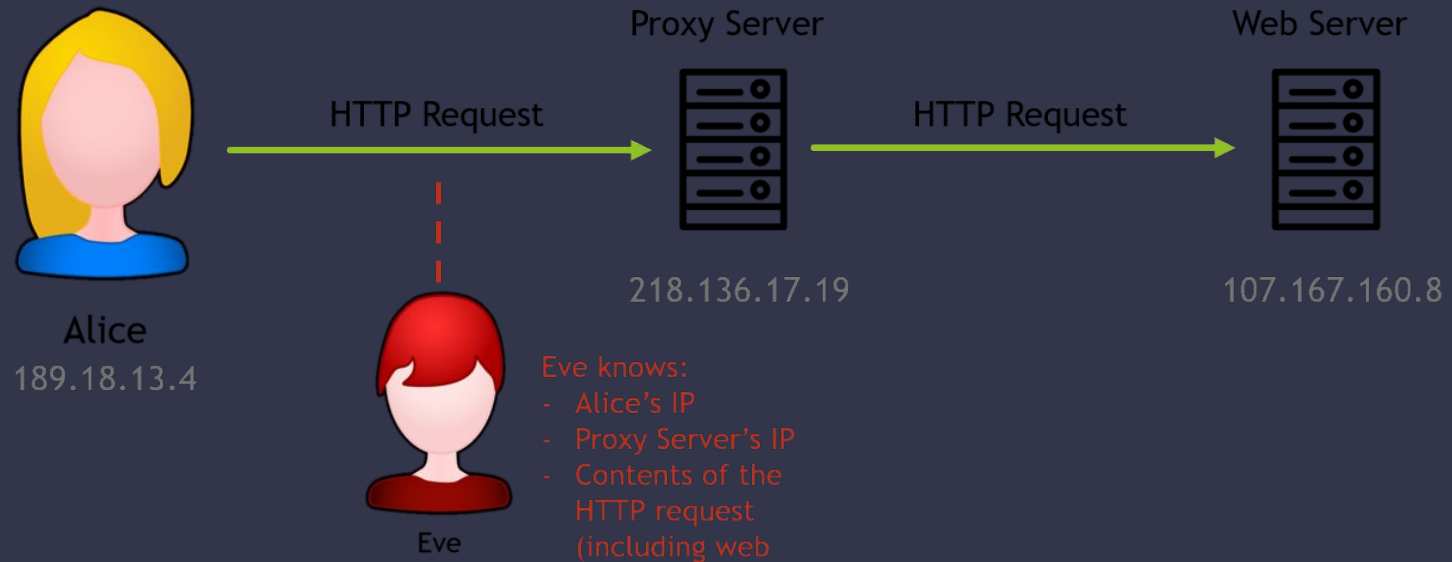
SHEFFIELD Ethical Student Hackers
Breaking into security.

Proxies



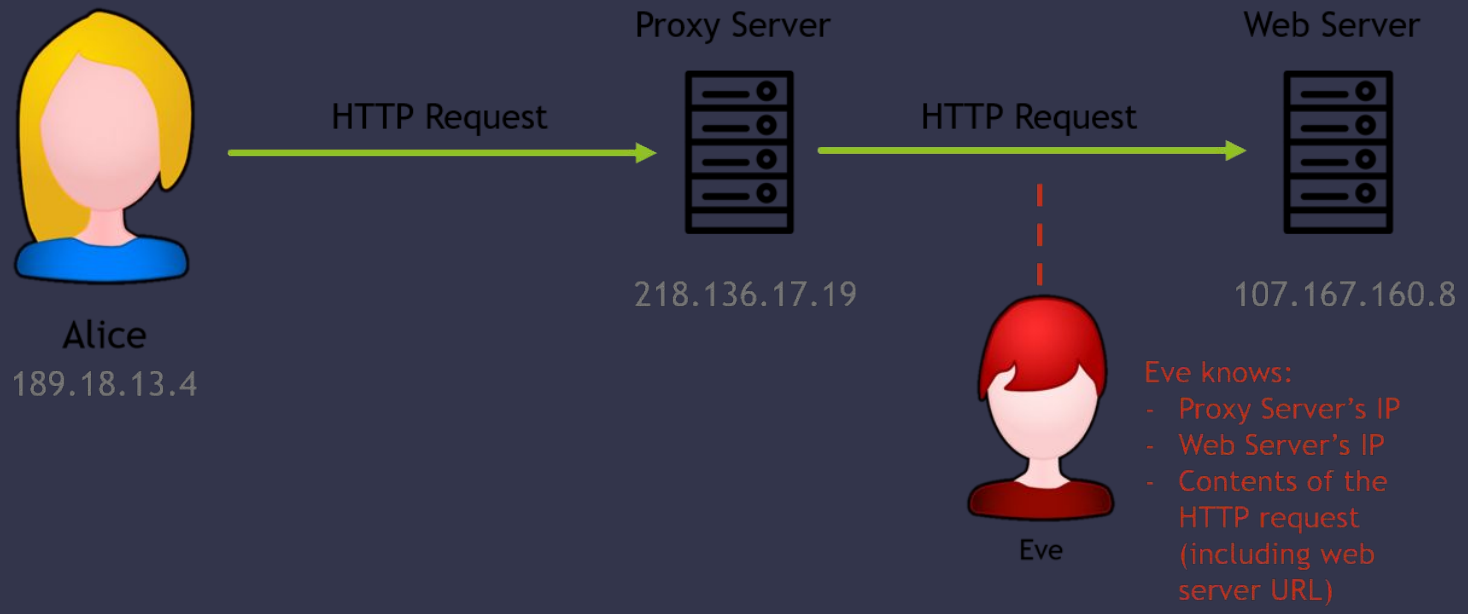
SHEFFIELD Ethical Student Hackers
Breaking into security.

