UNLEASH THE INFECTION MONKEY: A MODERN ALTERNATIVE TO PEN TESTS

Ofri Ziv, GuardiCore
ofri@guardicore.com

Who am I?

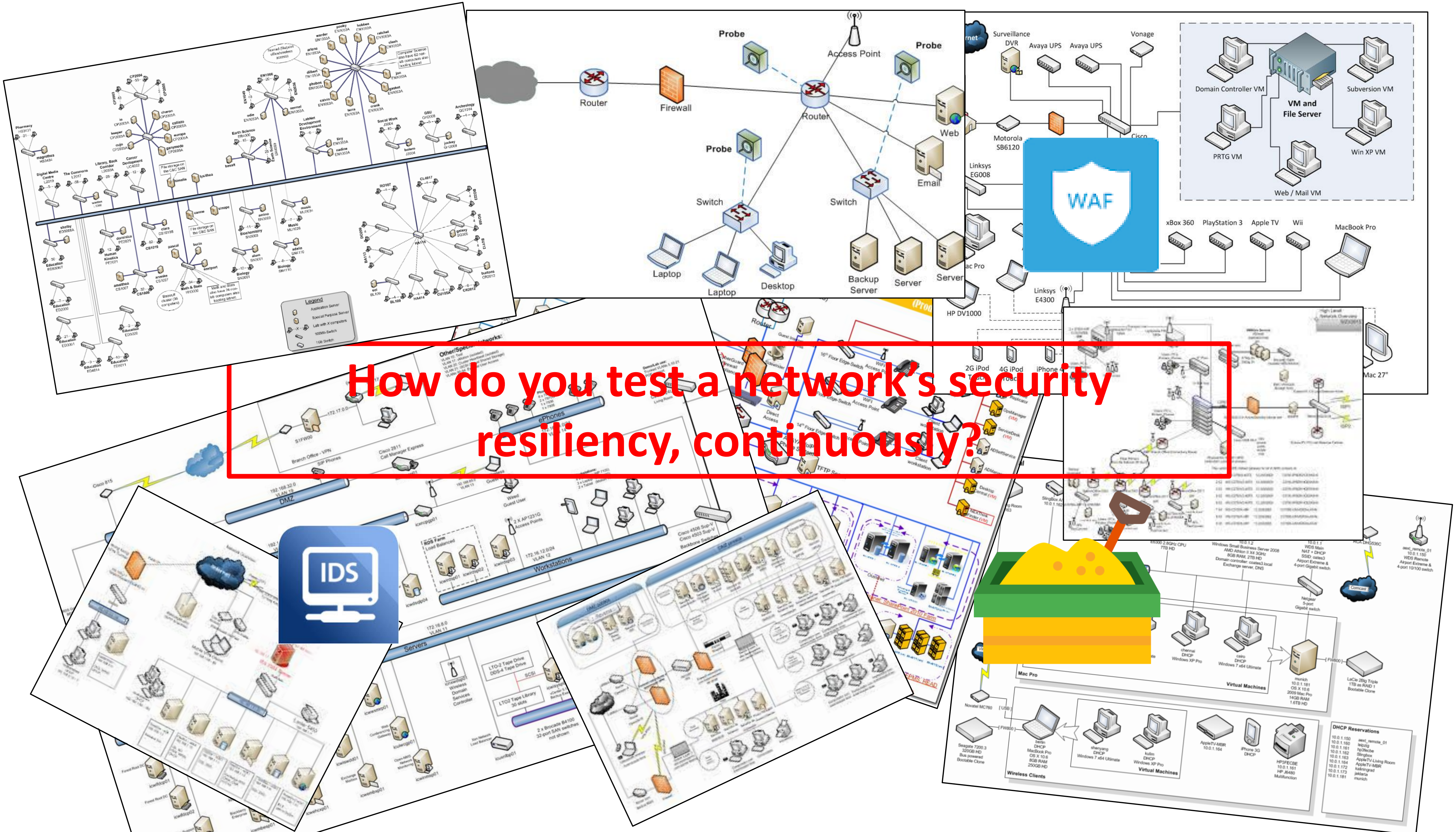
- Head of the Research Group at GuardiCore
  - Security research
  - Development of data analysis algorithms
- Msc in Computer Science
- Over 11 years of cyber security research experience

