RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: SP01-W03

Honeypot Predators: Hunter VS Prey

Aamir Lakhani

Red Team Researcher
Fortinet, FortiGuard Labs
@aamirlakhani

Who Am I?

Aamir Lakhani

- Red Team Researcher
- Fortinet, FortiGuard Labs
- Self-Proclaimed Professional Ghost Hunter

Let's Connect!

@aamirlakhani

me@this-conference.com

Blog: www.DrChaos.com

RSAConference2019

Introduction

What are honeypots?

Apply What You Learn

Today, we will hopefully complete the equation:

Educate + Learn = Apply

- Did I learn something new?
- Can I implement a honeypot safely in my environment?
- How do I make my organization more secure?

What is a Honeypot?

- System that mimics an organization's production environment
- Designed to attract and lure malicious actors
- Used to monitor cybercriminal behaviors
- Can interrupt the attack cycle, from initial information gathering to the active attack
- Primarily it intercepts cyber attacks in an observable environment
  - Learn cybercriminal tactics, techniques, and methodology

Types of Honeypots

Internal Honeypots

- Locked down systems with no advertisements
  - Access is a result of explicit attempts to find and exploit these systems
- They may provide vulnerable services – system is readily available for exploitation
- They are dangerous – use with caution!
  - Can be used by cybercriminals to perform ”land and expand” attacks
- They are used primarily to detect insider threats

External Honeypots

- Typically they operate outside your network, data centers, or domain
- Have public services
- Very open and available
  - Attract targeted and non-targeted attacks
- Attract sophisticated and simple attackers
- Can be dangerous if compromised unexpectedly

Low Interaction vs. High Interaction Honeypots

Low Interaction

- Passive in nature
- Collects usernames, passwords, login attempts
- Uses logs and packet capture for detailed analysis
- Examples include: SSH, Telnet, VoIP, elastic search, basic Windows services

High Interaction

- Allows attacker interaction with system
- Allows attackers to run commands and interact with systems
- Systems contain what appears to be valuable data (data is not really valuable)
- Records screens, commands, shells
- Almost a game or a challenge. Gives attackers a goal to infiltrate the system, bypass security, and use data exfiltration to transfer critical information from the system.

RSAConference2019

Implementation and Deployment

Where and how to run your honeypots

Honeypot Placement Considerations

Internal Honeypots

- On secure, isolated, and segmented network segments
- Not advertised in DNS, ActiveDirectory, or via simple network protocols or services (pings, SNMP scans)

External Honeypots

- Not connected to your network or data centers
- They generate a lot of ‘noise’
- Can be configured for multiple types of services such as WordPress, IoT devices, critical infrastructure, IoT/OT, custom applications

Honeypots – Easiest Implementations

Internal Honeypots

- Isolated network segments

External Honeypots

- Service providers
- Hosting providers
- Virtual Private Server (VPS) or cloud providers
  - CRITICAL - review terms of service with your hosting provider
- Another option - your friend's house (just kidding)
- CRITICAL - review terms of service with your hosting provider

Some Recommended Settings for Honeypots

2 public addresses

- One for management
- One for honeypot services

Do not use Network Address Translation

- Some attacker services are not correctly recorded with NAT

VPS services

- Lots of attacks will cause termination of services

Honeypot cautions and compromises

- Can become a malware host
- Beware of illegal content

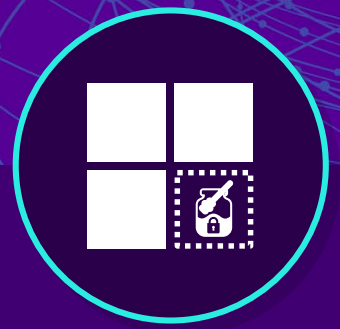
Honeypot Base Configurations

Base

- Ubuntu 14.0.4.1 LTS 64-Bit
- 2 Gb of RAM
- 20 Gb HD

Port 80 honeypots

- conpot
- glastopf
- wordpot
- shockpot



Windows honeypots (445 and 139)

