

# XFLTReaT: a new dimension in tunnelling

Balazs Bucsay / @xoreipeip  
Security Consultant @ NCC Group

# Bio / Balazs Bucsay

---

- Hungarian hacker
- Security Consultant @ NCC Group
- Strictly technical certificates: OSCE, OSCP, OSWP, GIAC GPEN, CREST CCT/2
- Lots of experience in offensive security
- Started with ring0 debuggers and disassemblers in 2000 (13 years old)
- Major projects:
  - GI John (2009) – Hacktivity
  - Chw00t (2015) – PHDays, DeepSec, Hacktivity
  - XFLTReaT (2017) – Shakacon ;)
- Twitter: @xoreipeip
- Linkedin: <https://www.linkedin.com/in/bucsayb>

# Presentations

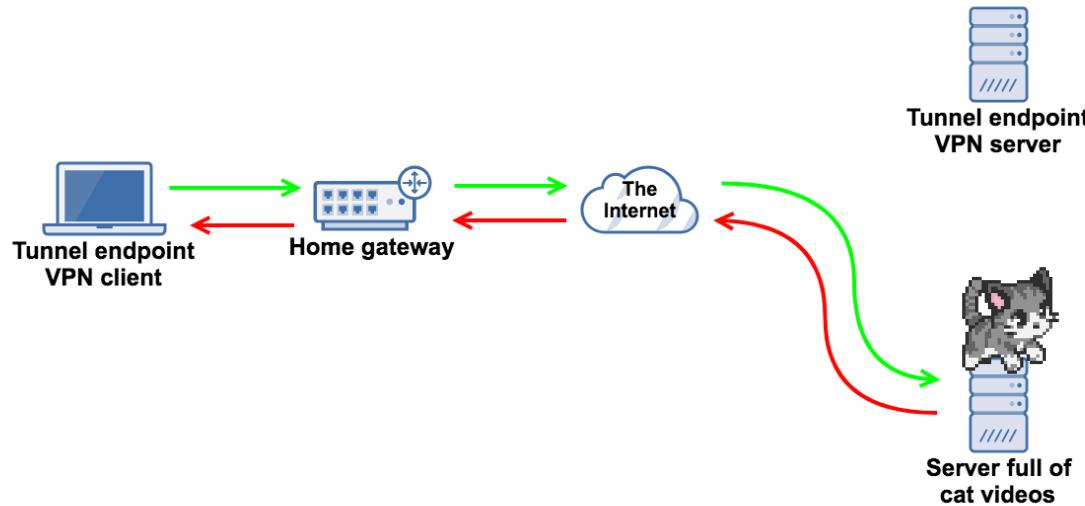
---

- Talks around the world:
  - Honolulu (HI) / Shakacon (returning speaker)
  - Atlanta (GA) / Hacker Halted
  - Moscow (RU) / PHDays
  - Oslo (NO) / HackCon
  - Vienna (AT) / DeepSec
  - Budapest (HU) / Hacktivity
  - London (UK) / Inf. Gov. & eDiscovery Summit
  - There is some more space here...

# Tunnels

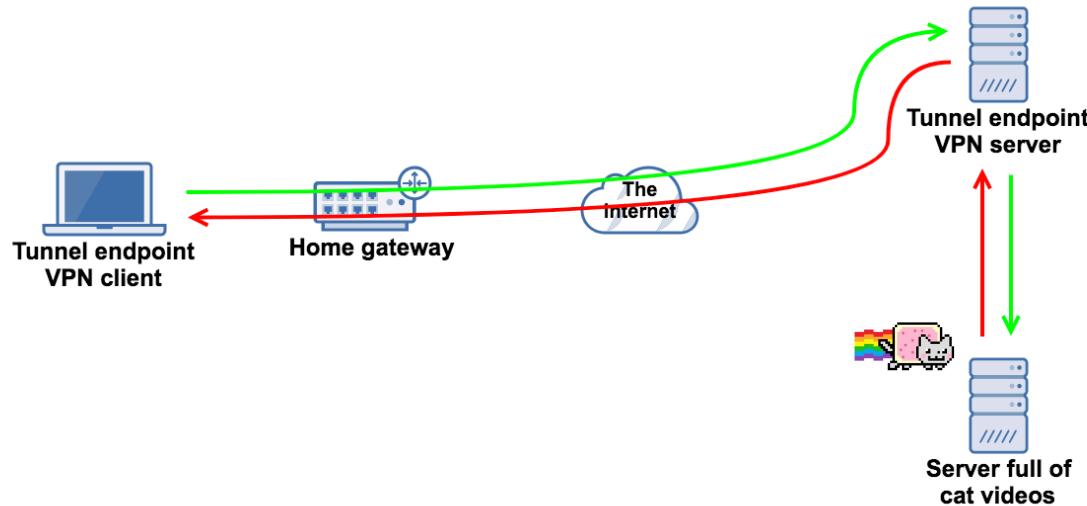


# Without a tunnel



@xoreipeip

# With a tunnel



@xoreipeip

# Why would one use tunnels?

---

- **Work VPN – to access the corporate internal network**
- **Hide real IP address**
  - Whistle-blowers/Journalists to communicate anonymously
  - Torrent
- **ISPs filtering some ports (secure IMAP, SMTPS, NetBIOS, ...)**
- **Bypass corporate proxy policy**
- **Bypass captive portals!?**
- **What about you?**

