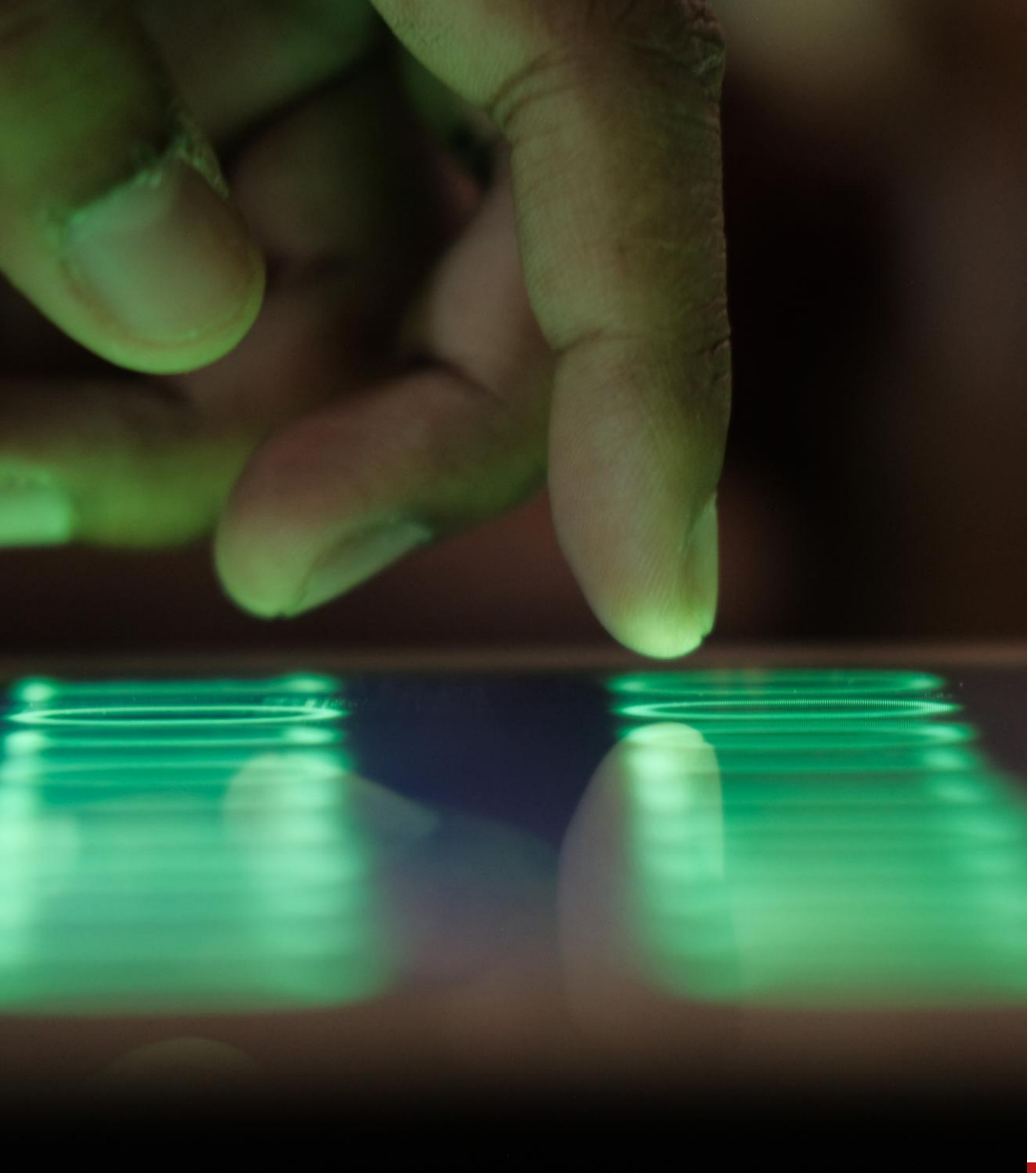


Metasploit

What Attackers Do With It & Why You Should Know

Copyright © 2026 Secure Ideas LLC



Agenda

- Blue Team vs Red Team
- The Hackers Toolkit
- The Metasploit Framework
- Demo
- Evasion Techniques
- Defense Strategies
- Case Study