GuardiCore

- Data center security company
- www.guardicore.com

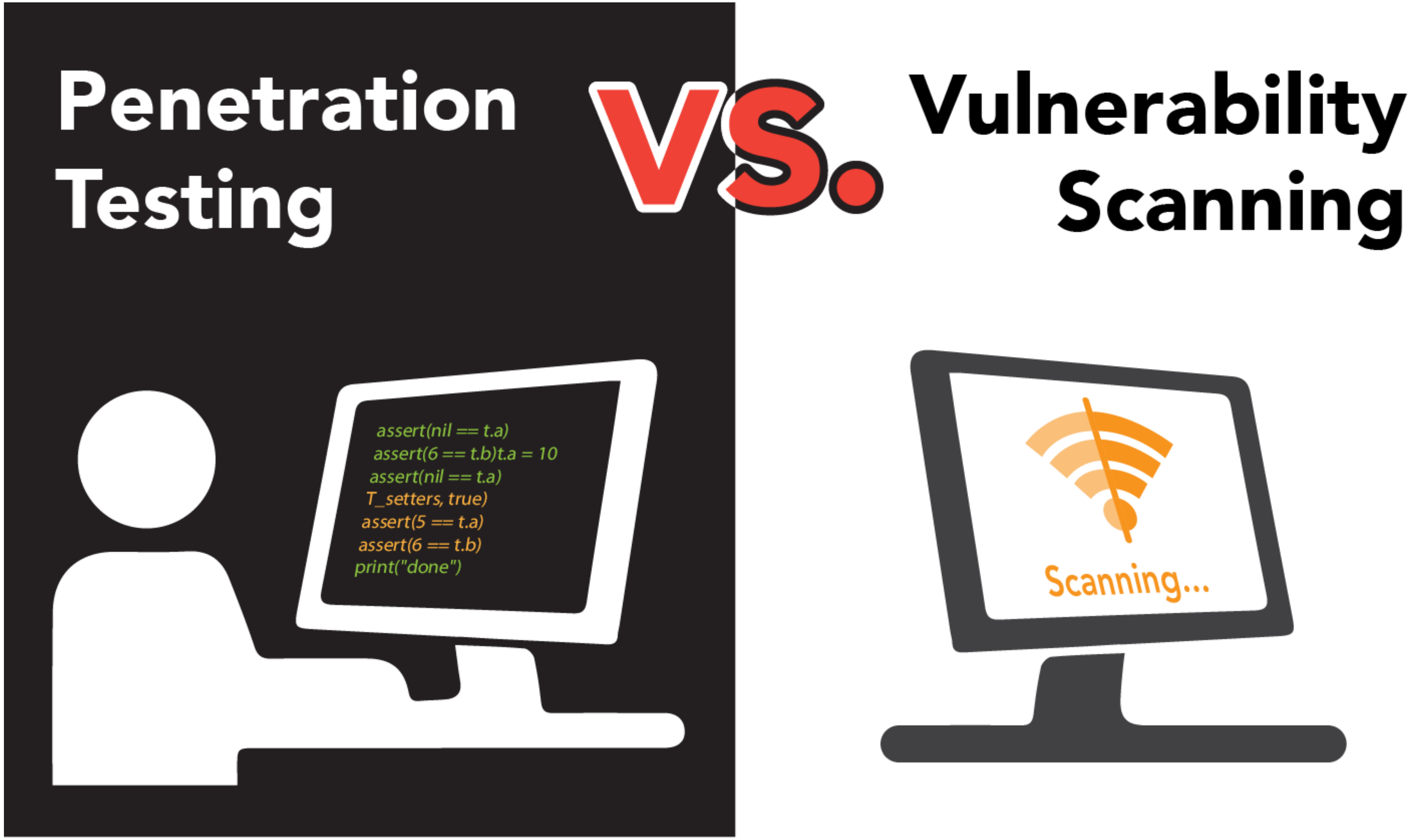
INFECTION MONKEY

Netflix Chaos Monkey



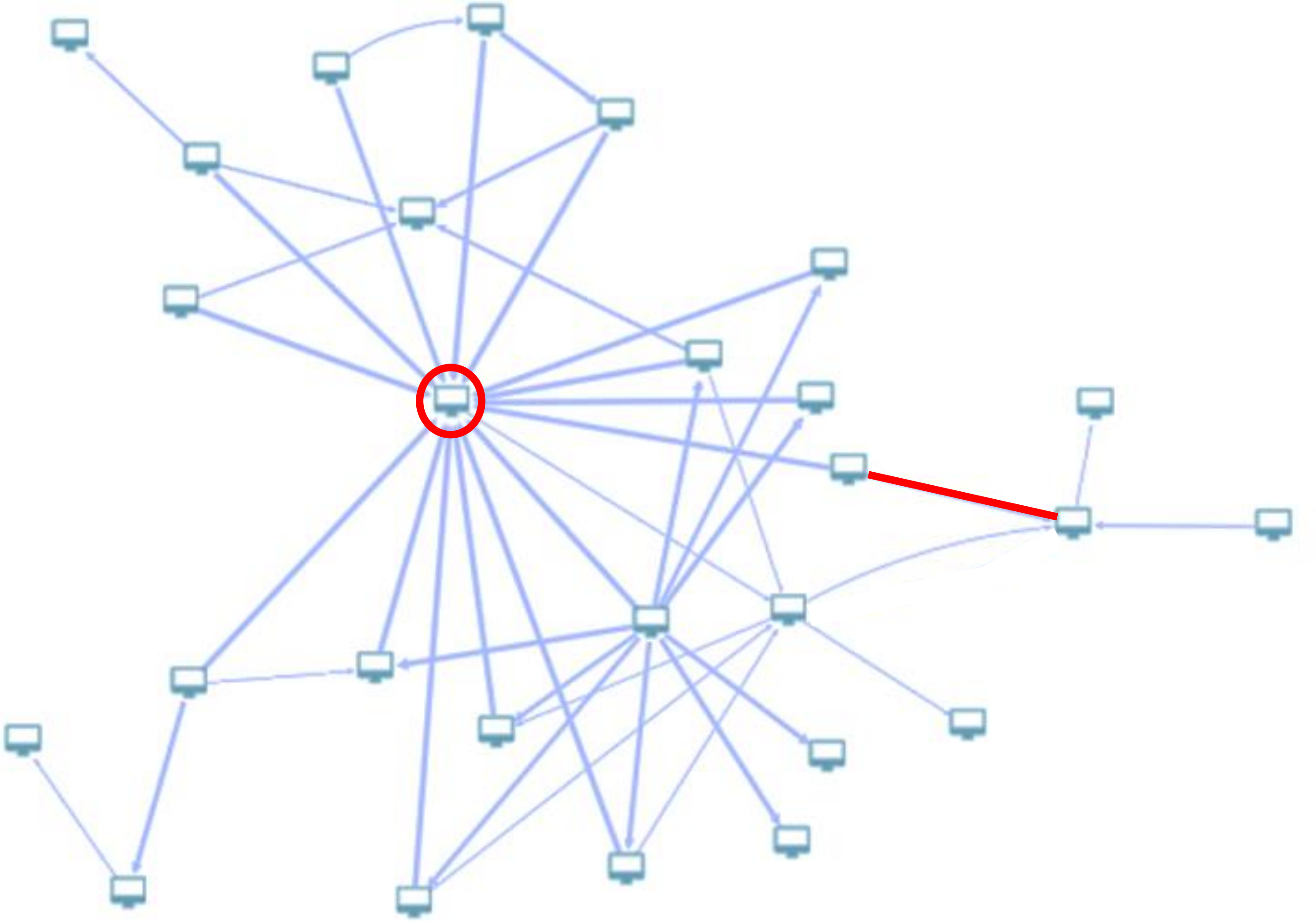
How do you test a network's security resiliency, continuously?