Proxies



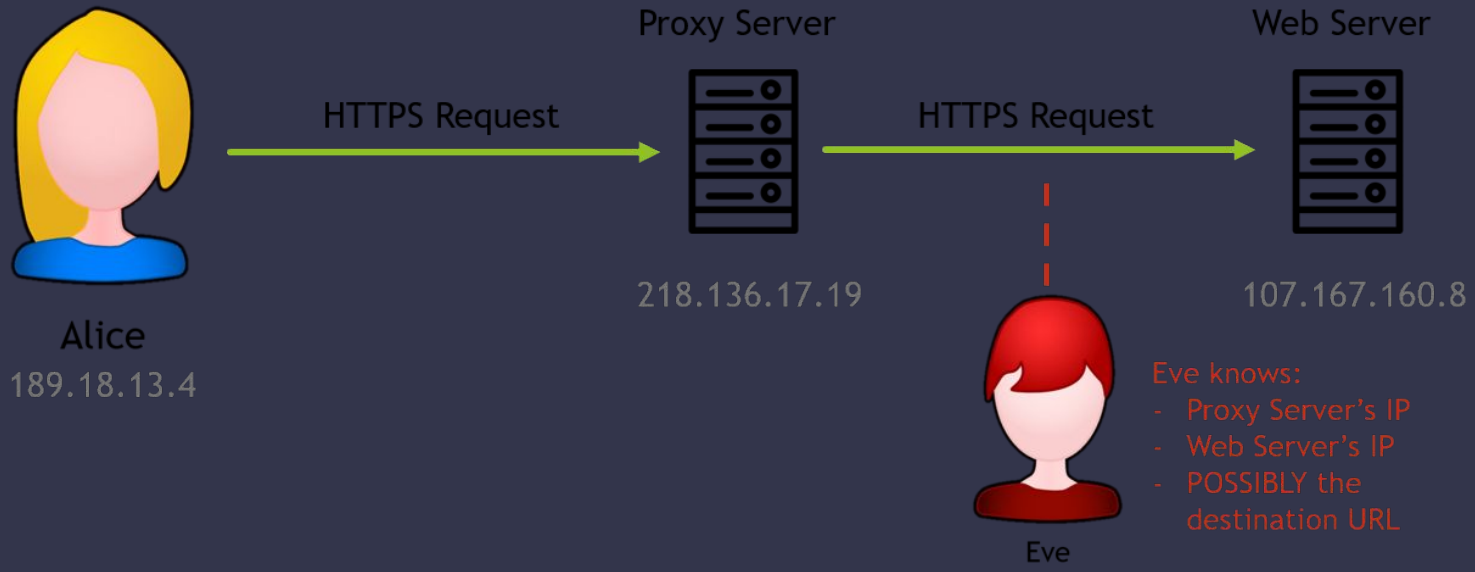
SHEFFIELD Ethical Student Hackers
Breaking into security.

Proxies



SHEFFIELD Ethical Student Hackers
Breaking into security.

Proxies



SHEFFIELD Ethical Student Hackers
Breaking into security.

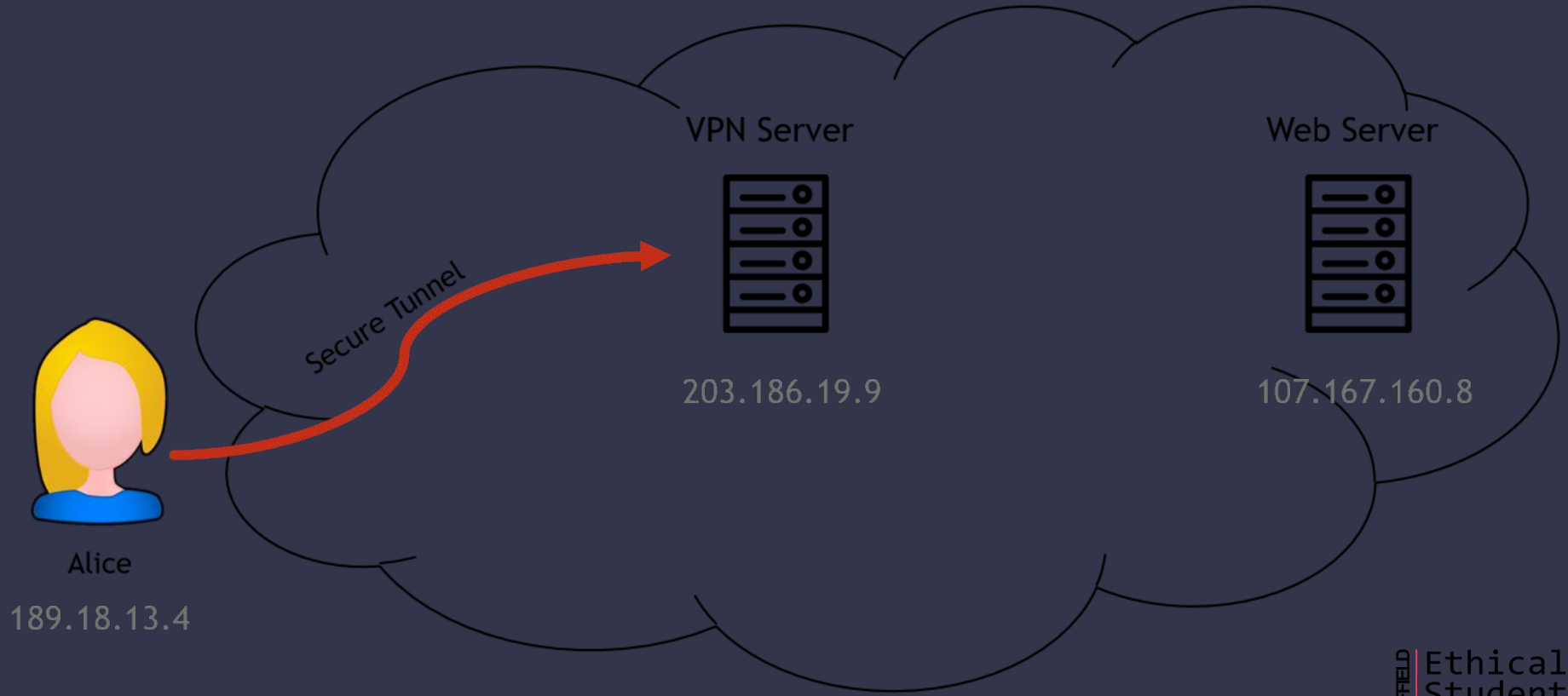
Virtual Private Networks (VPNs)

- Similar to a proxy (i.e. masking IPs), but with a couple of key differences
  - Connections to the VPN server are encrypted
  - They commonly catch all traffic from a host, rather than a specific protocol
  - Some VPNs encrypt the contents of packets

- Tunneling Protocol
  - The core feature of a VPN - extends a private (non-routable) network over a public one, like the internet, to keep data secure
  - ‘Encapsulates’ packets - the true contents of the packet is hidden all the way to the VPN server, sometimes even hiding details of the traffic type itself
  - When the traffic reaches the VPN server it is forwarded - the destination sees the VPN as the source
  - This prevents 3rd parties, including the ISP, from seeing the contents of a packet before it reaches the VPN server