Kathy Collins

Security Consultant Secure Ideas, LLC

- Been with Secure Ideas since 2021
- Based in Jacksonville, Florida
- Sec+, CISSP



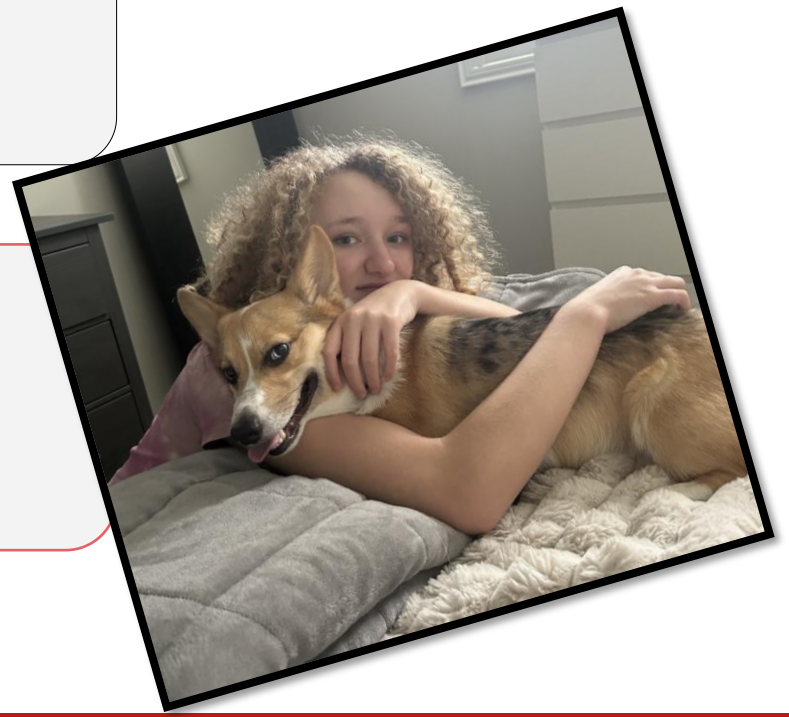
kathy.collins@secureideas.com

Focus Areas

- Networks
- Web Applications
- Physical Pentesting
- PCI-DSS

Other Fun Facts

- Former Chef
- Mother of Doggos (and a teenager)
- Horror Fan
- BSides Jacksonville Coordinator
- Costco Member



Copyright © 2026 Secure Ideas LLC

Blue Team vs Red Team

- **Defense**
  - *Prevention*
  - *Detection*
  - *Mitigation*

- **Offense**
  - *Attacking*
  - *Exploiting*
  - *Evading*



Copyright © 2026 Secure Ideas LLC

Bridging The Gap

- **Purple Team**
  - *Collaborating*
  - *Improving*
  - *Optimizing*



- **Penetration Testers**
  - *Testing*
  - *Reporting*
  - *Validating*



Copyright © 2026 Secure Ideas LLC

Hacker Toolkit



Kali Linux	Metasploit	Burp Suite
Nessus	Hashcat	Nmap
NetExec	Bloodhound	Eyewitness