Current Approaches



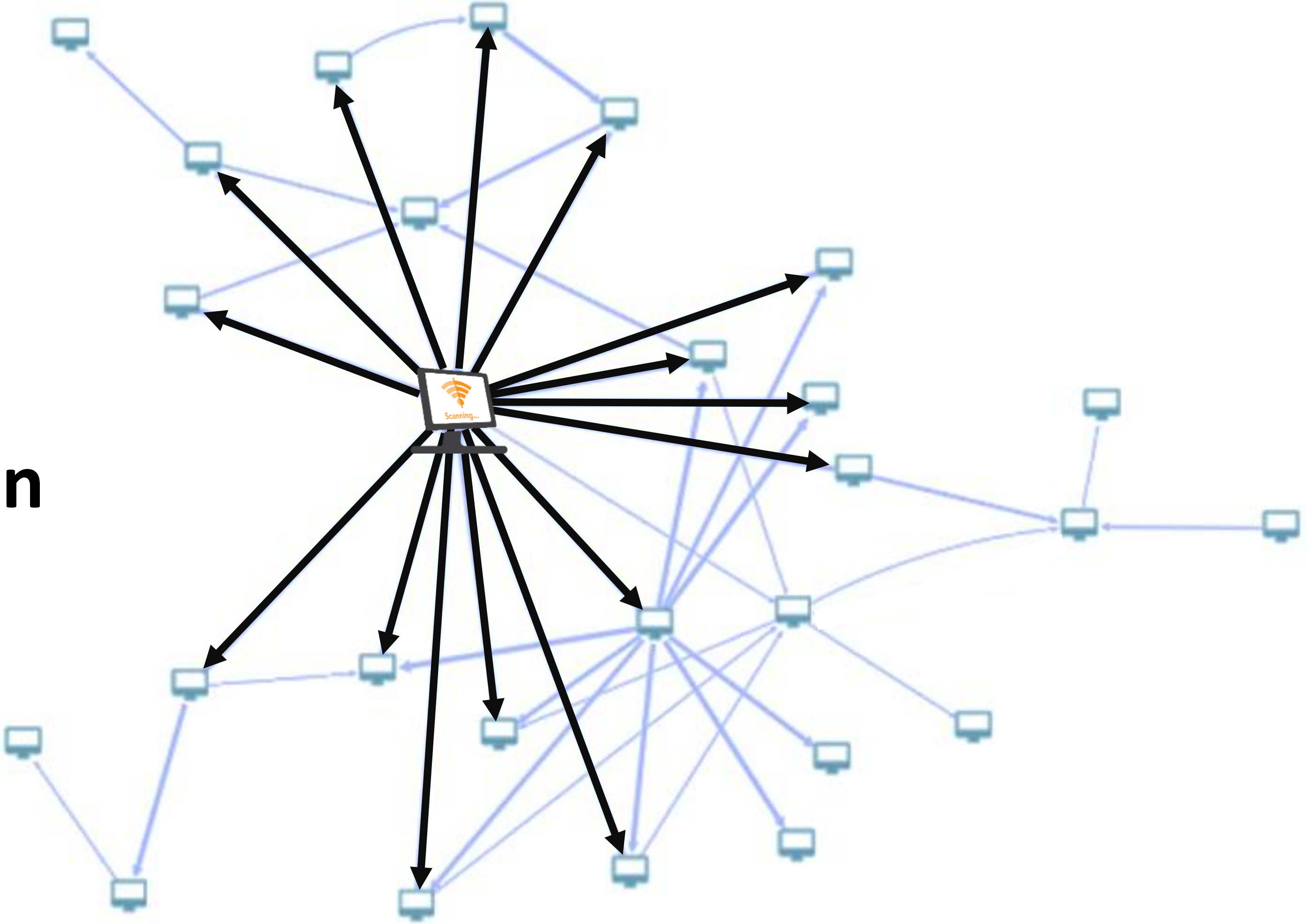
```
assert(nil == t.a)
assert(6 == t.b)t.a = 10
assert(nil == t.a)
T_setters, true)
assert(5 == t.a)
assert(6 == t.b)
print("done")
```

Here’s a network...



