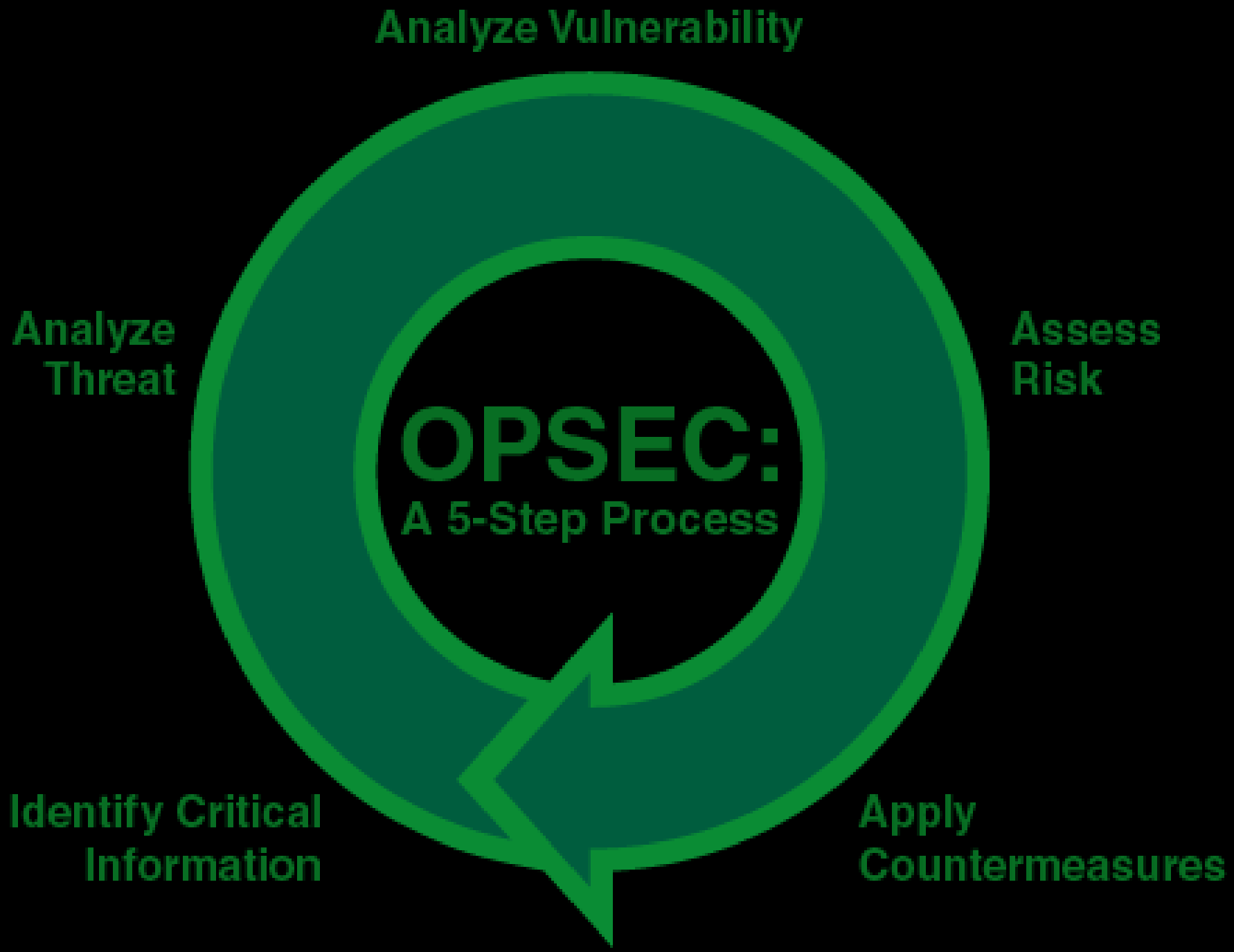
PRACTICAL OPSEC

What is OPSEC?

