
# Cloud Security

## An introduction to cloud security for researchers

Michael Karich

Dr. Thomas Laurenson

July 2024

# So why must we do this?

# What is being targeted?

- EDUCAUSE ranks cybersecurity as 2024 #1 core competency
- 116 disclosed successful cyberattacks against universities in 2023
- Now targeting libraries and third party components
  - RegreSSHion, Log4J, ZX Utils
- 97 zero day vulnerabilities in 2023
  - Decreasing number of financially motivated attacks
- Spam and Spear Phishing are still very common vectors for credential harvesting
- Average cost of a data breach is $6.03 Million NZD

ResBaz

# What are we doing?

- Training & Best Practices
- Scanning and awareness
- Managed services (Nectar, Connect VMs, Web Hosting)
- Security staff

KB5032249: Windows Server 2012 R2 Security Update (... Critical 390

| | Total | Critical | High | Medium |
|---|---|---|---|---|
| Exploitable | 63.1K | 13.1K | 18.6K | 28.8K |
| Malware | 10.4K | 4.9K | 4.3K | 1.1K |
| Core Impact | 0 | 0 | 0 | 0 |
| Canvas | 1.9K | 634 | 766 | 468 |
| Elliot | 185 | 14 | 114 | 57 |
| ExploitHub | 0 | 0 | 0 | 0 |
| Metasploit | 4.7K | 1.7K | 1.8K | 1.2K |

ResBaz

# Security of the Cloud & Security in the Cloud

- Cloud Provider (UoA / AWS / etc)
  - Patching *
  - Infrastructure
  - Capability
  - Visibility
  - Secure by Design / Default
- User
  - Code vulnerabilities & dependencies
  - Service availability
  - Patching *

ResBaz


The probe used multiple SQL injections.
I've yet to find any compromised files.

# Cloud Security


Main goals of today:

- Change thought pattern about security
- Outline methods to improve cloud security
- Review attacker techniques

ARDC Nectar Research Cloud

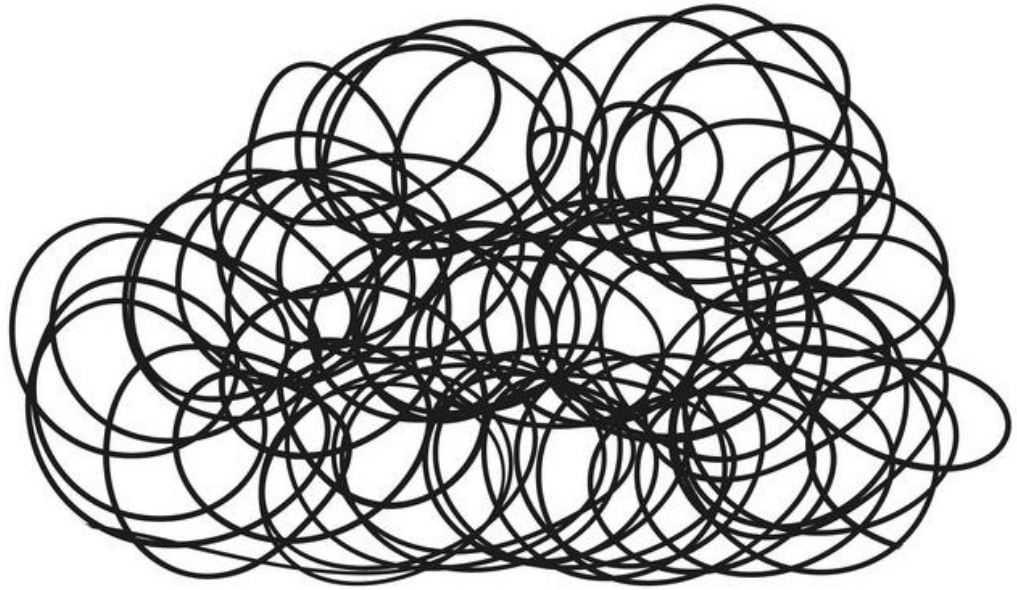
Azure

Google Cloud

ResBaz

# Cloud Security is Hard

- Multiple platforms
- Multiple systems/solutions
- Self-managed
- Not secure by default
- Information overload
- Difficult terminology



ResBaz

# Today's Top 5

1. Layers are essential
2. Expose ~~nothing~~ only essential services
3. Upgrade ~~everything~~ as much as possible
4. Harden ~~everything~~ essentials
5. Let someone else manage it