Copyright © 2026 Secure Ideas LLC

Hacker Toolkit











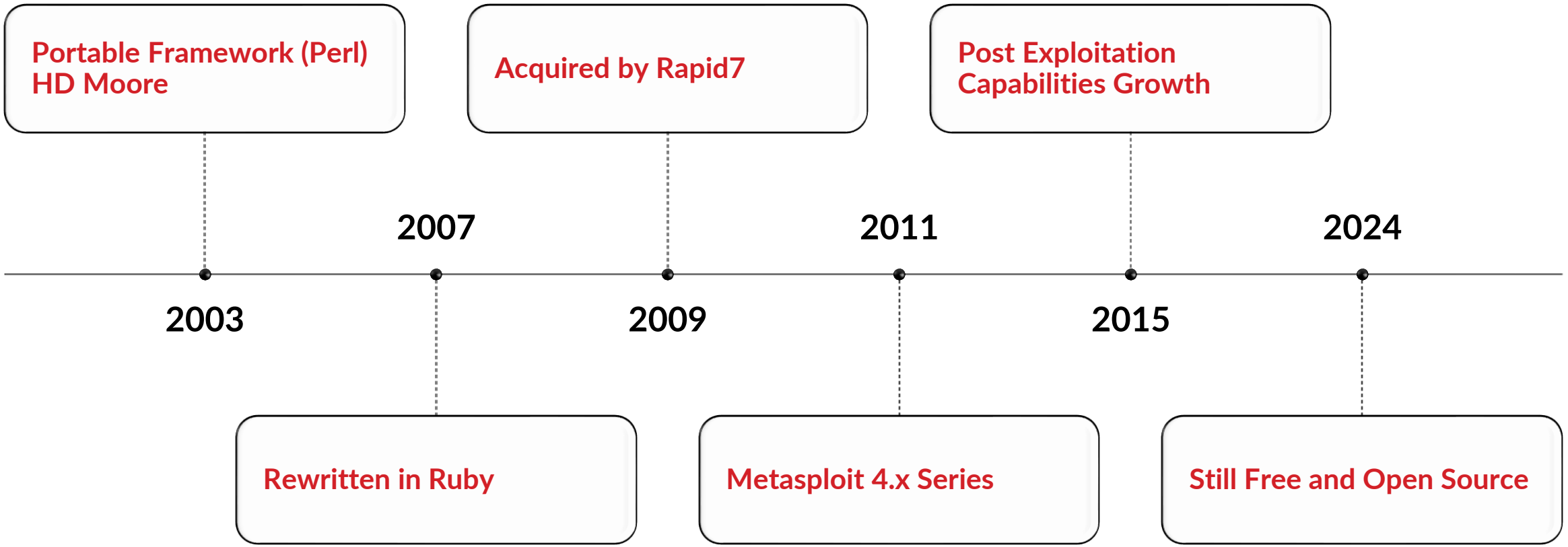