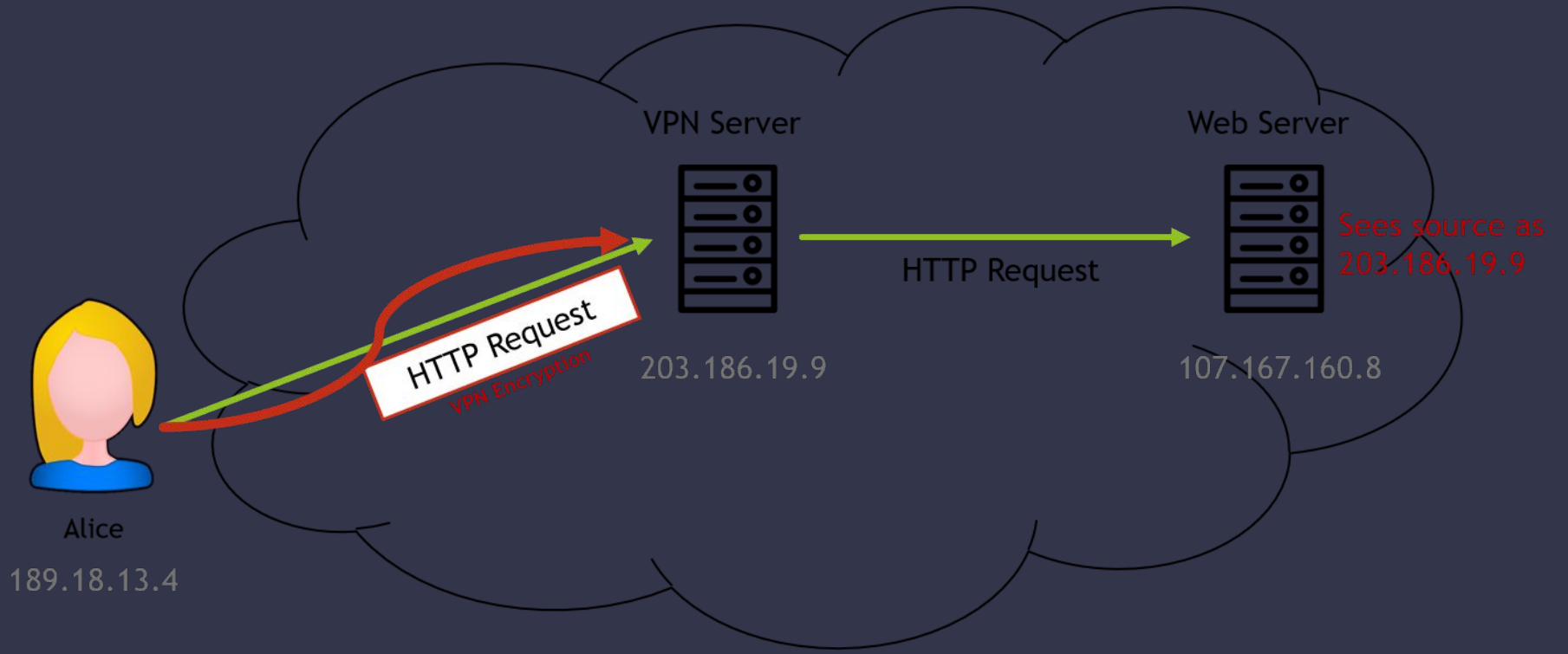
SHEFFIELD Ethical Student Hackers
Breaking into security.

Virtual Private Networks (VPNs)



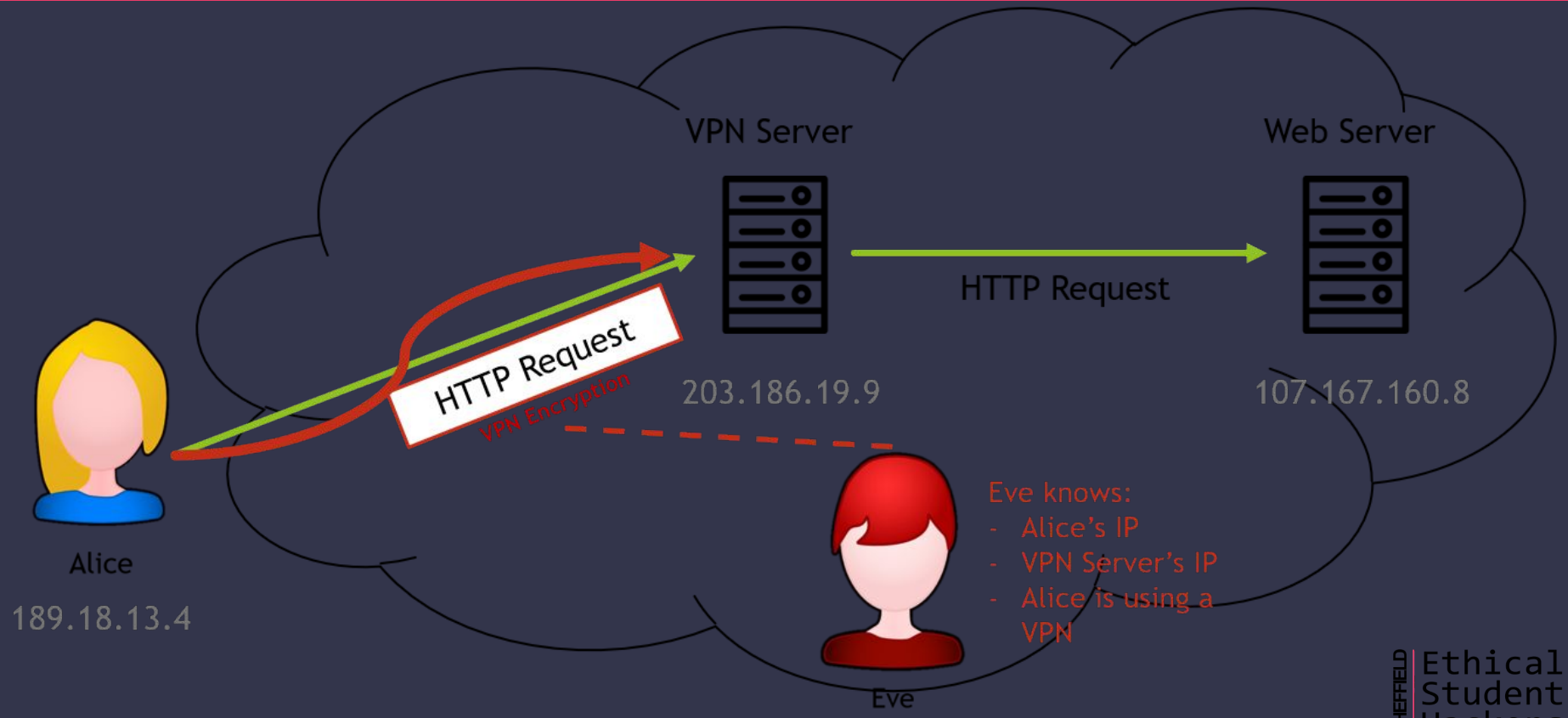
SHEFFIELD Ethical Student Hackers
Breaking into security.

