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
Netflix Chaos Monkey
How do you test a network's security resiliency, continuously?
Current Approaches

Penetration Testing VS. Vulnerability Scanning

```
assert(nil == t.a)
assert(t0 == t.b, a = 10
assert(nil == t.a)
T.setters.true)
assert(t5 == t.a)
assert(t6 == t.b)
print("done")
```
Here’s a network...
Vulnerability Scanning

Coverage

Frequency

Simulate an attacker
Pen testing

Coverage

Frequency

Simulate an attacker
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

Integrates with orchestration

C&C server
Self Propagation

PatientZero
192.168.1.21
Monkey Scans

- Fingerprinting
- ICMP
- Open ports
Monkey Attacks

- OS dependent
  - SSH
  - WMI/SMB/RDP
  - CVEs
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...
Eventually...
• 111 out of 176 machines were breached
• Over 30 tunnels were used to reach internal networks
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
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.”