NetExec





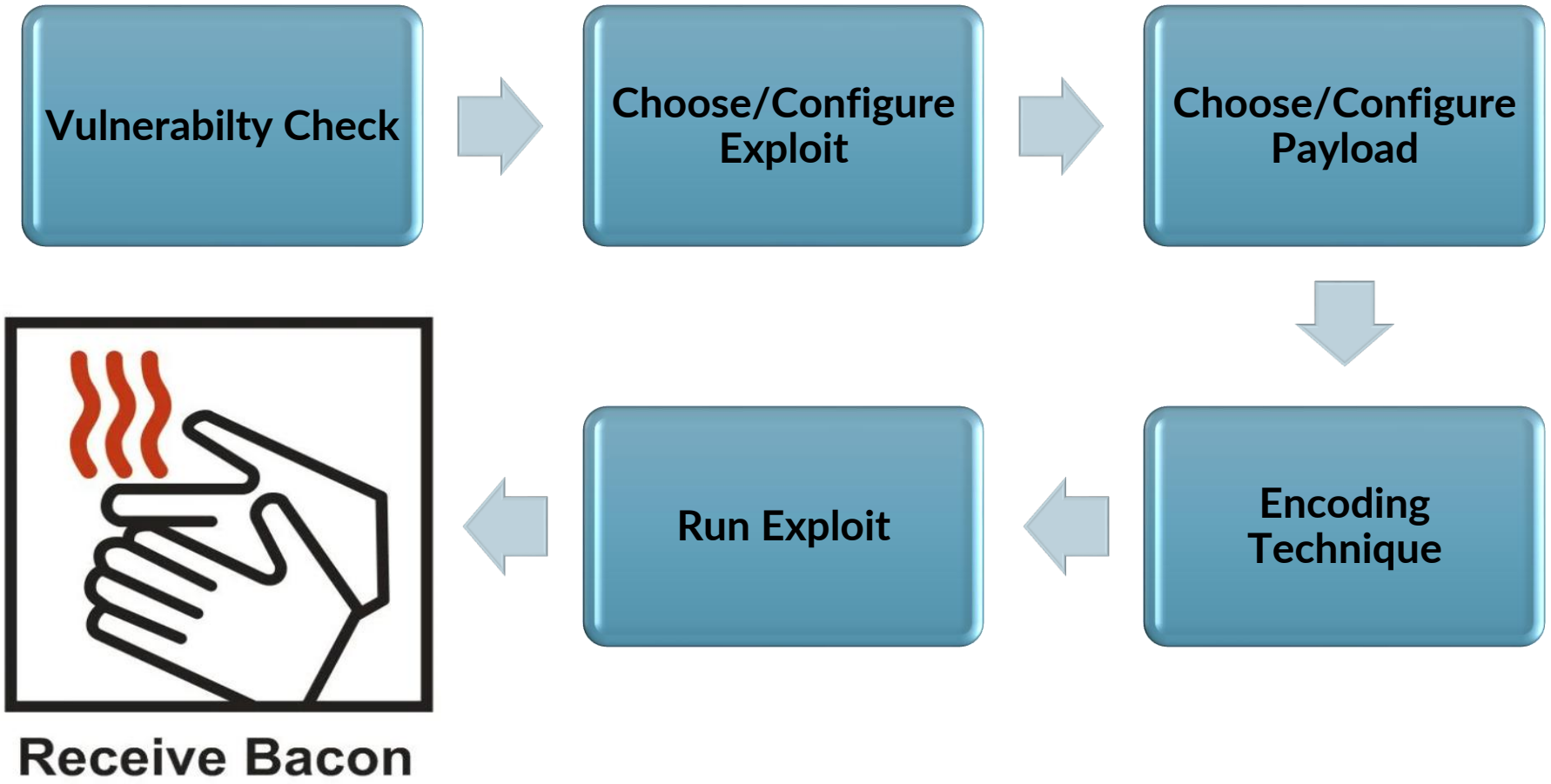
Copyright © 2026 Secure Ideas LLC

New Hack, Who Dis?