# Have you done ... tunnelling?

@xoreipeip

# Have you done ... tunnelling?

Protocol	Tool		
TCP	OpenVPN	Cisco AnyConnect	
UDP			

@xoreipeip

# Have you done ... tunnelling?

Protocol	Tool		
TCP	OpenVPN	Cisco AnyConnect	
UDP	OpenVPN		
ICMP			

@xoreipeip

# Have you done ... tunnelling?

Protocol	Tool		
TCP	OpenVPN	Cisco AnyConnect	
UDP	OpenVPN		
ICMP	Hans	Ping Tunnel	ICMPTx
DNS			

@xoreipeip

# Have you done ... tunnelling?

Protocol	Tool		
TCP	OpenVPN	Cisco AnyConnect	
UDP	OpenVPN		
ICMP	Hans	Ping Tunnel	ICMPTx
DNS	iodine	DNSCat*	Ozymandns
HTTP CONNECT	Proxifier		
Pure HTTP	?		
TLS v1.2	?		
TLS v1.2 with Kerberos auth	?		

@xoreipeip

# Two days on a ferry

(Port TCP/443 unfiltered)



# 10 hour flight to Japan

(ICMP unfiltered)



Not again!  
Why haven't I set up  
my ICMP tunnel?

# At the airport

(DNS unfiltered)



Bloody hell!  
The DNS tunnel  
crashed!?

Lol,  
lamer. Not mine.  
Why not use  
XFLTReaT?

# What did I see?

---

## Get tired of:

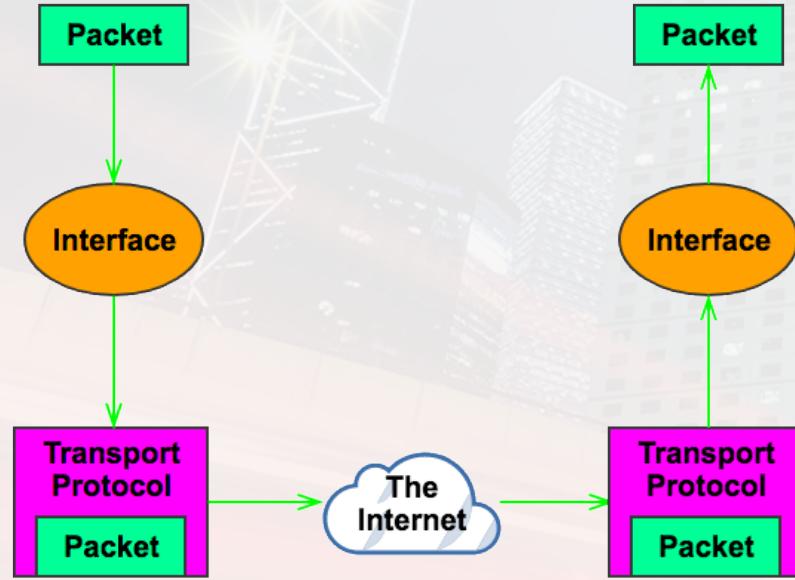
- As many protocols as many solutions
- Hard to modify the existing ones
- No modularity
- Portability issues
- Configuration issues
- Unsupported/EoL tools
- No automation at all
- It is just hard, but it does not have to be!

@xoreipeip

# XFLTReaT

The beast was born!

# Tunnelling theory 101 / MTU



@xoreipeip

# What is XFLTReaT?

---

## **XFLTReaT (say exfil-treat or exfiltrate)**

- Tunnelling framework
- Open-source (will be released soon)
- Python based
- OOP
- Modular
- Multi client
- Plug and Play (at least as easy as it can be)
- Check functionality

@xoreipeip

# Easy, modular, plug & play

---

- **Install:**
  - **git clone & pip install**
  - **edit config**
  - **run**
- **Tunnels, encryption, authentication etc. are modular**
- **Plug and play:**
  - **Copy new module into modules/, support files to support/**
  - **edit config**
  - **run**

@xoreipeip

# Framework, as it is

---

## You do not have to:

- Set up the routing
- Handle multiple users
- Create and set up an interface or interfaces
- Care about encryption, authentication or encoding