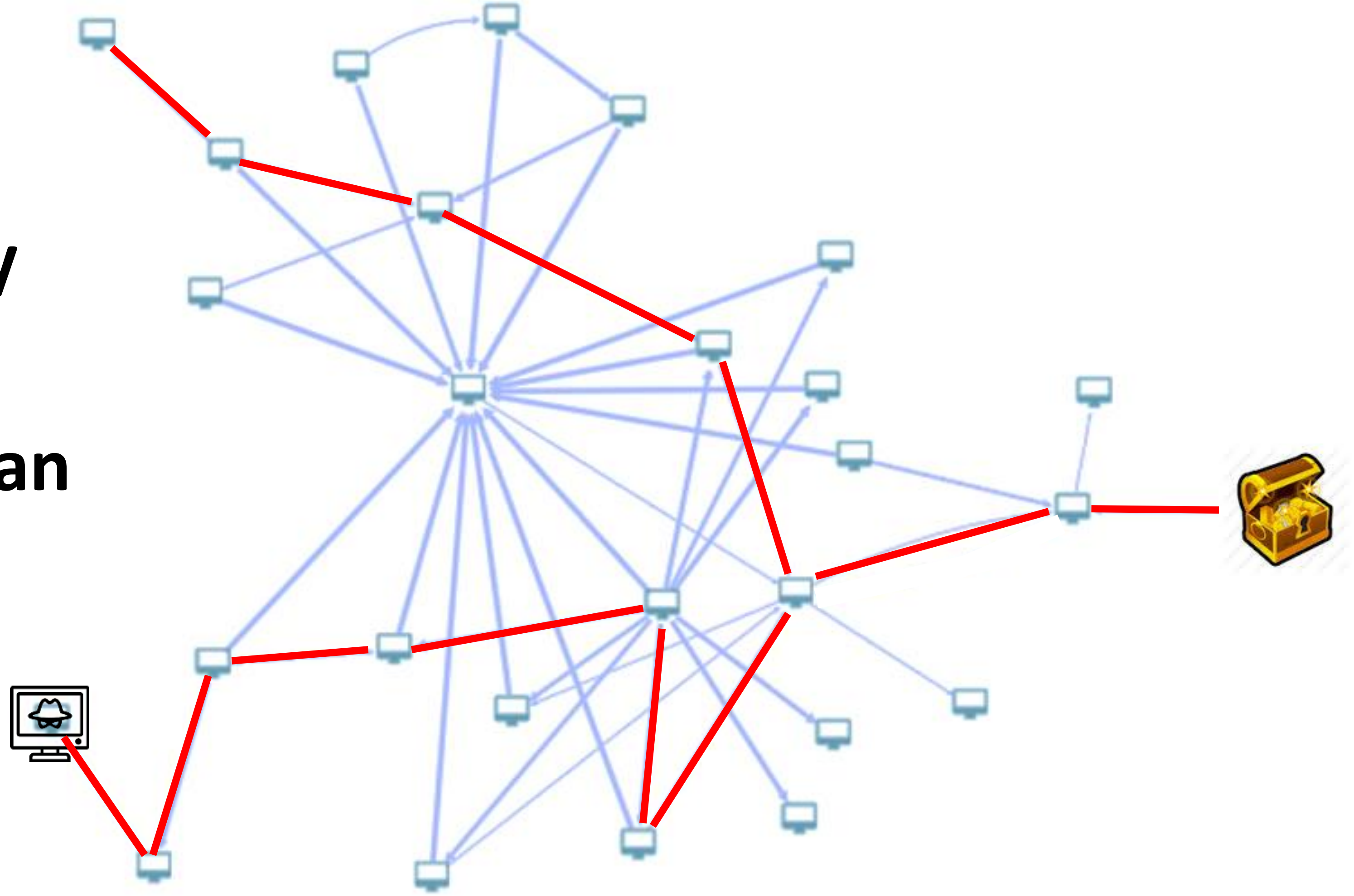
Vulnerability Scanning

- ☑ **Coverage**
- ☑ **Frequency**
- ☒ **Simulate an attacker**

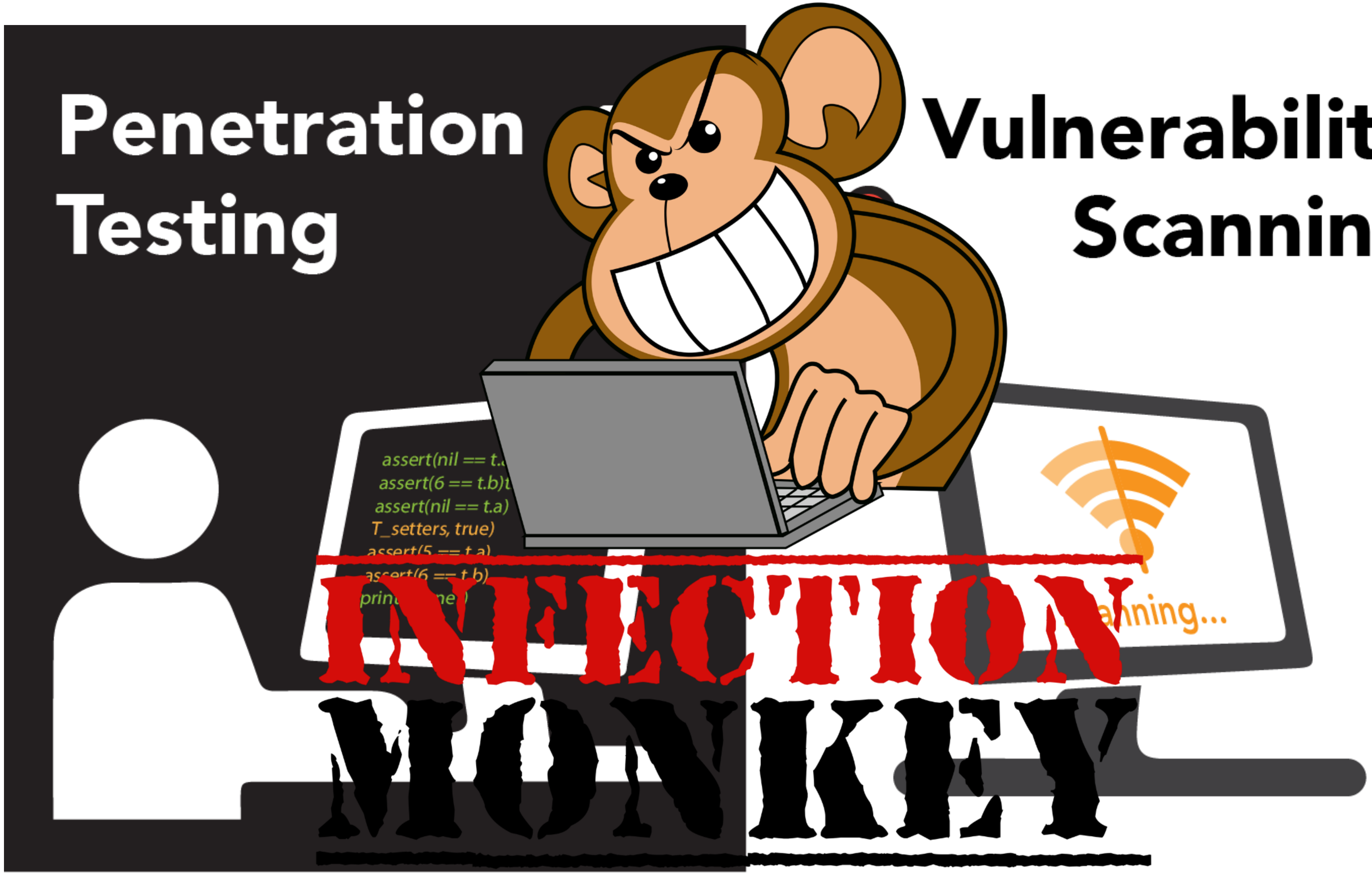


Pen te$ting

- ☒ **Coverage**
- ☒ **Frequency**
- ☑ **Simulate an attacker**



The Monkey Way

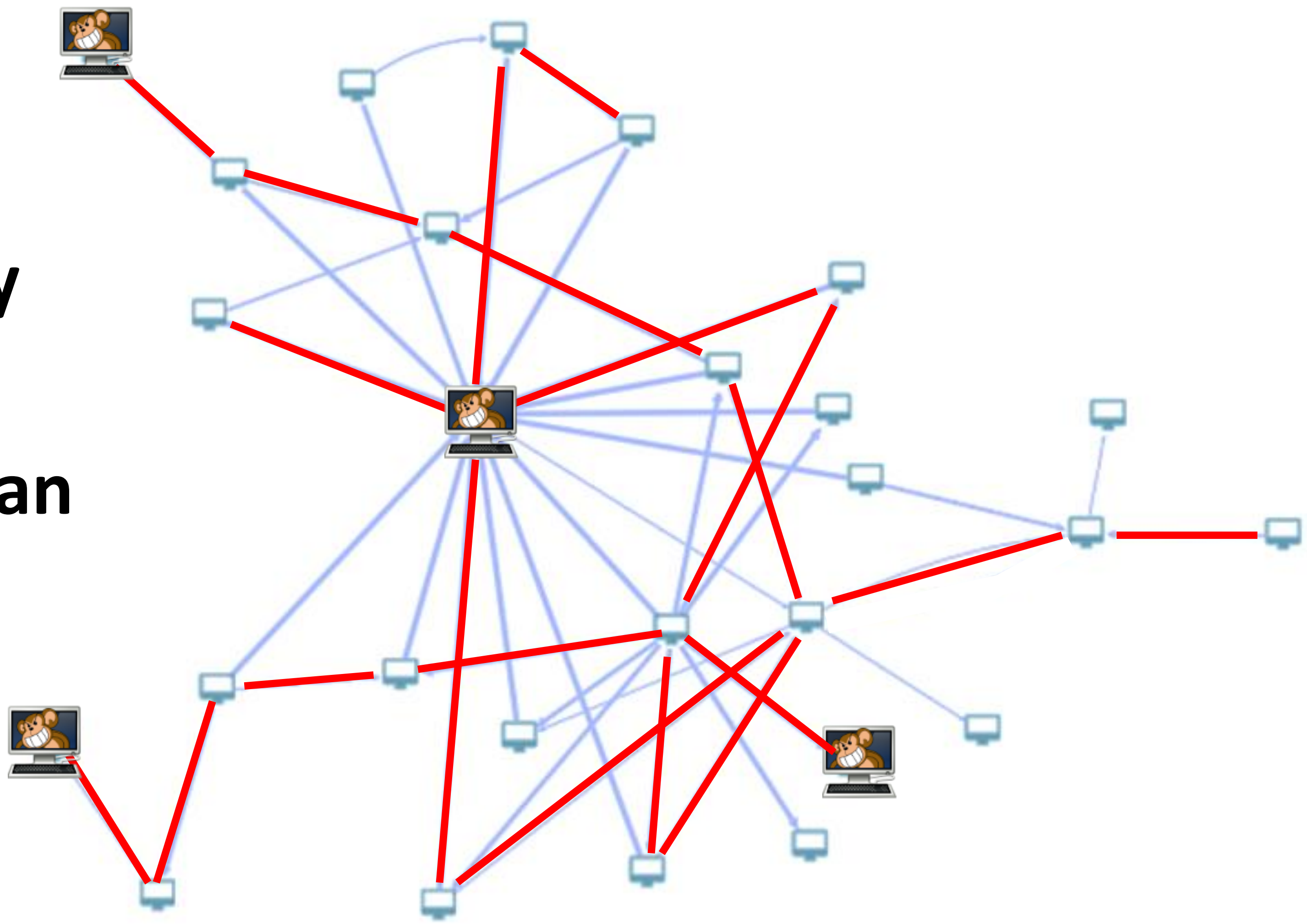


The Monkey Way

☑ **Coverage**

☑ **Frequency**

☑ **Simulate an attacker**



Monkey Benefits

1. Resiliency Testing
   - Simulates a real attacker
   - Propagate in-depth

2. Scale
   - “Pen Tester” in every VLAN
   - Full coverage

3. Automated tool
   - Continuous execution
   - Easy to use

Pick a random machine and see where the Monkey ends up…

- Start at a random location
- Find all propagation paths
- Continuous pen testing