Virtual Private Networks (VPNs)



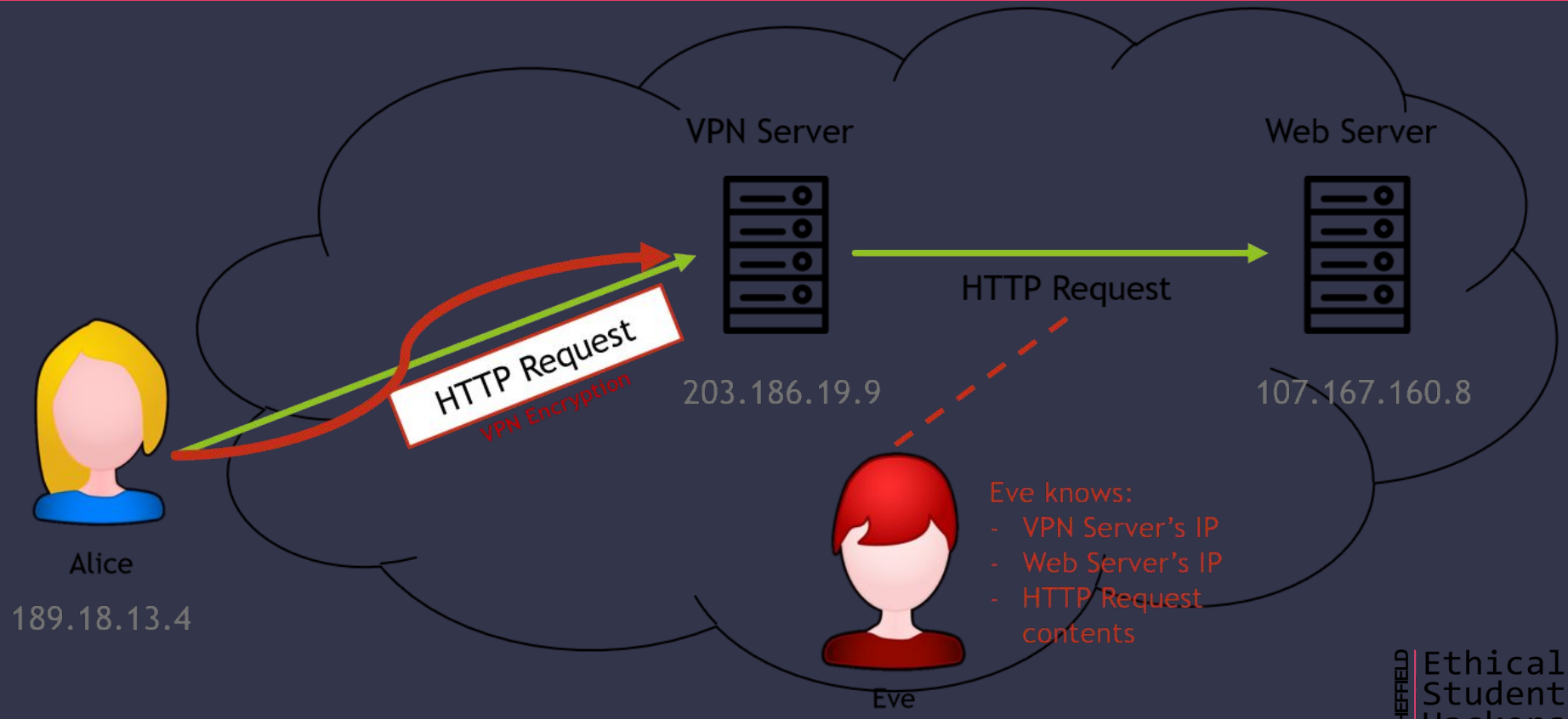
SHEFFIELD Ethical Student Hackers
Breaking into security.

Virtual Private Networks (VPNs)



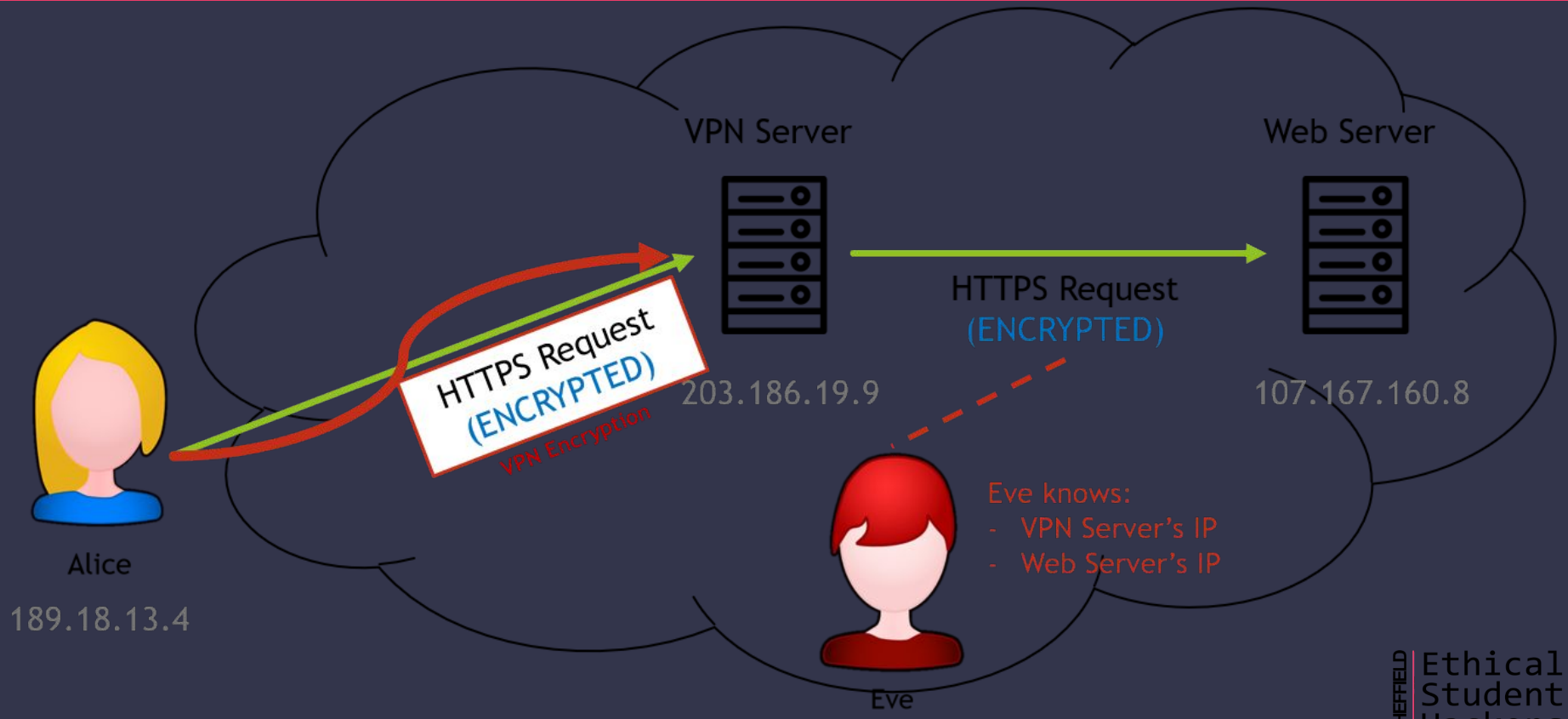
SHEFFIELD Ethical Student Hackers
Breaking into security.