- also known as procedural security, is a risk management process that encourages managers to view operations from the perspective of an adversary in order to protect sensitive information from falling into the wrong hands.


"Unclassified does
not mean
unimportant think
OPSEC"


Analyze Vulnerability
Analyze Threat
Assess Risk
OPSEC:
A 5-Step Process
Identify Critical Information
Apply Countermeasures

Five Steps of OPSEC

- Identify your sensitive data, including your product research, intellectual property, financial statements, customer information, and employee information. This will be the data you will need to focus your resources on protecting.

Five Steps of OPSEC

- Identify possible threats. For each category of information that you deem sensitive, you should identify what kinds of threats are present. While you should be wary of third parties trying to steal your information, you should also watch out for insider threats, such as negligent employees and disgruntled workers.

Five Steps of OPSEC

- Analyze security holes and other vulnerabilities. Assess your current safeguards and determine what, if any, loopholes or weaknesses exist that may be exploited to gain access to your sensitive data.

Five Steps of OPSEC

- Appraise the level of risk associated with each vulnerability. Rank your vulnerabilities using factors such as the likelihood of an attack happening, the extent of damage that you would suffer, and the amount of work and time you would need to recover. The more likely and damaging an attack is, the more you should prioritize mitigating the associated risk.

Five Steps of OPSEC

- Get countermeasures in place. The last step of operational security is to create and implement a plan to eliminate threats and mitigate risks. This could include updating your hardware, creating new policies regarding sensitive data, or training employees on sound security practices and company policies.

For Cybersecurity / OSINT Researchers

- OPSEC is how you secure yourself from being tracked, hunted, and exposed on the internet.

Preparing the Machines

- Operating System
- AVs
- Host FWs
- VMs
- VPNs
- Proxies
- Password Managers
- Data Encryption
- Email and Communication Encryption
- Instant Messaging Platforms
- Collaboration Tools
- Browsers and Extensions
- Secure emails
- ISP
- Burner Phones / Mobile Devices

Preparing the Machines

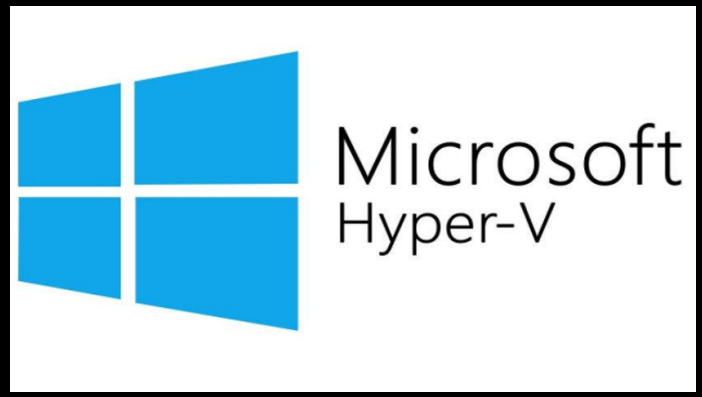
- Operating Systems:

Preparing the Machines

- It is better to have an antivirus software than none. Free AVs mostly have basic features. Use the best rated free AV.

Preparing the Machines

- Virtual Machines are an emulation of a computer system. Virtual machines are based on computer architectures and provide functionality of a physical computer. Their implementations may involve specialized hardware, software, or a combination.