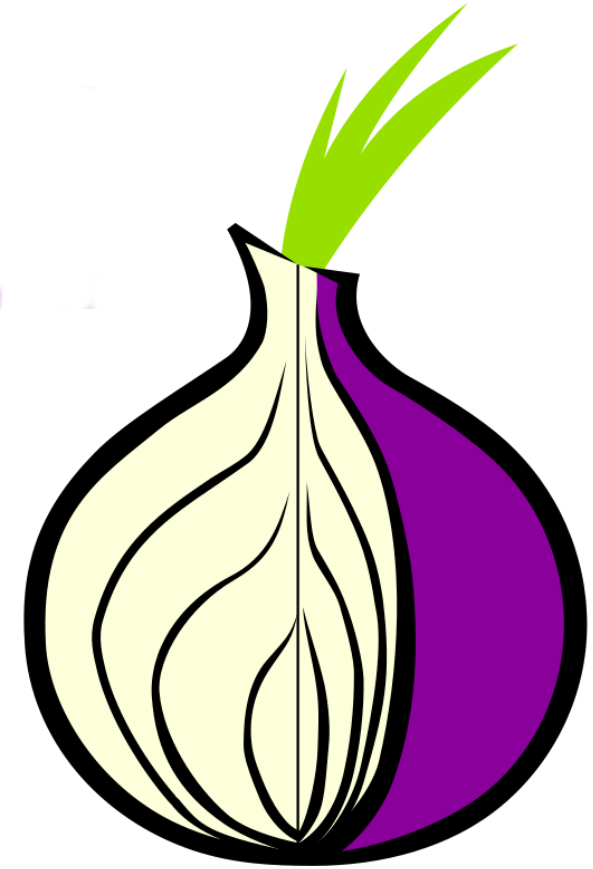
ResBaz

# 1 Layered Security

- Security is like onions 😭
- Layered approach - numerous solutions
- No one single solution is enough to reduce risk

**Example:**

- Login using username/password
- Then enter authentication code from phone
- Traffic is *encrypted* between you and server
- Your password is *hashed* on server



ResBaz

# 2 Expose Only Essential Services

- Cloud computing and the Internet are inherently linked
- Provides Internet-accessible "resources" (e.g., server)
- Console is Internet-accessible (web UI, remote access)

**Best Practices:**

- Only expose what needs to be on the Internet
- Restrict access using "Security Groups"
- Remove access by "Network Segmentation"


ResBaz

# 3 Upgrading

- Keeping your operating system up-to-date
- Keeping installed software up-to-date
- Aspects can be automated

```
sudo apt upgrade -y

sudo yum update
```


ResBaz

# 4 Hardening

- Configuring system/software to be more secure

**Examples:**

- Set HTTPS on your web server, disable any HTTP
- Set SSH to only allow key authentication, disable password login
- Set RDP connections to only accept from specific IP addresses
- Install intrusion prevention software (e.g., fail2ban)

ResBaz

# 4 Hardening – How?

- CIS Benchmarks
  - https://www.cisecurity.org/cis-benchmarks
  - AWS CIS Foundations Benchmark
  - CIS compliance with Ubuntu LTS

- AWS Best Practices
  - https://aws.amazon.com/getting-started/aws-security-essentials/
  - https://docs.aws.amazon.com/security/