Components

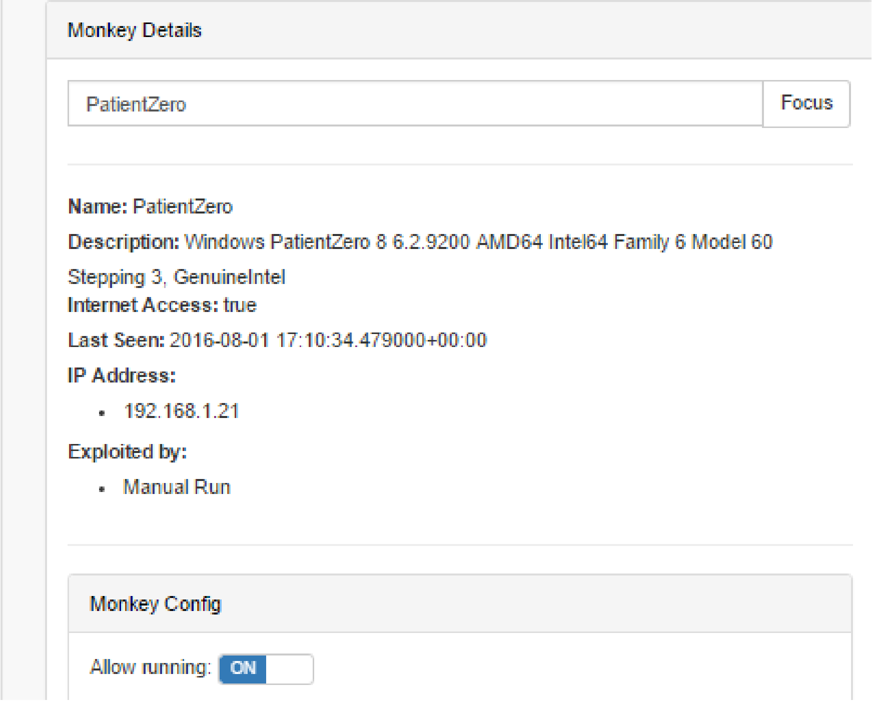
Self propagation tool

C&C server

Integrates with orchestration

Self Propagation

PatientZero
192.168.1.21



Name: PatientZero
Description: Windows PatientZero 8 6.2.9200 AMD64 Intel64 Family 6 Model 60 Stepping 3, GenuineIntel
Internet Access: true
Last Seen: 2016-08-01 17:10:34.479000+00:00
IP Address:

- 192.168.1.21

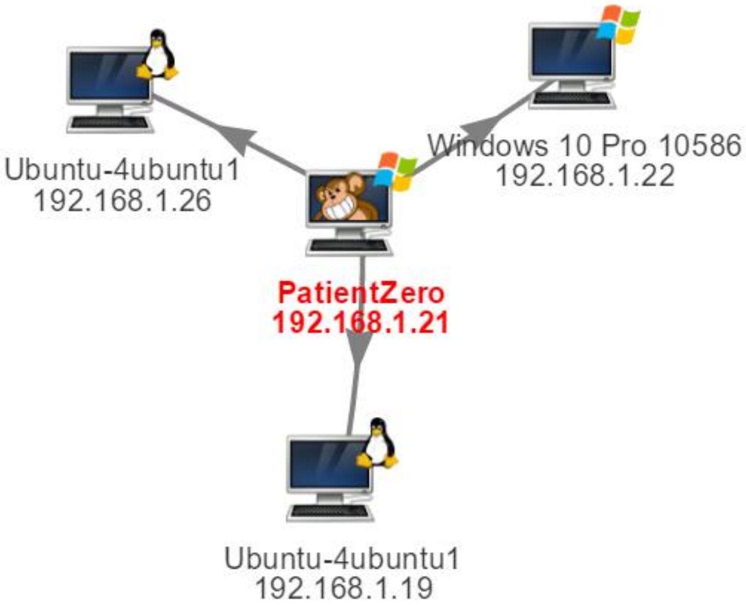
Exploited by:

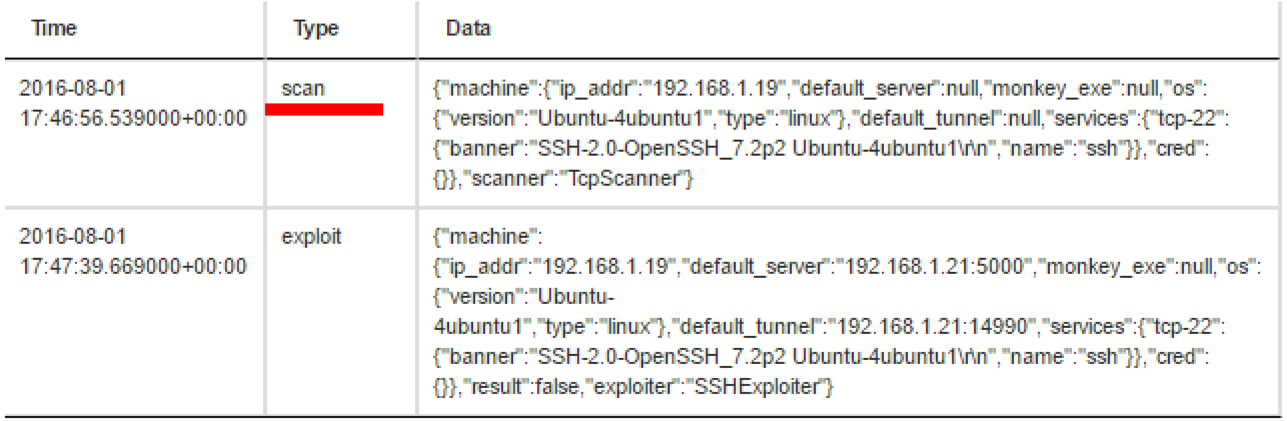
- Manual Run

Allow running: ON

Monkey Scans

- Fingerprinting
  - ICMP
  - Open ports





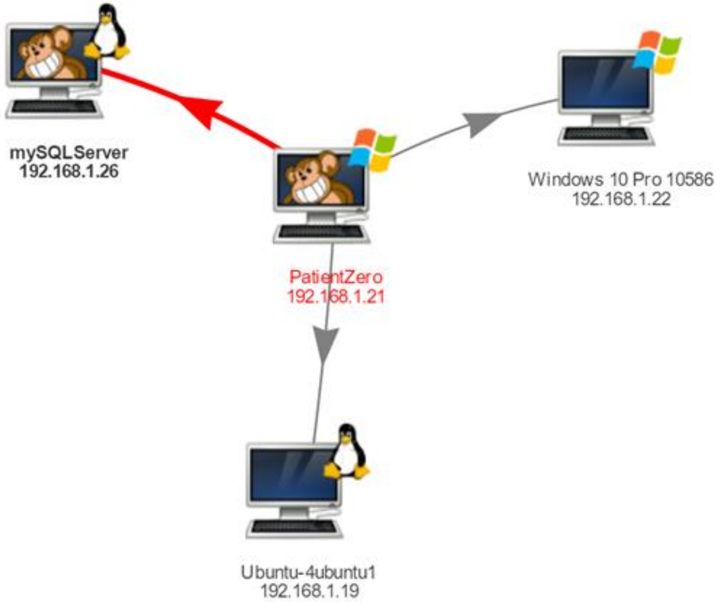
Time	Type	Data
2016-08-01 17:46:56.539000+00:00	scan	{"machine":{"ip_addr":"192.168.1.19","default_server":null,"monkey_exe":null,"os":{"version":"Ubuntu-4ubuntu1","type":"linux"},"default_tunnel":null,"services":{"tcp-22":{"banner":"SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu1\r\n","name":"ssh"}},"cred":{}},"scanner":"TcpScanner"}
2016-08-01 17:47:39.669000+00:00	exploit	{"machine":{"ip_addr":"192.168.1.19","default_server":"192.168.1.21:5000","monkey_exe":null,"os":{"version":"Ubuntu-4ubuntu1","type":"linux"},"default_tunnel":"192.168.1.21:14990","services":{"tcp-22":{"banner":"SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu1\r\n","name":"ssh"}},"cred":{}},"result":false,"exploiter":"SSHExploiter"}

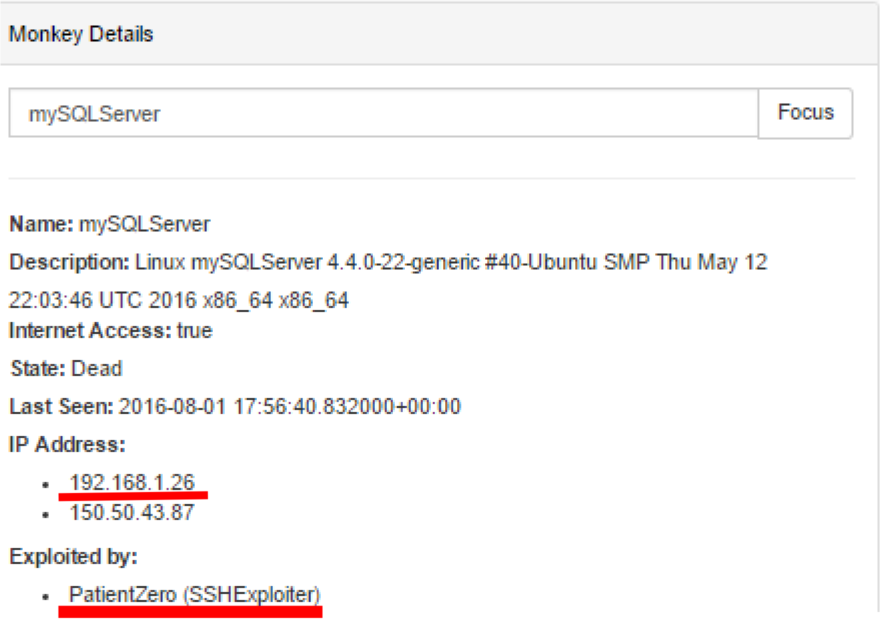
INFECTION MONKEY

MONKEY ISLAND

Monkey Attacks

- OS dependent
  - SSH
  - WMI/SMB/RDP
  - CVEs




Monkey Details

mySQLServer Focus

Name: mySQLServer

Description: Linux mySQLServer 4.4.0-22-generic #40-Ubuntu SMP Thu May 12 22:03:46 UTC 2016 x86_64 x86_64

Internet Access: true

State: Dead

Last Seen: 2016-08-01 17:56:40.832000+00:00

IP Address:

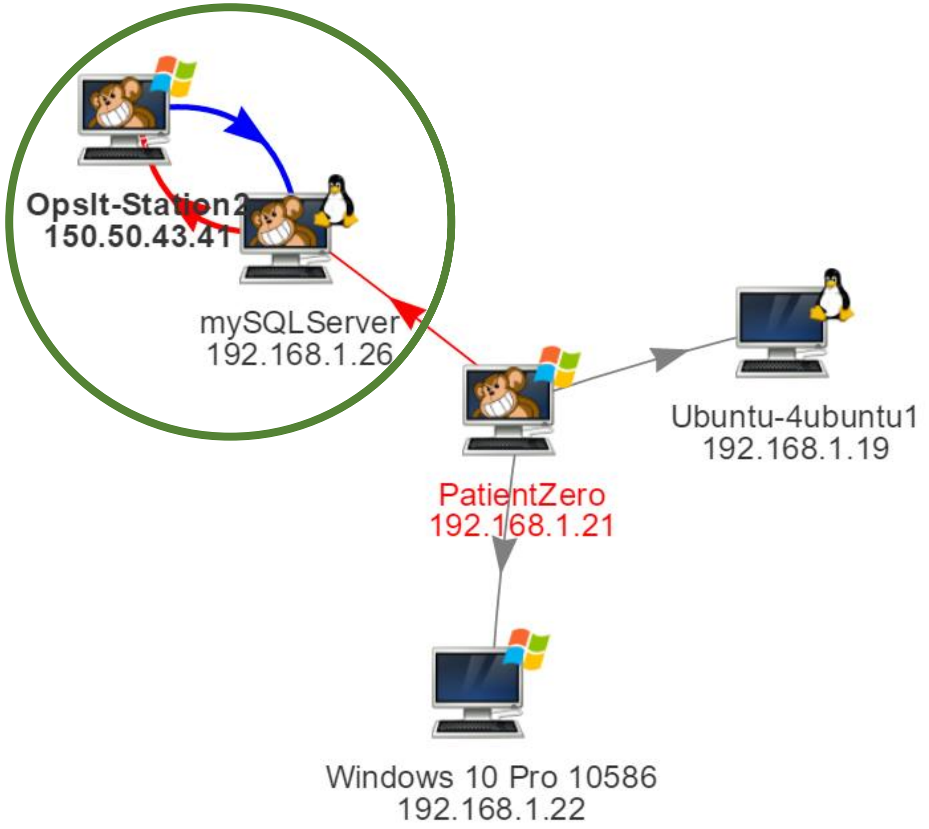
- 192.168.1.26
- 150.50.43.87

Exploited by:

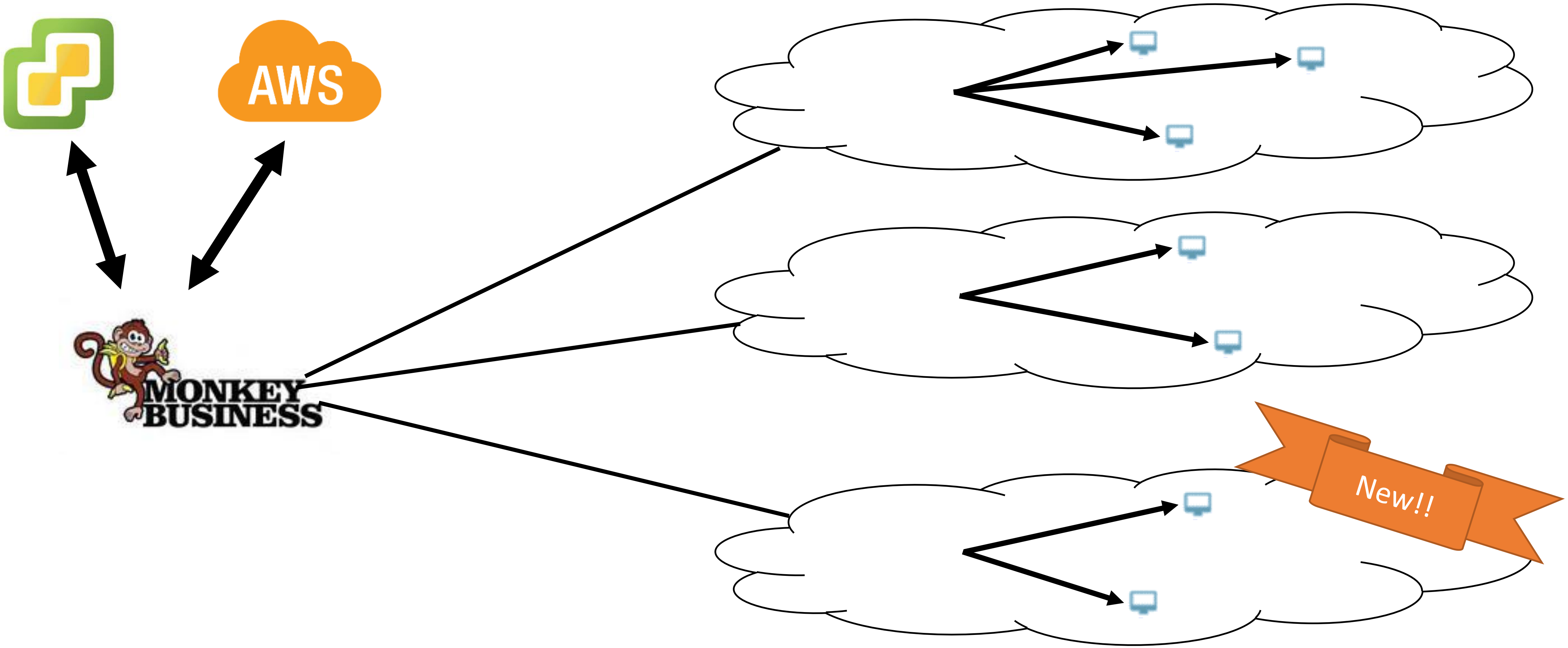
- PatientZero (SSHExploiter)

Monkey Tunnels

- Reach internal networks
- Tunnel through the Monkey chain



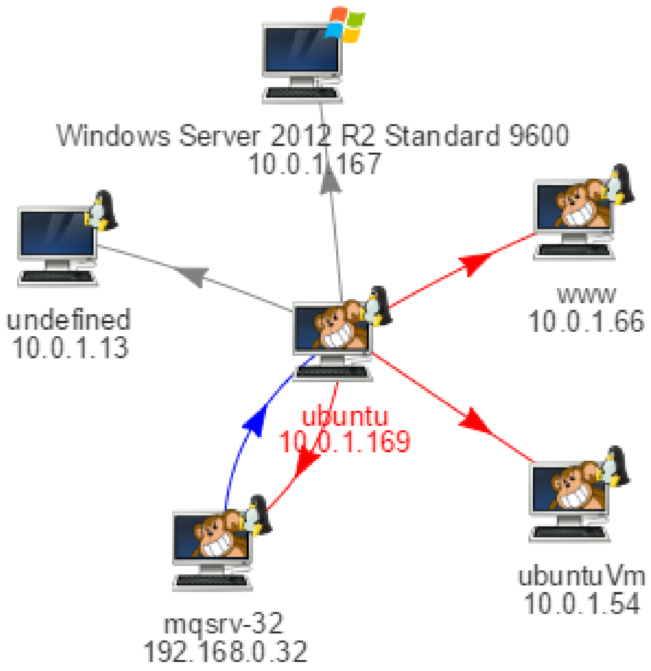
Monkey leverages orchestration data



Case Study

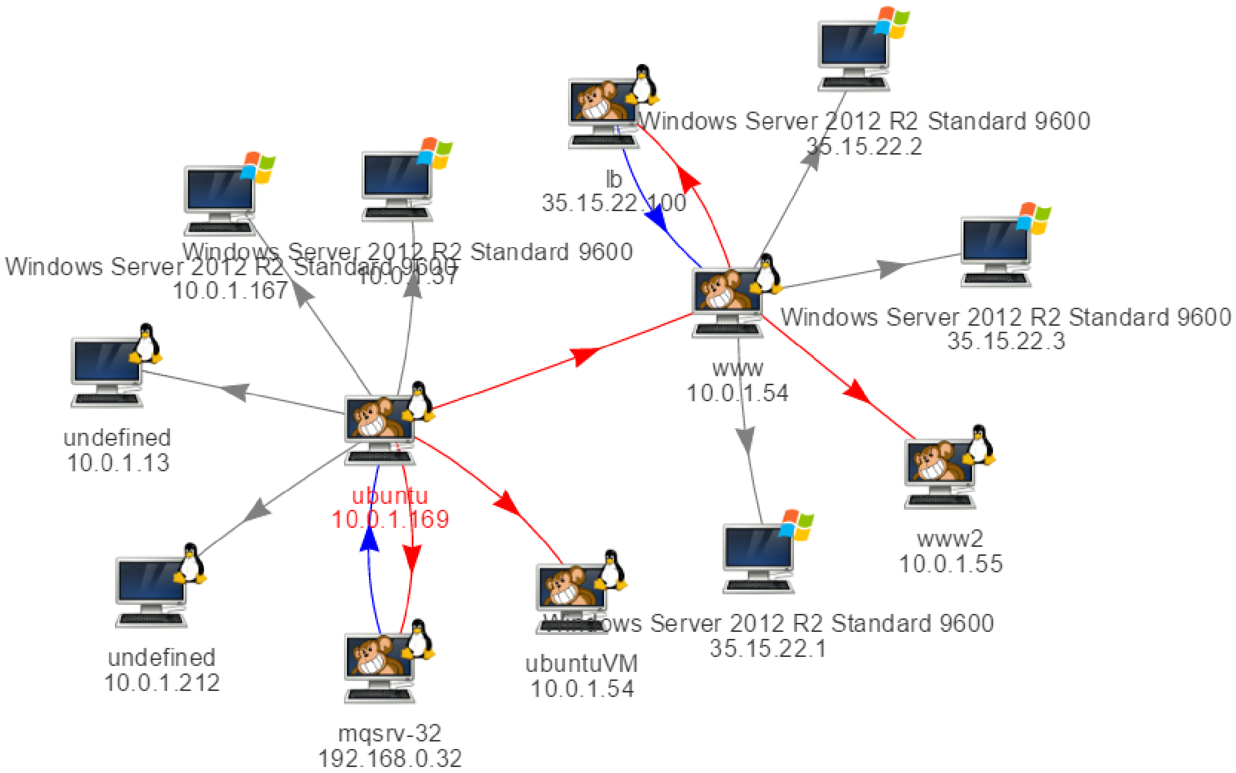
- Details:
  - Production network
  - 176 machines (Linux / Windows)
  - Dozens of separate networks