Virtual Private Networks (VPNs)



SHEFFIELD Ethical Student Hackers
Breaking into security.

Virtual Private Networks (VPNs)



SHEFFIELD Ethical Student Hackers
Breaking into security.

Attacks Against VPNs & Proxies

- Traffic analysis
  - Analysing grouping and timing of packets (some attacks require visibility of both endpoints)
  - Fingerprinting traffic based on unencrypted headers (such as browser window size)
- Compromised VPN Providers
- Traffic Interception
  - Traffic is unencrypted after leaving the VPN server
  - MITM attacks could, in theory, impersonate your VPN provider, or a HTTPS proxy by generating on on-the-fly certificate (https://security.stackexchange.com/questions/2914/can-my-company-see-what-https-sites-i-went-to)
- Blacklisting
  - Scraping proxy sites

SHEFFIELD Ethical Student Hackers
Breaking into security.

Mitigations and OpSec

- Operational Security
  - Kill Switches can be used to prevent mistakes from users
  - VPNs can’t protect you if you leak your personal information in some other way
- Extra Encryption
  - Using HTTPS over a VPN or Proxy can mitigate the effects of traffic interception
- Strong Encryption
  - The better encryption algorithm a provider uses, the safer you are

The Onion Router (Tor)

- Onion Routing - another way of creating indirect connections from source to destination
  - A Tor ‘circuit’ consists of many relay nodes (minimum three in theory, exactly three in practice)
  - Packets are encrypted multiple times, according to the number of relay nodes
  - Each relay node decrypts one layer of encryption, revealing the address of the next
  - The final (‘exit’) node reveals the destination address and contents of the packet
  - On the way back, each node re-encrypts the packet and passes it to whichever node sent it to them the first time
  - Nodes are picked according to several rules which seek to lower the chance of endpoint attacks - for example, never picking the same node twice

- Because of this, there is no one point of compromise in the network
  - Even a malicious node cannot get a complete picture of the traffic

- For a detailed description of all things Tor, see this link: https://skerritt.blog/how-does-tor-really-work/

SHEFFIELD Ethical Student Hackers
Breaking into security.

The Onion Router (Tor)

Alice

189.18.13.4

Web Server

.onion domain

SHEFFIELD Ethical Student Hackers
Breaking into security.

The Onion Router (Tor)

Tor Relay

Tor Relay

Tor Relay

Alice

189.18.13.4

Web Server

.onion domain

SHEFFIELD Ethical Student Hackers

Breaking into security.

The Onion Router (Tor)

