RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: LAW-T08

DHS Hackers and the Lawyers Who Advise Them

MODERATOR: **Gabriel Taran**
Assistant General Counsel, Cybersecurity – DHS Office of General Counsel (OGC)

PANELISTS:

From the Cybersecurity and Infrastructure Security Agency (CISA)'s National Cybersecurity Assessments and Technical Services (NCATS) Team

Rob Karas
NCATS Director

Kelly Thiele
NCATS Program Lead: Phishing Campaign Assessments

Jason Hill
NCATS Chief: Red Team Assessments

From DHS's Office of General Counsel

Matt Slowik
Attorney-Advisor Cybersecurity

CISA: Cybersecurity and Infrastructure Security Agency

- *Previously*: The National Protection and Programs Directorate
- *Newly Created*: Cybersecurity and Infrastructure Security Agency

CISA
CYBER+INFRASTRUCTURE

Defend Today,

Secure Tomorrow

Nota Bene: "CISA" has also been used to reference the Cybersecurity Information Sharing Act of 2015, now informally called "**CISA 2015**"

How CISA is Helping Federal & Non-Federal Entities

- Vulnerability Scanning
- Incident Response
- Automated Indicator Sharing
- Architecture Review
- Hunt
- Self Assessment
- Risk and Vulnerability Assessments
- Red Team Assessments
- Phishing Campaign Assessments

Assessment Goals

- Improve policy makers ability to make informed, risk-based decisions
- Identify and eliminate remote attack paths prior to their exploitation by malicious actors;
- Champion and promote data-driven standards, policies, guidelines and capabilities
- Drive effective cybersecurity risk mitigation strategies

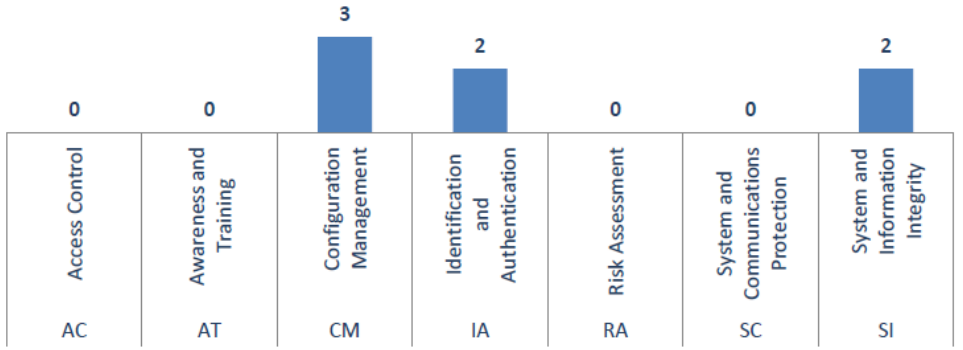


Figure 4: Most Frequently Cited NIST Controls

Recommendations	Remediation Time Table	Finding ID
Reset administrative credentials; ensure default passwords have been changed; and implement secure password complexity, reuse, and storage requirements.	1-6 months	1
Implement stricter access control for administrative interfaces, error logs, and sensitive data.	6-18 months	2
Implement appropriate application and operating system hardening measures, and change, remove, or deactivate all default credentials.	6-18 months	2, 3
Review insecure configuration options for devices. Ensure default passwords have been changed and verify that appropriate hardening measures have been implemented across the environment.	6-18 months	4

Figure 7: Prioritized Remediation Recommendations

Detailed Findings

ID	Finding	Severity	Affected System	Service	Location
3	Exposed Administrative Interface	Medium	172.20.20.49	Penetration Testing	Internal

Description

An exposed administrative interface can enable an unauthorized user to access management and administrative functions of the device or application. This type of access is typically restricted and usually does not include additional layers of access control. An attacker can conduct a brute force attack against an administrative interface that places no restrictions on login attempts.

The affected system has an exposed interface with no local authentication, granting administrative access to any user.

Recommended Mitigation

Properly restrict access to management and configuration interfaces and other potentially sensitive files on remotely accessible web servers, applications, and services.

Implement some form of authentication.

Relevant Screenshot

This screenshot shows the admin interface with no local authentication enabled.

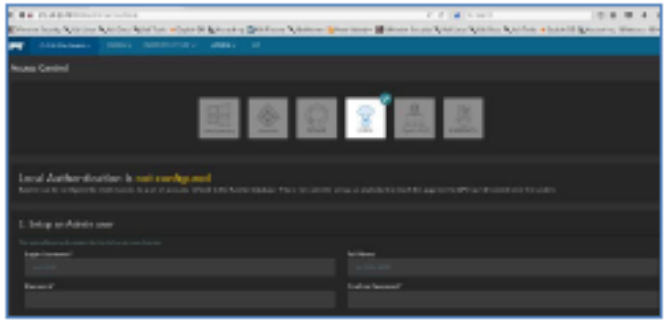


Figure 12: Rancher Local Administrative Access

Security Reference (FCRM, NIST, etc.)