- Amun
- Dionaea

Others with no port conflict

- kippo
- p0f
- elastichoney

Other Honeypot Ideas

- Open ‘listen’ ports for major malware attacks
- Mimic ports on major devices (IoT, OT, etc.)
- Use logs and packets captures (PCAPs)
- Create Windows systems with malware URL feed
  - Run malware sites thru a non-admin account
  - If compromised - you might have found a zero day
- Open FTP server (or one that can be brute forced easily)

RSAConference2019

Honeypot Demo

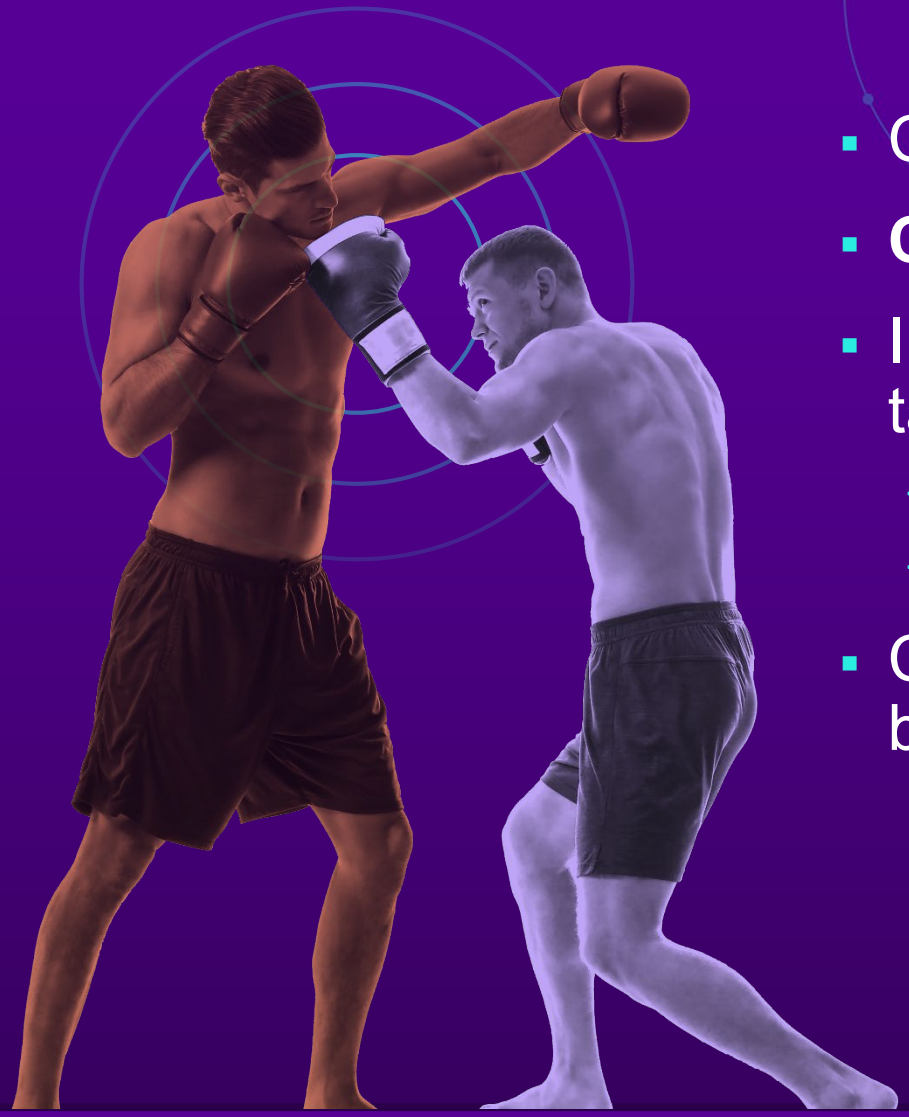
MHN, FTP Honeypot Demo

RSAConference2019

Offensive Security

Hackback and other techniques

What is a Hack Back?