3 machines were breached

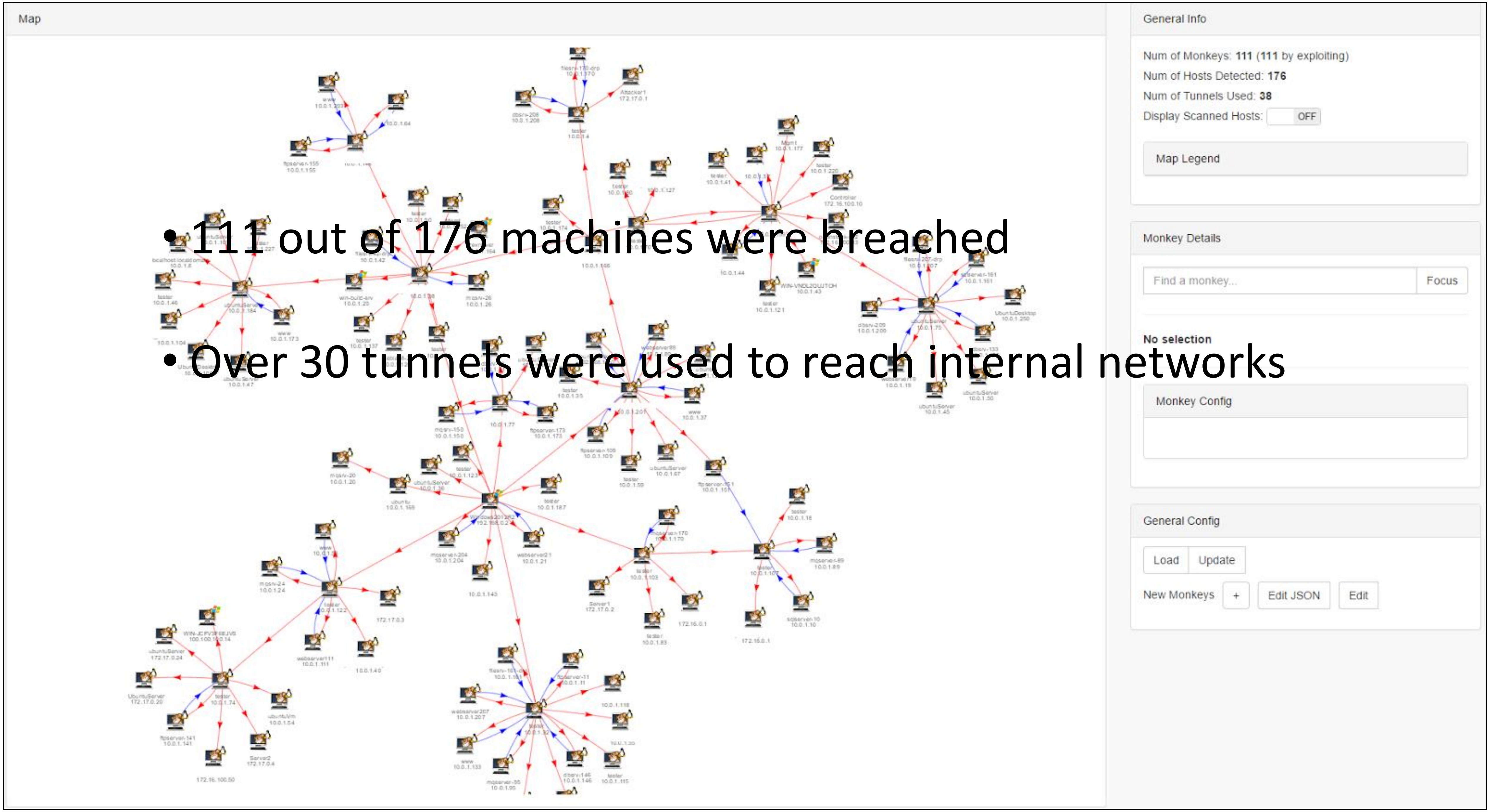


45 minutes later…

There’s always a way in…


lb
35.15.22.100
Windows Server 2012 R2 Standard 9600
35.15.22.2
Windows Server 2012 R2 Standard 9600
10.0.1.37
Windows Server 2012 R2 Standard 9600
10.0.1.167
Windows Server 2012 R2 Standard 9600
35.15.22.3
www
10.0.1.54
undefined
10.0.1.13
ubuntu
10.0.1.169
www2
10.0.1.55
Windows Server 2012 R2 Standard 9600
35.15.22.1
undefined
10.0.1.212
ubuntuVM
10.0.1.54
mqsrv-32
192.168.0.32

Eventually…



- 111 out of 176 machines were breached

- Over 30 tunnels were used to reach internal networks

General Info

Num of Monkeys: **111** (**111** by exploiting)

Num of Hosts Detected: **176**

Num of Tunnels Used: **38**

Display Scanned Hosts: OFF

Map Legend

Monkey Details

Find a monkey... Focus

No selection

Monkey Config

General Config

Load Update

New Monkeys + Edit JSON Edit

Live Demo

WIIFY

- Predict attacks by thinking like a hacker

- Mitigate threats before actual compromise

- Continuously validate network resiliency

Other Primates

- Metasploit
- Netflix’s Simian Army
- SafeBreach (startup)

Black Hat Sound Bytes

- Download the monkey at https://www.guardicore.com/infectionmonkey/
- Use the Infection Monkey to continuously test your network
- Contribute code and share techniques and ideas at https://github.com/guardicore/monkey

INFECTION
MONKEY

Q&A

infection.monkey@guardicore.com

https://www.guardicore.com/infectionmonkey/

Just Remember…

“What the monkey chooses to do with the technology is not necessarily an indictment of the technology itself.”