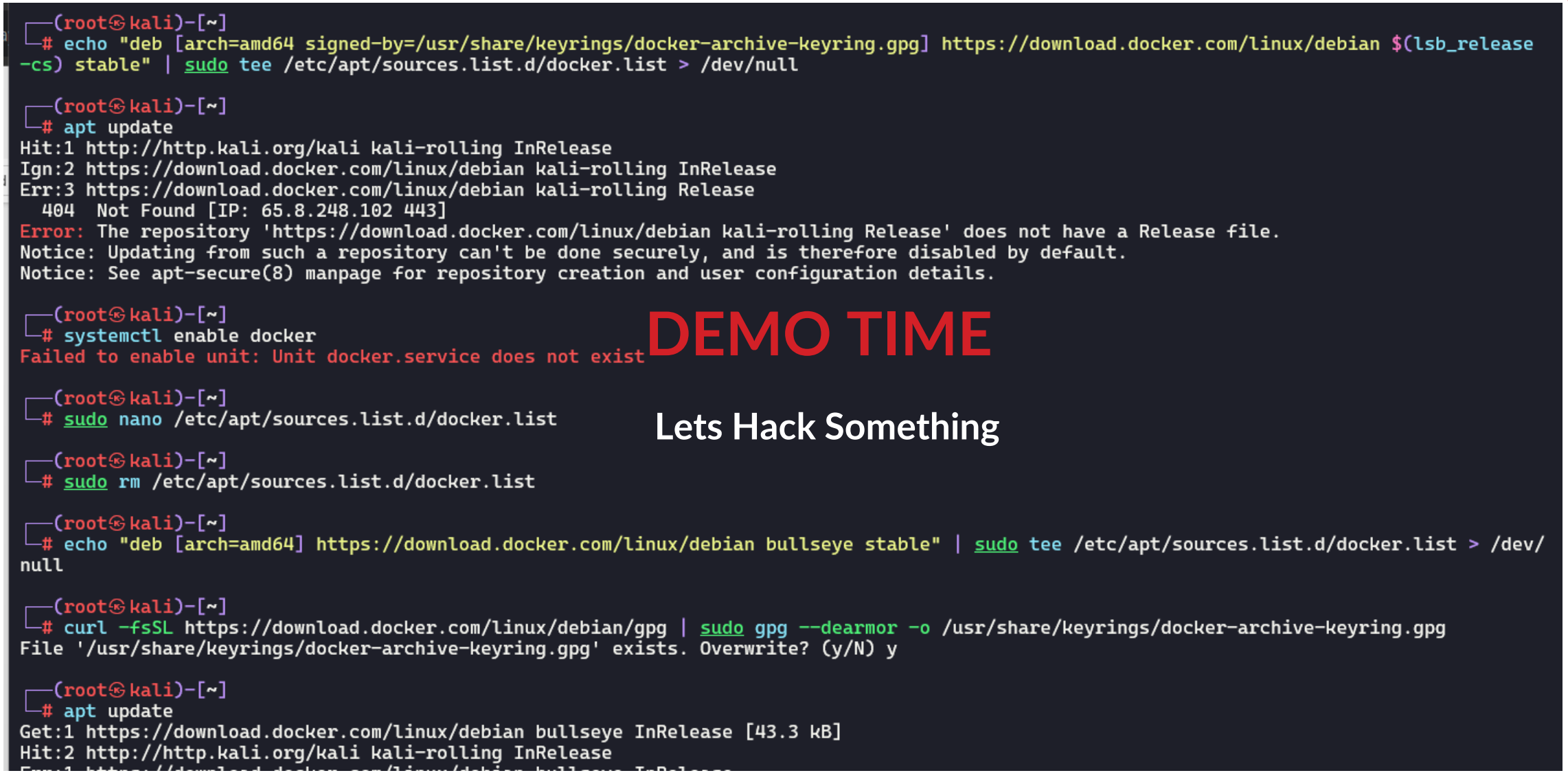


Copyright © 2026 Secure Ideas LLC

Metasploit Framework



Copyright © 2026 Secure Ideas LLC



DEMO TIME

Lets Hack Something

Copyright © 2026 Secure Ideas LLC

Evasion Techniques

- HTTPS
- SVG Smuggling
- Evading EDR

LockBit 3.0 Ransomware Silently Disables EDR Using TDSSKiller

- Malware Cleansing (Virtest)
- Changing Device Data
- Constant Tweaking



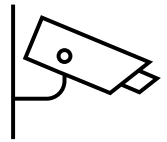
Copyright © 2026 Secure Ideas LLC



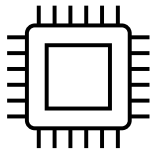
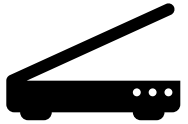
Defend, Detect, Deter

Physical





Technical

Administrative





Knock, Knock, Who's There???

IDS



IPS



Copyright © 2026 Secure Ideas LLC



Strategic Maneuvering

- Be Proactive
- Patch Management
- Password Management
- Configuration Management
- User Training
- Logging
- Threat Monitoring
- EDR
  - Monitoring
  - Detection
  - Response
  - Data Collection
  - Automation (quarantine, blocking)

Cyber Threats in Healthcare

Patient Records

- Personal Data
- Financial Data
- Medical Data

Biggest Threats

- Data Breaches
- Ransomware
- Patient Safety

Mitigations

- Security Awareness Training
- Network Segmentation
- Data Encryption
- Patch Management
- Incident Response Plan