- Nectar Knowledge Base
  - https://support.ehelp.edu.au/support/solutions

CIS Center for Internet Security®

ResBaz

# 5 Third Party Management

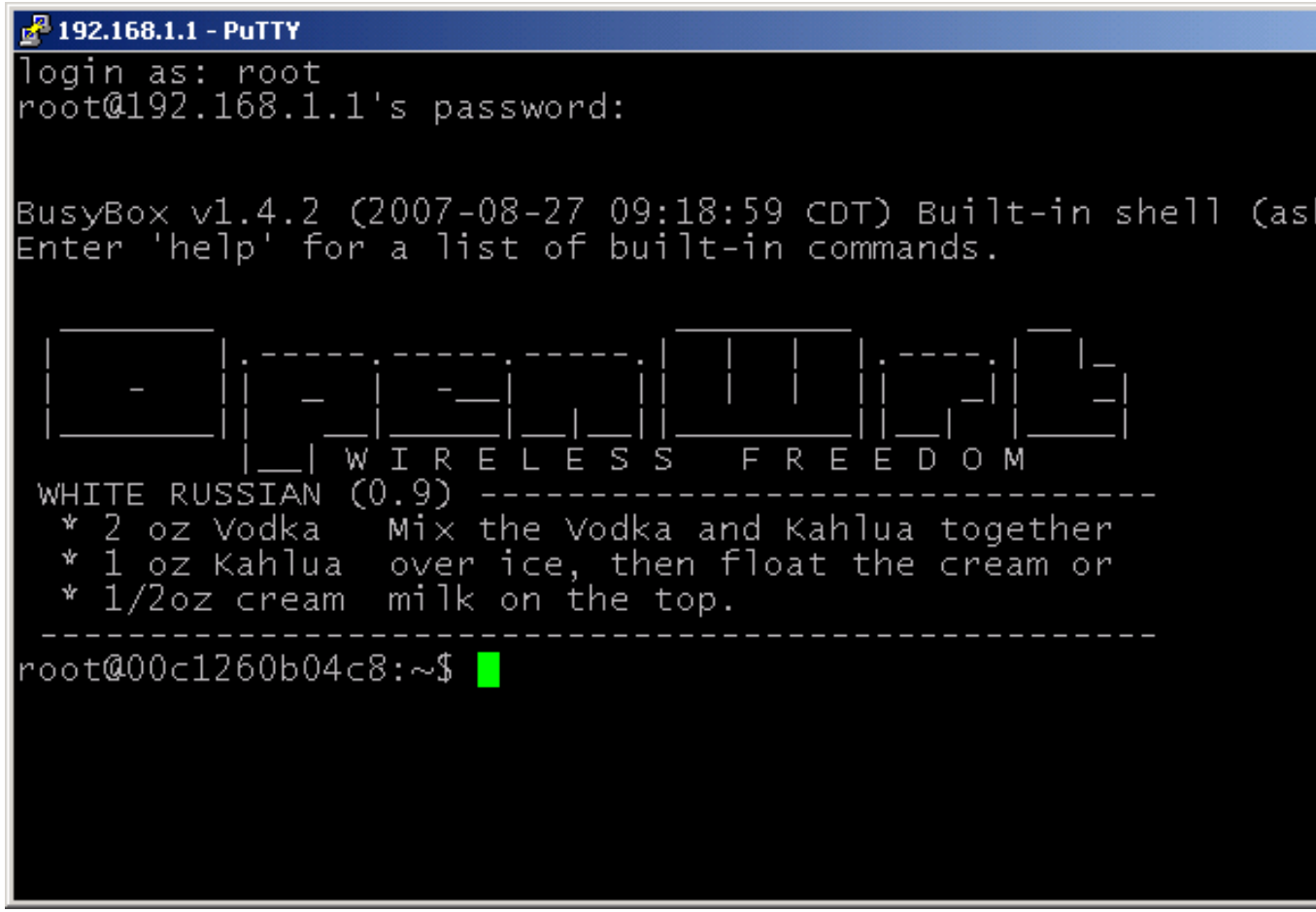
- Use a "university-managed" service
  - Nectar External
  - Virtual Machines

- Use "vendor-managed" service
  - AWS Managed Services (do security, backups etc.)