- Counter-attacking those that attack you
- **Caution** – not legal in many countries
- I do not condone what we will be talking about now
  - Everything is hypothetical
  - This has legal implications
- Consider the following occurring in the make believe place of MagicLand

US Hack Back Laws

- Active Cyber Defense Certainty Act (ACDC)
- Computer Fraud and Abuse Act
- Hack back is obviously not a defensive strategy

Phishing to Plant Malware

1

Phisher sends email or contact regarding malware that is seen on your device

2

You are fooled into opening up your system or installing malware to give attacker access to your system

3

Lets pretend it's a fake Microsoft helpdesk claiming our computer is spewing malware. They are a "contractor" of Microsoft when asked.

Counter Phishing Honeypots

1

Setup safe place to interact with phisher — sandbox

2

Act stupid and talk about The Matrix and Blackhat movies. Maybe mention hacking movies and how cool Mr. Robot is.

3

Wrap sharing software with malware

4

Frustrate phisher but offer sharing software to help show why things are not working

Building a Sandbox – Cuckoo as a Honeypot

- The steps to fully install Cuckoo are super complex so read our guide in my book or blog
- Malware looks for Cuckoo
  - Looks for virtualization processes
    - Memory, CPU, Cores, VM Tools, registry entries
    - Looks for specific DLL files such as sbie.dll
    - Real malware analysis means bare metal testing

Dropper, RAT, Empire and Metasploit

Dropper

Beaconing software that doesn't provide a full tunnel and can call back desired data

RAT

Full tunnel to compromised system

Empire

Powershell tool that can communicate using a dropper

Metasploit

Developer meterpreters that can be installed on the victim system

Getting Your RAT

- RATs are detected by AV
  - Counter it by building your own using a PowerShell or Python framework
  - Works on Mac OSX and Windows devices
- EggShell is a good Python based RAT framework that works on MacOS
- ViralmaniaR PowerShell RAT is a another good example
- Infects by connecting back to a public server
  - Send a phishing link
  - Send an uninfected file

Easy Honeypot Projects

- MHN – Modern Honey Net from Threatstream
- HoneyPI
- Fortinet Deceptor
- Thinkst Canary
- TrapX
- Illusive Networks
- Attivo Networks

How We Use Honeypots

Malware Honeypots

- Replication attacks
- Simulate known vulnerable clients, IoT/OT devices, others

Spam Honeypots

- Simulation of open email relays, open Web proxies, open DNS servers
- Allows small number of attacks to occur
- Blocks large attacks (common setup procedure)

Server Honeypots

- Open ports, services, applications (SQL, ElasticSearch), and system emulation

Proxy Honeypot

Top Countries
(from IP Geo Lookup)