Preparing the Machines

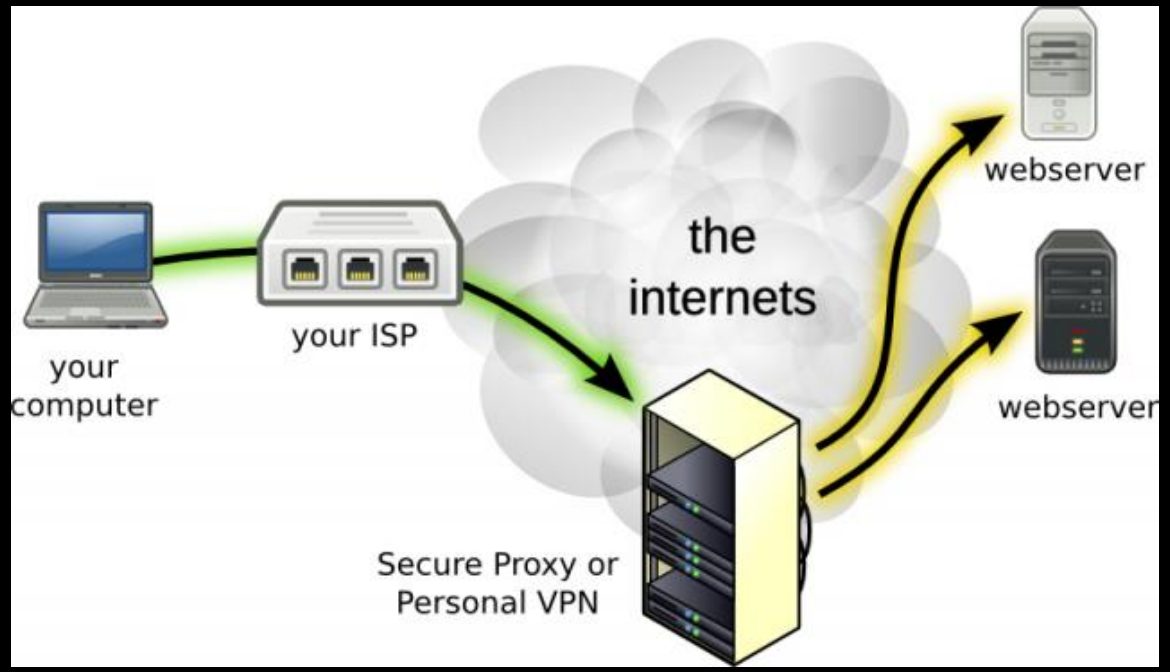
- Sample Linux Distros for OSINT

Tails
WHONIX
Qubes
Buscador Linux -> recommended distro for OSINT
Tsurugi Linux
Parrot Security OS
Kali Linux

Preparing the Machines

- Virtual Private Networks (VPN) extends a private network across a public network, and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. Applications running across a VPN may therefore benefit from the functionality, security, and management of the private network