## You only have to:

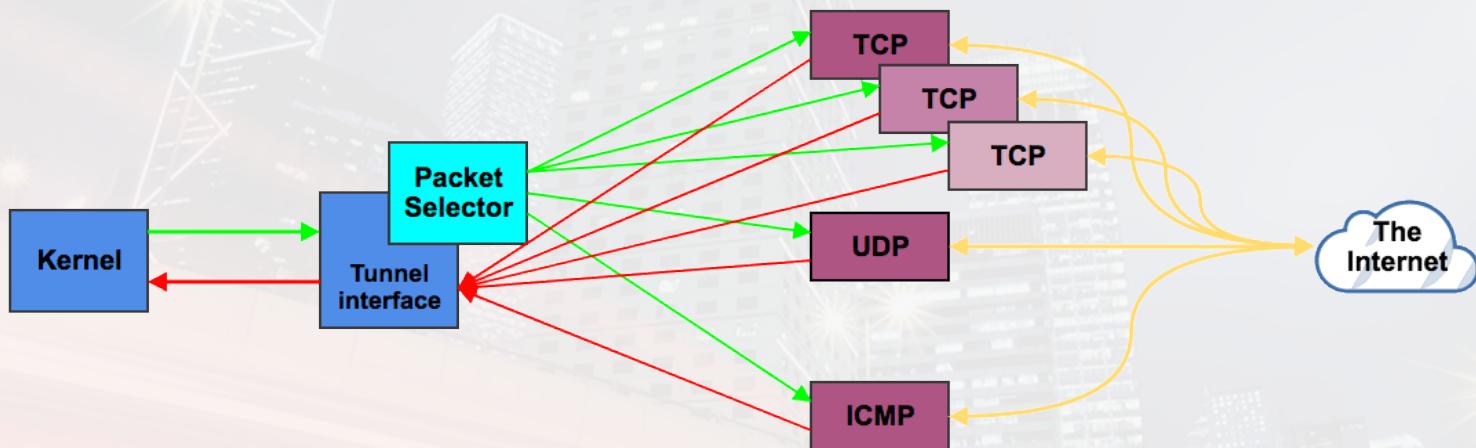
- Package your packets into your protocol
- Implement protocol related things

# Check functionality

---

- Easy way to figure out, which protocol is not filtered on the network
- Automated approach: No deep knowledge is needed
- Client sends a challenge over the selected (or all) modules to the server
- If the server responses with the solution:
  - We know that the server is up and running
  - The specific module/protocol is working over the network
  - Connection can be made

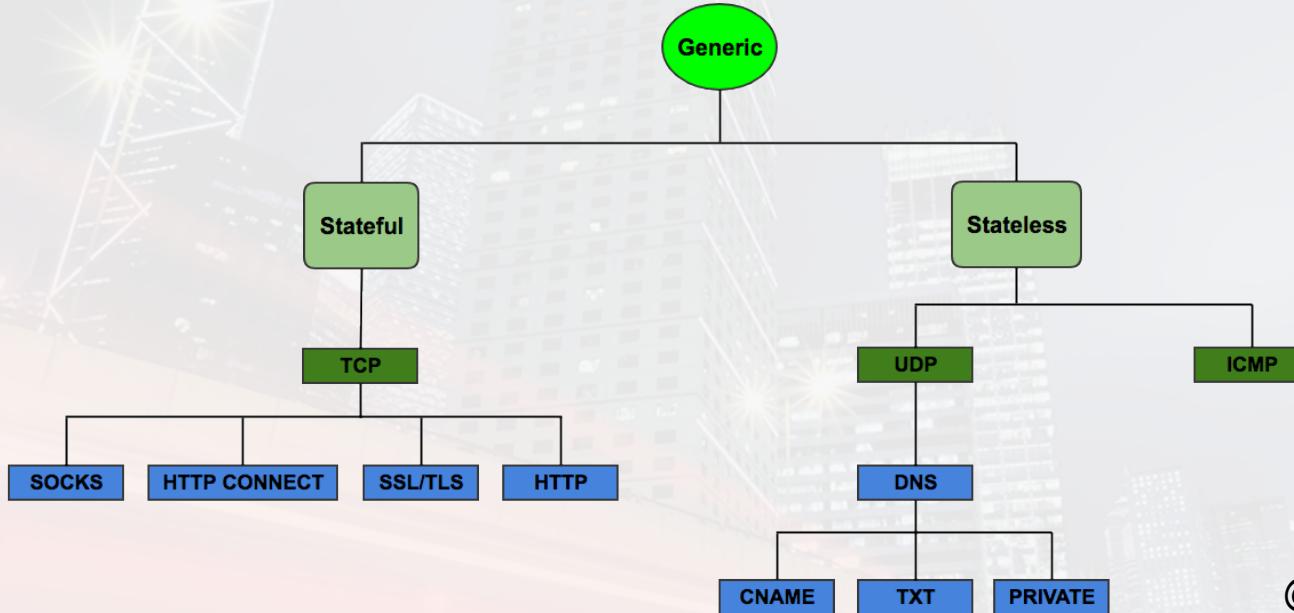
# One interface to rule them all



@xoreipeip

# Ease of development

# Module tree



@xoreipeip

# Ease of use/development

---

- Only web traffic allowed?