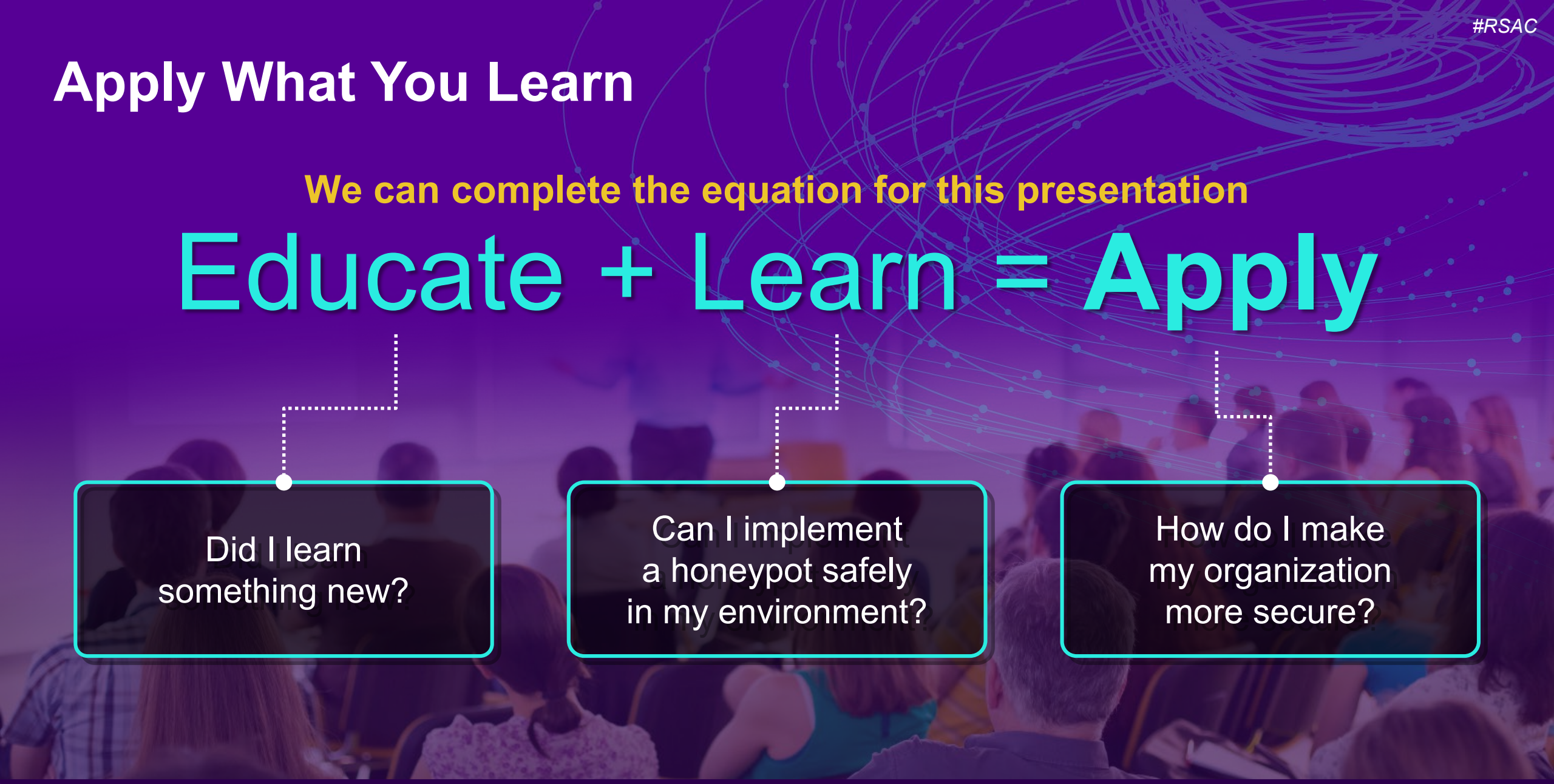
- Unlisted Proxy created
- Ports for proxy were 80, 8080, 3128
- SSL Proxy created for HTTPS on port 443 with self-signed certificate
- Top Sites:
  - Google
  - Various adult themed sites

Apply What You Learn

We can complete the equation for this presentation

Educate + Learn = Apply

- Did I learn something new?
- Can I implement a honeypot safely in my environment?
- How do I make my organization more secure?



What We Covered

Honeypots

- Deceptive tools designed to learn about the attacker's motivations and techniques
- Can be simple as open ports or simple network services running on a system
- Software such as MHN, Dionaea, HoneyNet provide pre-configured honeypots
- Can be compromised and cause lots of damage

What We Learned

Where to deploy honeypots

- Do you care about insider threats? External threats?

How to automate honeypots

- Use a supported commercial tool
- Use open source tools
- Create your own

What I can do with a honeypot

- Learn who is attacking you
- The techniques they are using
- Automate IOCs into security and logging devices

RSAConference2019

Proxy Honeypot Demo

Look what we found

RSAConference2019

Thank You!

Aamir Lahani

Fortinet, FortiGuard Labs

@aamirlakhani