Preparing the Machines



Preparing the Machines

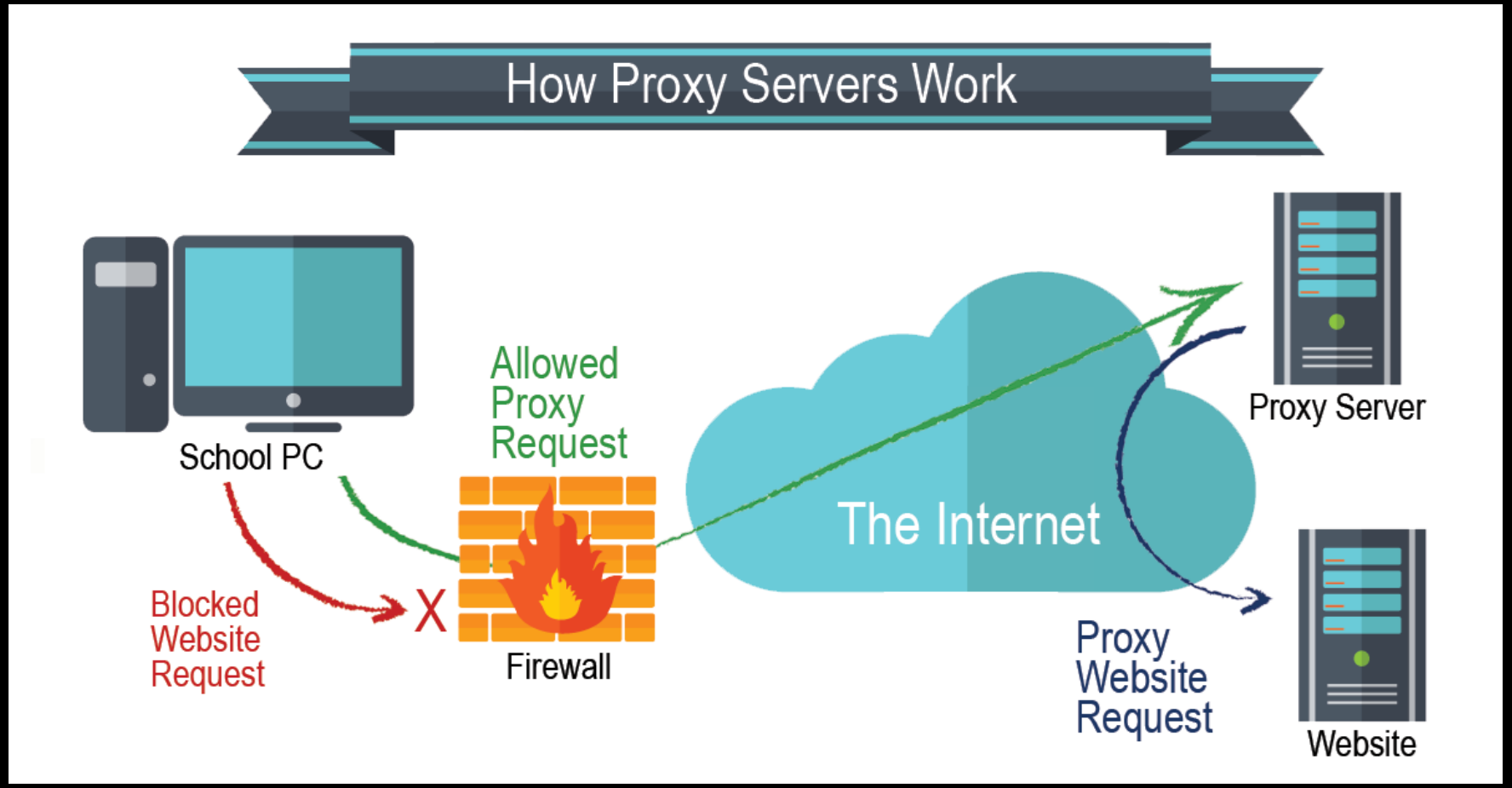
- Useful Personal VPN services:

Express VPN, ProtonVPN, Windscribe, NordVPN and Private Internet Access

Preparing the Machines

- A proxy server is a computer on the web that redirects your web browsing activity. Here's what that means.
- Normally, when you type in a website name (Amazon.com or any other), your Internet Service Provider (ISP) makes the request for you and connects you with the destination—and reveals your real IP address, as mentioned before.
- When you use a proxy your online requests get rerouted.
- While using a proxy, your Internet request goes from your computer to your ISP as usual, but then gets sent to the proxy server, and then to the website/destination. Along the way, the proxy uses the IP address you chose in your setup, masking your real IP address.