Tor Relay

HTTP Request

Alice

189.18.13.4

Tor Relay

Tor Relay

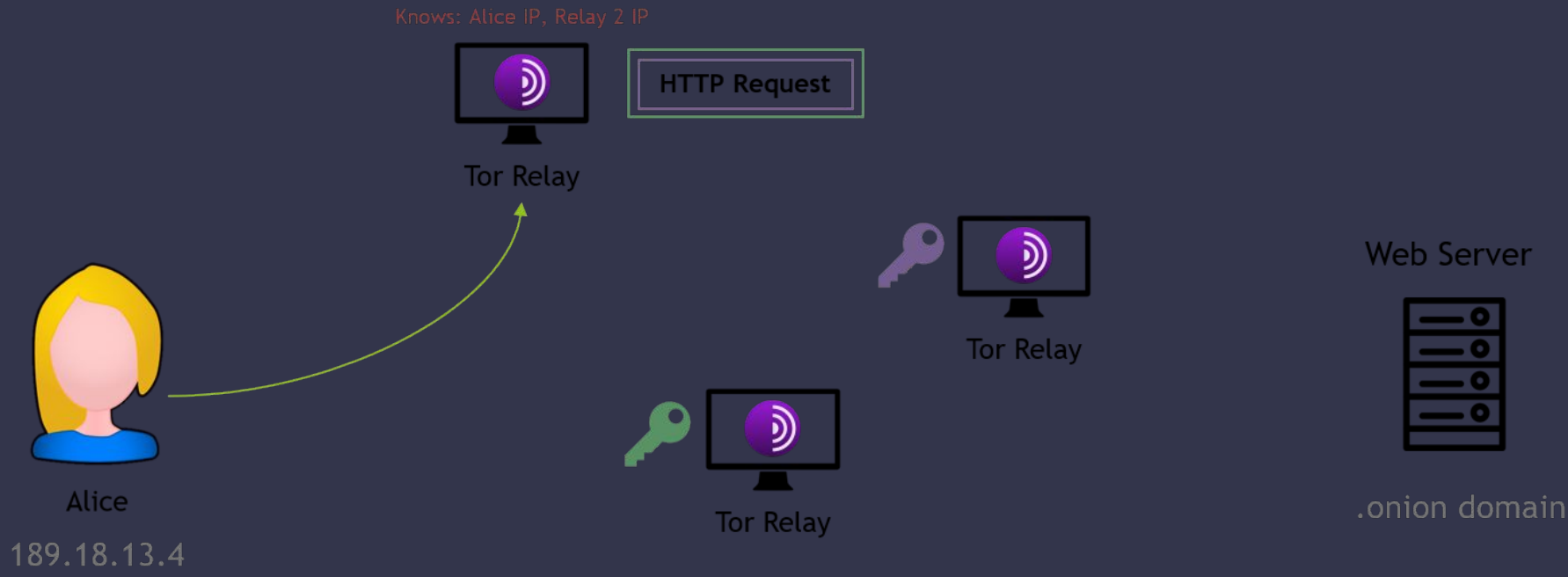
Web Server

.onion domain

SHEFFIELD Ethical Student Hackers

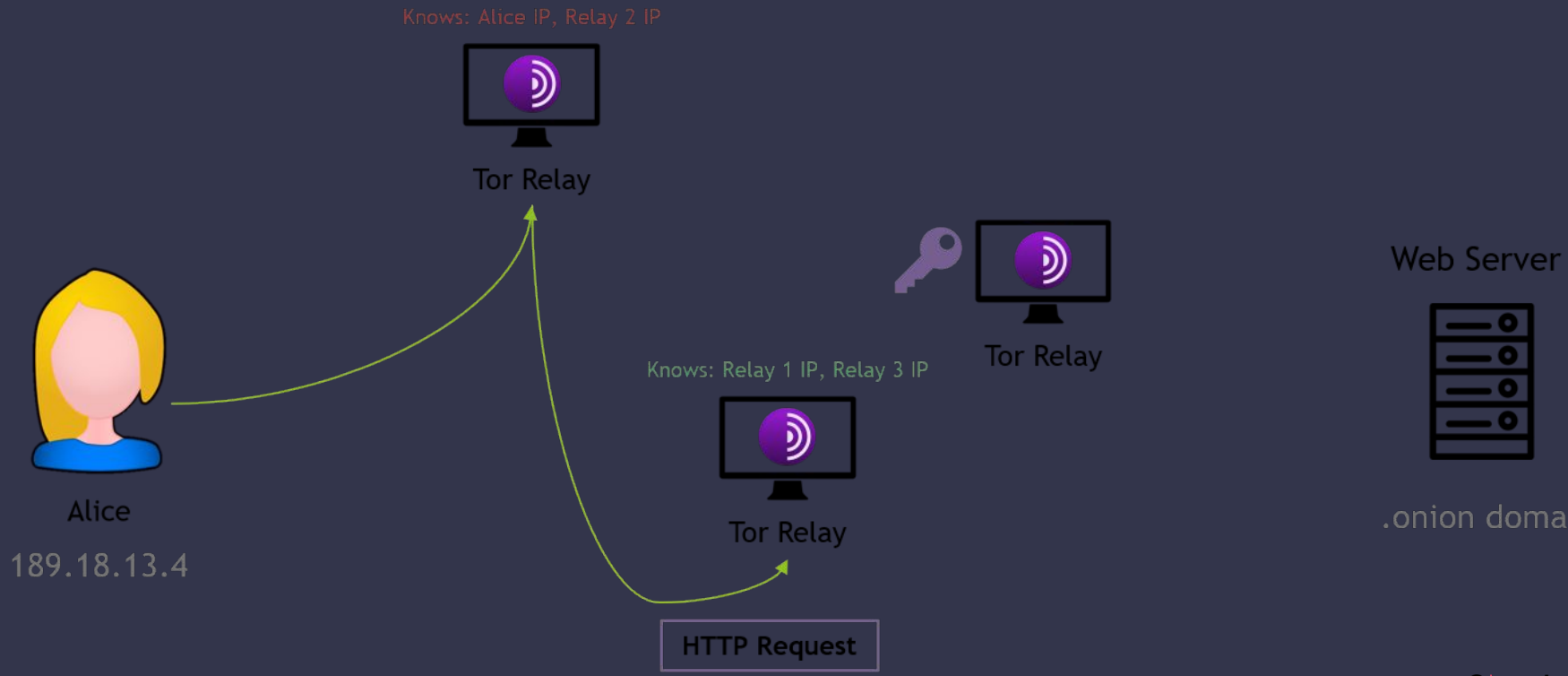
Breaking into security.

The Onion Router (Tor)



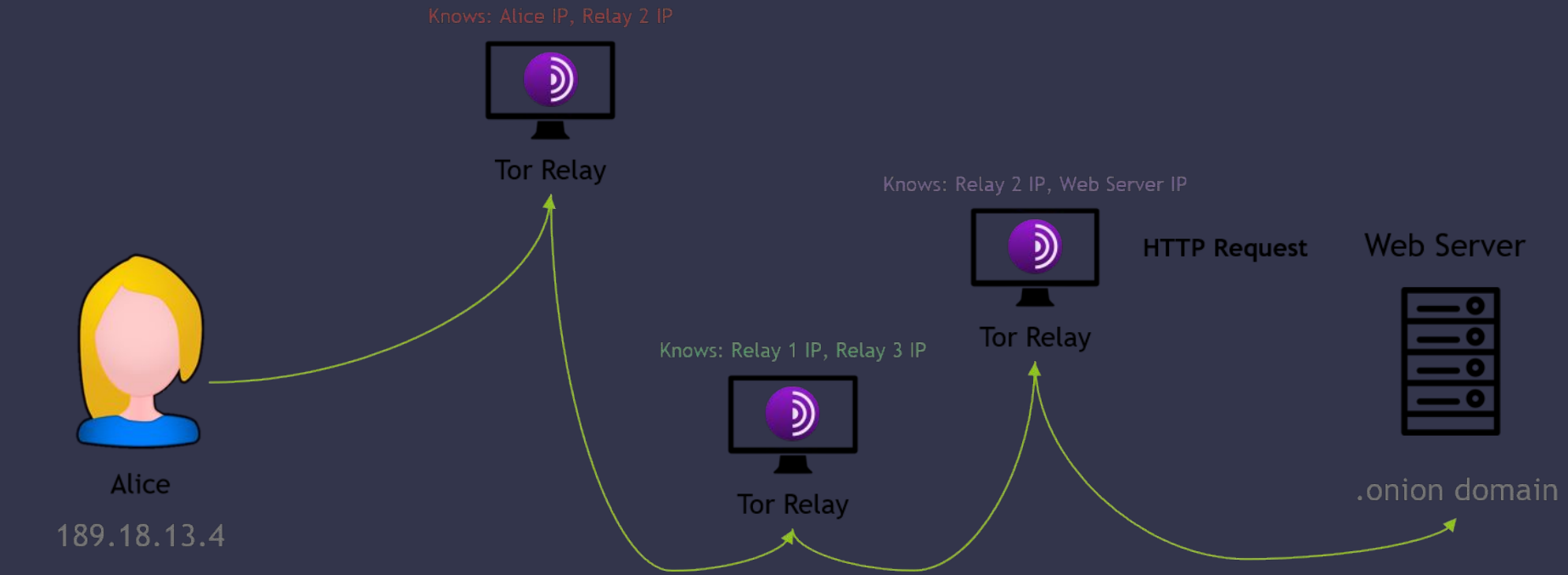
SHEFFIELD Ethical Student Hackers
Breaking into security.