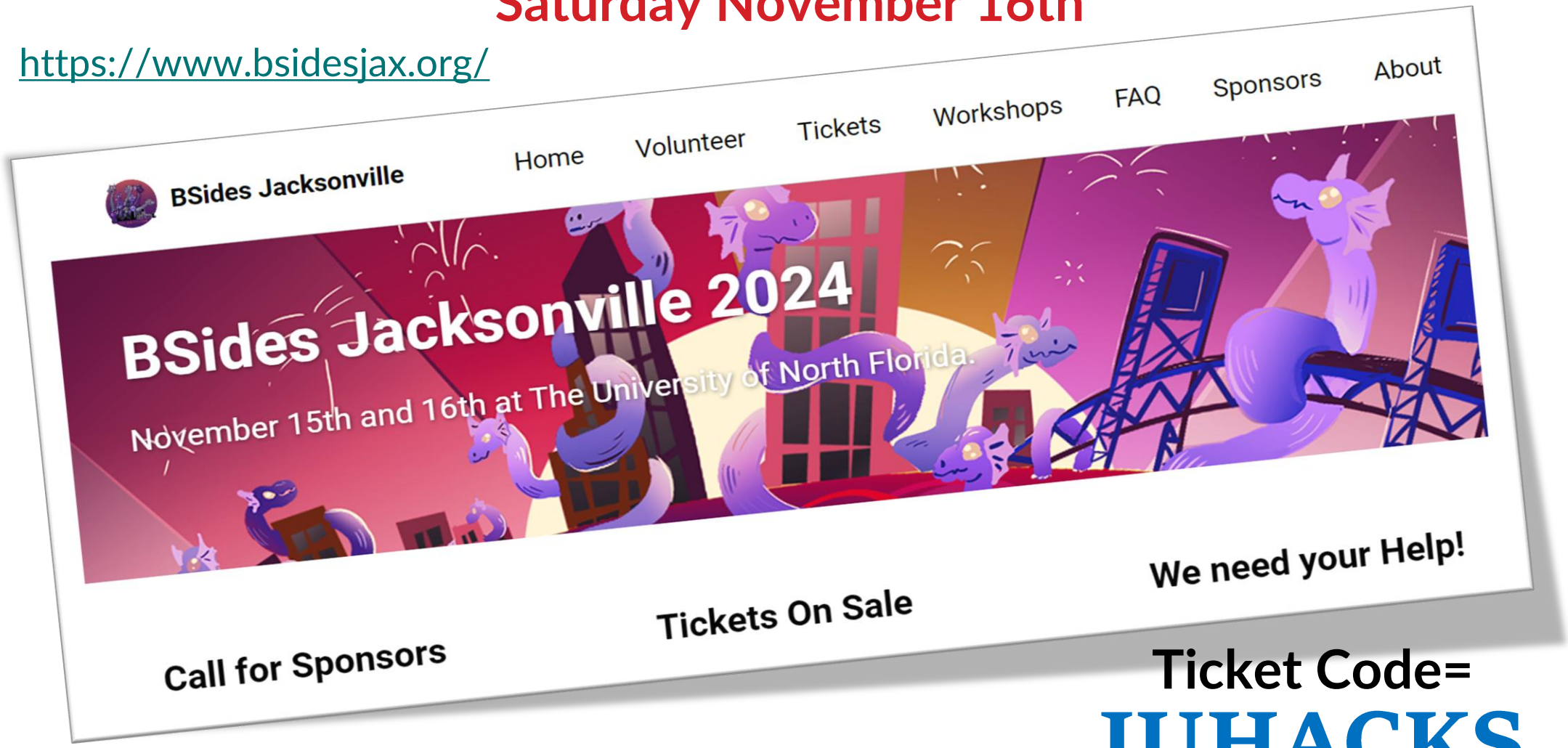
Copyright © 2026 Secure Ideas LLC



Questions?

BSides Jax Conference
Saturday November 16th

https://www.bsidesjax.org/



Ticket Code=

JUHACKS

Copyright © 2026 Secure Ideas LLC