Preparing the Machines



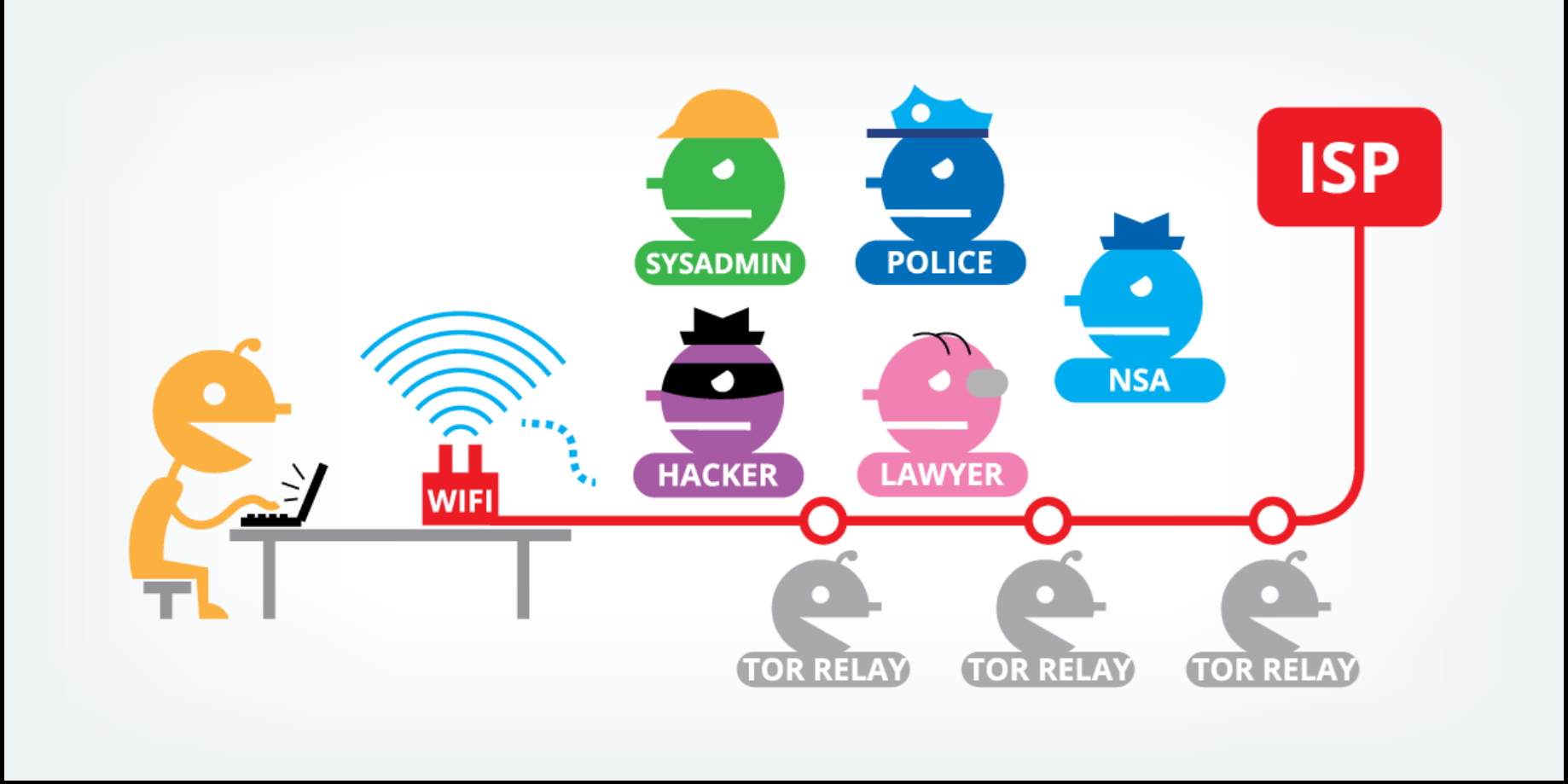
Preparing the Machines

(the onion router)

Directs internet traffic through a free, worldwide, volunteer overlay network consisting of more than seven thousand relays to conceal a user's location and usage from anyone conducting network surveillance or traffic analysis.

Applications whose traffic is commonly anonymized using Tor include Internet Relay Chat (IRC), instant messaging, and World Wide Web browsing.

Preparing the Machines



Preparing the Machines

- Password managers enables us to store passwords in secured databases.
- Recommended tools: KeePass and LastPass

Preparing the Machines

- Browsers: Edge? Firefox? Chrome? Opera? Torch?
- Extensions are added functionalities that enable browsers to do specialized tasks.