@xoreipeip

# Ease of use/development

---

- Only web traffic allowed? Set your server on port TCP/80
- Only ICMP type X allowed?

@xoreipeip

# Ease of use/development

---

- Only web traffic allowed? Set your server on port TCP/80
- Only ICMP type X allowed? Copy ICMP module, change type 8 to X
- HTTPS allowed but only with TLS v1.2?

@xoreipeip

# Ease of use/development

---

- Only web traffic allowed? Set your server on port TCP/80
- Only ICMP type X allowed? Copy ICMP module, change type 8 to X
- HTTPS allowed but only with TLS v1.2? Copy TLS module, set it to 1.2 only
- HTTP should work, but only with special header?

# Ease of use/development

---

- Only web traffic allowed? Set your server on port TCP/80
- Only ICMP type X allowed? Copy ICMP module, change type 8 to X
- HTTPS allowed but only with TLS v1.2? Copy TLS module, set it to 1.2 only
- HTTP should work, but only with special header? Set the header in source
- Want to send data over text/SMS?

# Ease of use/development

---

- Only web traffic allowed? Set your server on port TCP/80
- Only ICMP type X allowed? Copy ICMP module, change type 8 to X
- HTTPS allowed but only with TLS v1.2? Copy TLS module, set it to 1.2 only
- HTTP should work, but only with special header? Set the header in source
- Want to send data over text/SMS? Handle connection with your phone from a module
- Special authentication over HTTP proxy?

# Ease of use/development

---

- Only web traffic allowed? Set your server on port TCP/80
- Only ICMP type X allowed? Copy ICMP module, change type 8 to X
- HTTPS allowed but only with TLS v1.2? Copy TLS module, set it to 1.2 only
- HTTP should work, but only with special header? Set the header in source
- Want to send data over text/SMS? Handle connection with your phone from a module
- Special authentication over HTTP proxy? Implement the auth, change the config
- **PROTIP:** just use the source!

# DEMO

# Offense

---

- **Bypass basic obstacles**
  - Specific ports are unfiltered (TCP / UDP)
  - DNS allowed
  - ICMP allowed
- **Bypass not that basic obstacles**
  - Specific protocol allowed (IPS or any other active device in place)
  - Special authentication required
- **Exfiltrate information from internal networks**
- **Get unfiltered internet access**

@xoreipeip

# Defense

---

## Check your network settings

- Check functionality
- Try to exfiltrate data – check whether your active network device can catch it

## Captive portals

- Drop all packets that are addressed to external until not authenticated
- All DNS query should have the same response (the portal)

# Defense for companies

---

## No solution is 100% secure

- Do not route your network to the internet
  - Disable all traffic between the internet and internal network
- Use HTTP Proxy and enforce it
  - Whitelist ports (80 and 443, would you need anything else?)
  - Blacklist websites (does not really help on XFLTReaT)
- DNS
  - Filter external DNS queries if possible (let HTTP proxy do the resolving)

# Defense for companies

---

## No solution is 100% secure

- **Do you have an inventory? (IP, owner, purpose, location)**
- **Do baselining**
  - Check relation between IPs
  - What protocol is in use?
  - What frequency, volume?
- **Any unusual activity should generate an alert/be blocked when you are done**

# TODO

---

- Python 2.x and 3.x support
- Multi OS support
- More modules (DNS is the next one)
- Encryption and authentication modules
- Adding more comments to the code

@xoreipeip

# Release

---

- Will be released on Github
- It takes some little more time, because:
  - Adding comments
  - More modules
  - Bug fixes
  - etc.

@xoreipeip

# Q&A - Thank you for your attention

Balazs Bucsay / @xoreipeip

# Office Locations

## Europe

Manchester - Head Office  
Amsterdam  
Basingstoke  
Cambridge  
Copenhagen  
Cheltenham  
Delft  
Edinburgh  
Glasgow  
The Hague  
Leatherhead  
Leeds  
London  
Madrid  
Malmö  
Milton Keynes  
Munich  
Vilnius  
Zurich

## North America

Atlanta, GA  
Austin, TX  
Boston, MA  
Campbell, CA  
Chicago, IL  
Kitchener, ON  
New York, NY  
San Francisco, CA  
Seattle, WA  
Sunnyvale, CA  
Toronto, ON

## Asia-Pacific

Singapore  
Sydney

## Middle East

Dubai