The Onion Router (Tor)



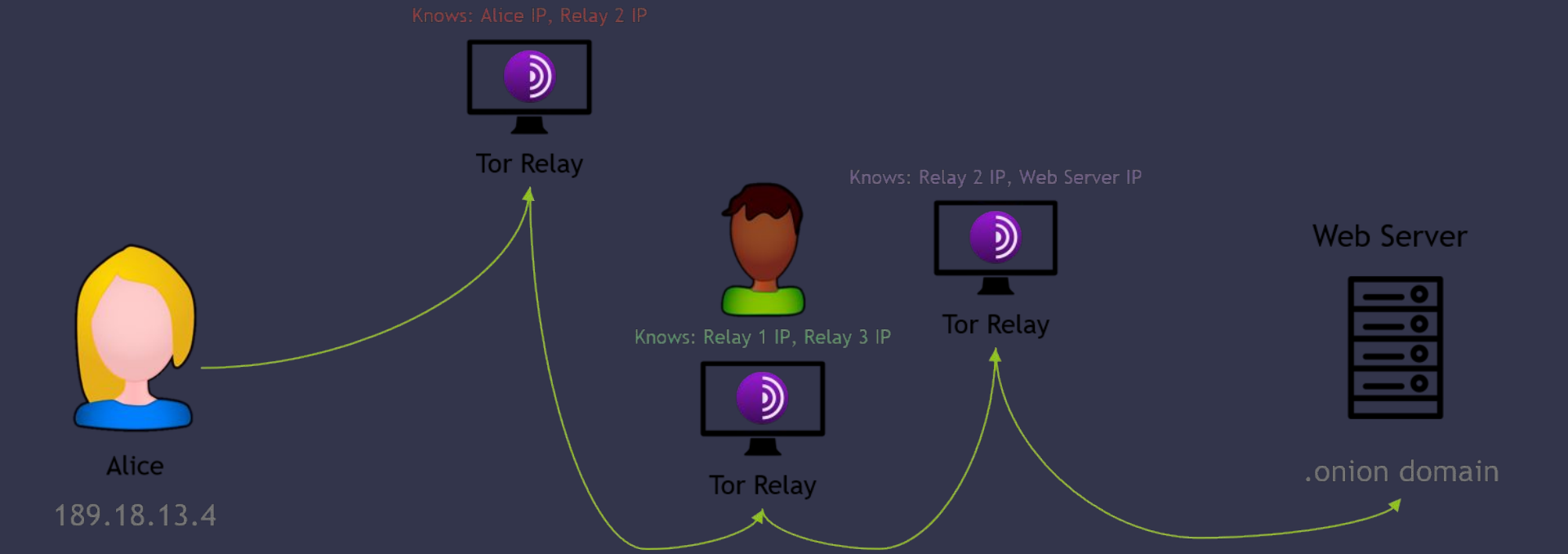
SHEFFIELD Ethical Student Hackers
Breaking into security.

The Onion Router (Tor)



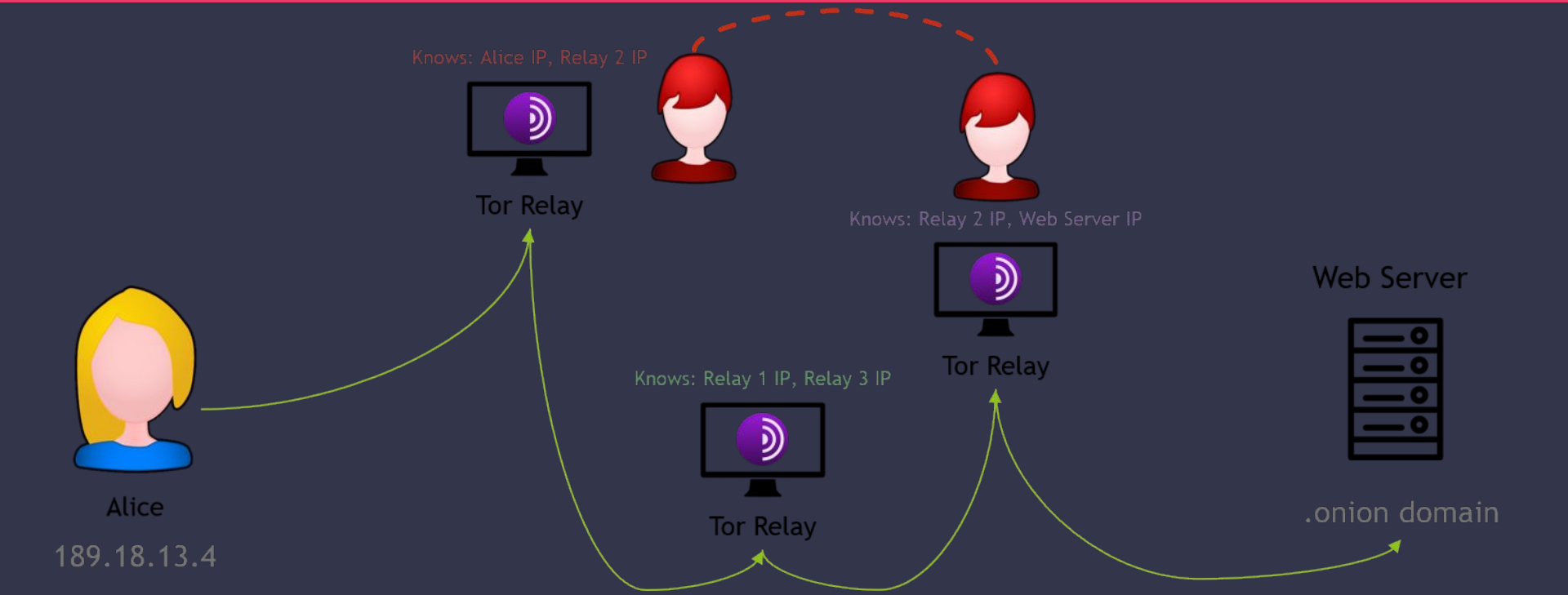
SHEFFIELD Ethical Student Hackers
Breaking into security.