Preparing the Machines

- Useful Firefox Extensions:

uBlock origin
Exif viewer
Image search options
Distill
Nimbus Screen Capture
Multi-Account Containers -> used for opening various social media accounts in one browser
Mailvelope -> enables the exchange of encrypted emails following the OpenPGP encryption standard

Preparing the Machines

- Useful Chrome Extensions:

Adblock
Fireshot – screenshot purposes
360Social – social media
Treeverse – twitter specific
Distill – monitors webpage or feeds for chan
Mostly Harmless – reddit monitoring

Preparing the Machines

- Privacy Focused Browser

Brave
Iridium
GNU IceCat Browser
Tor Browser
Pale Moon Browser

Preparing the Machines

- Privacy Focused Search Engine

DuckduckGo

Preparing the Machines

- Look for secure / burner emails for specific uses only.

Recommended: Protonmail / Tutanota

Preparing the Machines

- Burner ISPs

Pocket Wifi / Broadband
Prepaid SIMs

Globe
WIRELESS LTE BROADBAND

Smart
Bro

Preparing the Machines

- Burner ISPs

  -use custom firmware on Huawei routers to enable LTE signal selection (936, 938 Models)

  -install OpenVPN Client

  -use a variety of OpenVPN configs

Preparing the Machines

- Burner Phones / Mobile Devices (multi-sim)
- Online Free SMS Inboxes (https://temp-sms.org/)

For 2FA, SMS confirmation, Number Registration etc

Online Collaboration Tools

- Signal
- Telegram
- WhatsApp
- Discord
- In-Game Chats (MOBA, FPS, RTS etc)

Online Collaboration Tools

- Applying Public-Private Key Encryption for COMSEC
  - -Mailvelope
  - -GPG4Win / Kleopatra

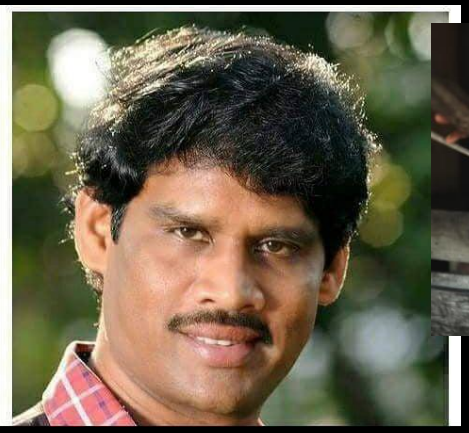
Online Collaboration Tools

- Anonymous File Transfers
  - -WeTransfer
  - -Send Anywhere (Chrome Extension)
  - -MyAirBridge
  - -SendGB
  - -Reep.io
  - -Onionshare

Preparing the Human

- Sock Puppet ->Avatars (Keepass / LastPass)
- Psyche
- Network slowly
- Maintain a Blog
- Let it grow naturally (patience is the KEY)





Preparing the Human

- Sock Puppet

FakeName Generator
ThisPersonDoesNotExist
Use AI
And other “public” sources


The Only Thing I'm Giving Away
Pure Hilarity
Is Your Personal Information

REFERENCES FOR SOCK PUPPETS

- https://jakecreps.com/2018/11/02/sock-puppets/
- https://www.secjuice.com/the-art-of-the-sock-osint-humint/
- https://osintcurio.us/2018/12/27/the-puppeteer/
- https://www.paliscope.com/2019/10/21/how-to-build-a-solid-fake-identity-for-online-investigations/

REFERENCES FOR OPSEC

- https://isc.sans.edu/forums/diary/OpSec+and+OSInt/25100/
- https://osintcurio.us/2019/04/18/basic-opsec-tips-and-tricks-for-osint-researchers/
- https://www.sans.org/webcasts/operations-security-opsec-tradecraft-tips-online-open-source-intelligence-osint-research-112735
- https://nixintel.info/osint/opsec-for-osint-why-you-need-to-deal-with-browser-fingerprinting/
- https://github.com/AxelSeg/osint-opsec-tool
- https://github.com/SiloGit/OpSec-In-OSINT

END