ResBaz

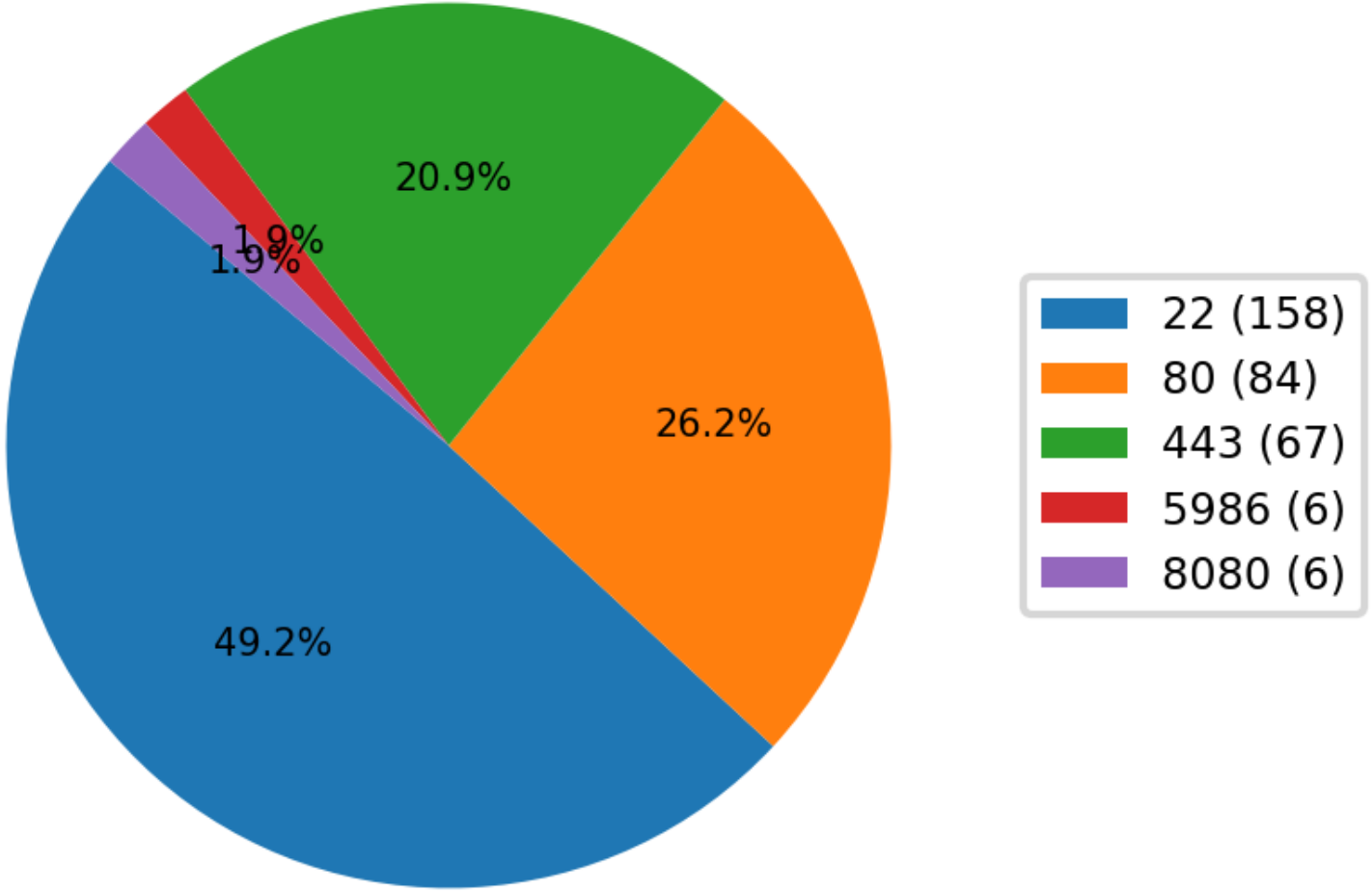
# Security Scenario - SSH

- Secure Shell
- Linux (and others)
- Used for remote management
- Log in, run commands
- Ubiquitous




ResBaz

# Security Scenario – Why SSH?




ResBaz

# Security Scenario – Why SSH?

- New SSH security vulnerability
  - Remote
  - Unauthenticated
  - Code execution
- CVE-2024-6387
- July 2024


ResBaz


HACKERMAN

# Security Scenario – Auditing SSH

- Review SSH log
- Attack!
  - Check SSH access from remote IP
  - Review SSH service information leakage
  - Perform password attack against SSH
- Review SSH log again
- Secure!
  - Implement SSH security group
  - Check SSH access from remote IP

ResBaz

# "User" Input is Dangerous

- Anywhere you allow a **user to input anything**
- Think forms on web pages
- However, attackers can do tricky things...

**Users can input things where you allow machines to input**

ResBaz

# Today's Top 5 - Revisiting...

1. Layers are essential
2. Expose ~~nothing~~ only essential services
3. Upgrade ~~everything~~ as much as possible
4. Harden ~~everything~~ essentials
5. Let someone else manage it

ResBaz

# Nectar ♥ Researchers

- Linux distributions have:
  - Automatic security updates configured
  - Pre-installed and configured fail2ban service
  - SSH configured for keys-only by default

- Windows systems have:
  - Very strict RDP security

- Some new things being planned:
  - Additional default security groups using best practices
  - Security alerts for dangerous configurations

ResBaz


ResBaz
RESEARCH BAZAAR
Any Questions?
Michael Karich
Dr. Thomas Laurenson
July 2024