The Onion Router (Tor)



SHEFFIELD Ethical Student Hackers
Breaking into security.

The Onion Router (Tor)



SHEFFIELD Ethical Student Hackers
Breaking into security.

The Onion Router (Tor)

- Chaum Mixing
  - Mixes packets between ‘hops’ so they are harder to trace from start to finish
- Encryption
  - AES is used to encrypt packets in a Tor circuit, with Diffie-Hellmann Key Exchange
  - Public Key Cryptography is used for Hidden Services
- Hidden Services
  - Tor allows users to setup hidden (‘onion’) services such as web servers and SSH servers, without exposing their IP address
  - These are the *.onion* domains you see on Tor - for example, https://protonirockerxow.onion
  - Hidden services are registered with a Hidden Service Directory, which is like a ‘phone book’ - it stores details of the hidden services’ IPs, and directs users to them via a rendezvous point
  - The keys for the dictionary are the onion address; the Hidden Service ‘descriptors’ consist of the IP address and a list of ‘introduction points’; the descriptor is signed with its private key

Ethical Student Hackers
Breaking into security.

Tor Relay Nodes

- Volunteer-run - about 6500 relay nodes

- What each node knows
  - Previous and next node address
  - Inner nodes don’t know what point in the circuit they are
  - Entry nodes know the IP of the source
  - Exit nodes know the IP of the destination, and any unencrypted traffic content

- Node Types
  - Guards - The ‘entry’ points into the network - computationally expensive to run
  - Exit - The final point in the circuit - malicious exits can be flagged with bad_exit
  - Bridge - An optional node that aren’t publicly listed (to prevent blocking)
  - Directory - Maintain a list representing the state of the network - centralised(ish)
  - HSDir - Hidden service directory nodes, forming a distributed hash table

SHEFFIELD Ethical Student Hackers
Breaking into security.

Attacks Against Tor

- Traffic Fingerprinting
- Malicious Exit Nodes
  - Monitor traffic, examine its contents, and even redirect it
  - https://www.zdnet.com/article/a-mysterious-group-has-hijacked-tor-exit-nodes-to-perform-ssl-stripping-attacks/
  - Combine this with a malicious entry node...
- HSDir Attacks
  - Controlling a majority share makes it possible to monitor HSDir requests, and provide false information
- Blocking
  - Via Directory nodes
  - Via Deep Packet Inspection

SHEFFIELD Ethical Student Hackers
Breaking into security.

Mitigations

- HTTPS (again)
  - Protecting your traffic with an extra layer of encryption is always a bonus
  - See this page for a visual explanation: https://www.eff.org/pages/tor-and-https
- Chaum Mixing mitigates against traffic analysis
- Large number of nodes makes it difficult to guarantee control of both a guard and exit
- Malicious nodes can be struck off the list of safe exits

Invisible Internet Project (I2P)

- I2P is a Peer-to-Peer (P2P network)
  - P2P networks are decentralised topologies, which are often fully interconnected
  - They are designed to share resources (e.g. storage, bandwidth, processing power)
  - Examples include Napster and Windows 10 Content Distribution

- I2P is volunteer-run, with around 55,000 nodes. It operates as an entirely separate layer to the internet, and ‘outproxying’ (i.e. ‘exiting’ traffic) to the internet is not advised (unlike Tor)

- Garlic Routing
  - Similar to Onion Routing, in that multiple layers of encryption are applied (when both routing traffic and building ‘tunnels’)
  - Messages are also bundled together in ‘bulbs’, making traffic analysis harder

- End to End Encryption is used throughout the network

SHEFFIELD Ethical Student Hackers
Breaking into security.

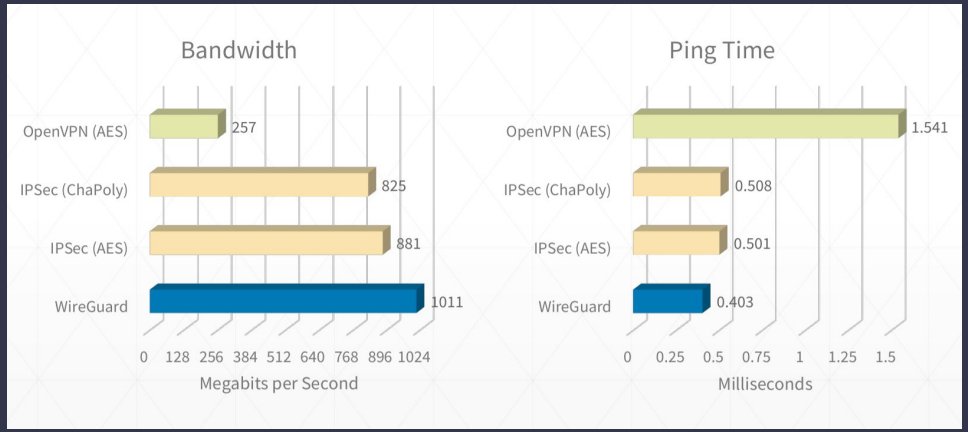
Make Your Own!

- As Tor, I2P, and many VPN / proxy solutions are open-source, it's possible to host your own!
- For proxies, the Arch Wiki has a nice set of information regarding software choice and setup
- The most popular VPN solutions are OpenVPN, IPSec, and WireGuard
  - See this comparison of different VPNs for more information
- For running your own Tor node, there is a wealth of information on the Relay Operations page
- Today we'll be setting up a WireGuard VPN server!

SHEFFIELD Ethical Student Hackers
Breaking into security.

Why WireGuard?

- The setup is easy, with only the keys needing to be shared + one simple conf
- Uses modern and fast cryptography everywhere
- Minimal attack surface (~4,000 lines of kernel code vs 600,000 for OpenVPN)
- High performance



SHEFFIELD Ethical Student Hackers
Breaking into security.

Creating a WireGuard Server

1. First, you'll need a Linux machine to host the server on!
   a. If you have a computer with a static IP or a dynamic DNS provider, you can use that
   b. Otherwise, you could pick up a VPS from AWS, Linode, or Vultr
2. Then you'll need to configure the WireGuard server!
   a. My notes are available here
   b. Some excellent (and more advanced) documentation can be found here
3. Set up your VPN peers to connect to the server
   a. WireGuard offers clients for many platforms

Upcoming Sessions

What's up next?

www.shefesh.com/sessions

Next week

The week after that

And the week after that

And the week after that

And the week after that

Any Questions?

www.shefesh.com

Thanks for coming!

SHEFFIELD Ethical Student Hackers

Breaking into security.