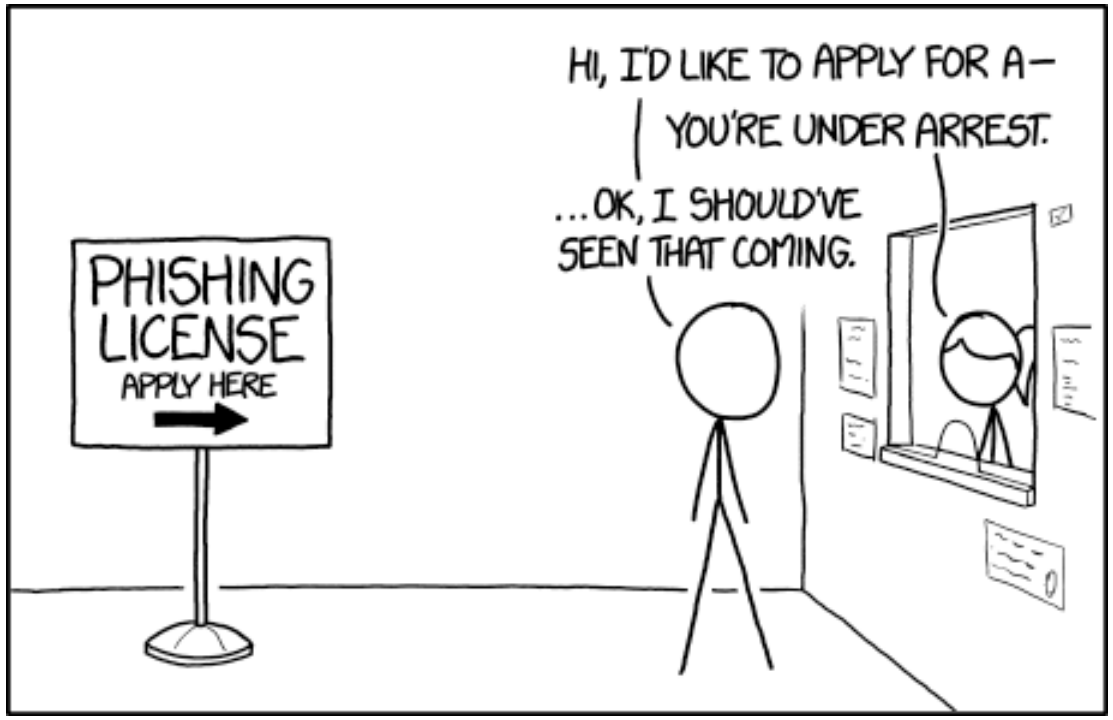
NIST 800-53: CM-6; NIST Cybersecurity Framework: ID.AM-4, PR.AC-3, PR.PT-3; NCATS-ID: 8

Cybersecurity Implicates Many Areas of Law

- **Criminal Law**
  - 18 U.S.C. § 1030 - Computer Fraud and Abuse Act
    - Accessing a computer "without authorization or exceeding authorized access"
  - 18 U.S.C. § 2511 –Wiretap Act
- **Torts and Contract Law:** What constitutes a "protected computer"?
- **Constitutional Law**: primarily the Fourth Amendment
- **Corporate/Employment Law**: Get Phished ⇨ Adverse Employee Action?
- **State Data Breach Law**: Pen Tester exposure to sensitive data
- **Cyber Info Sharing**: Cyber Info Sharing Act of 2015 and data protections

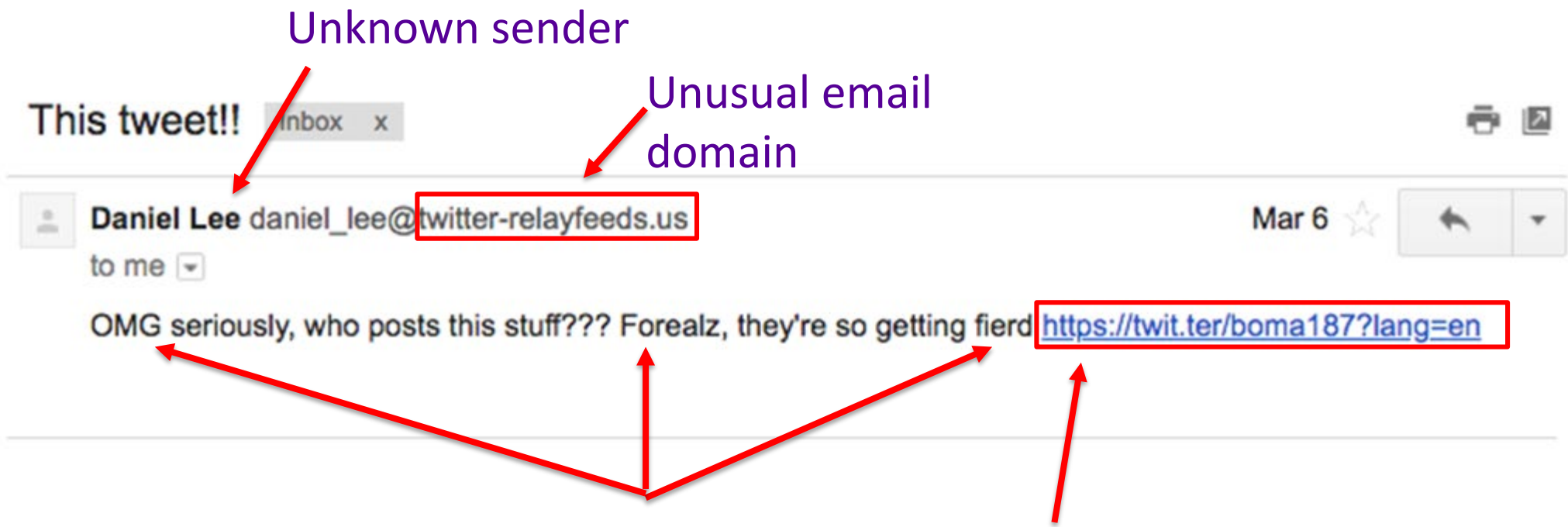
We use a **Rules of Engagement** (RoE) document to address these issues.

Phishing Campaign Assessment



http://xkcd.com/1694/

Phishing Campaign Assessment



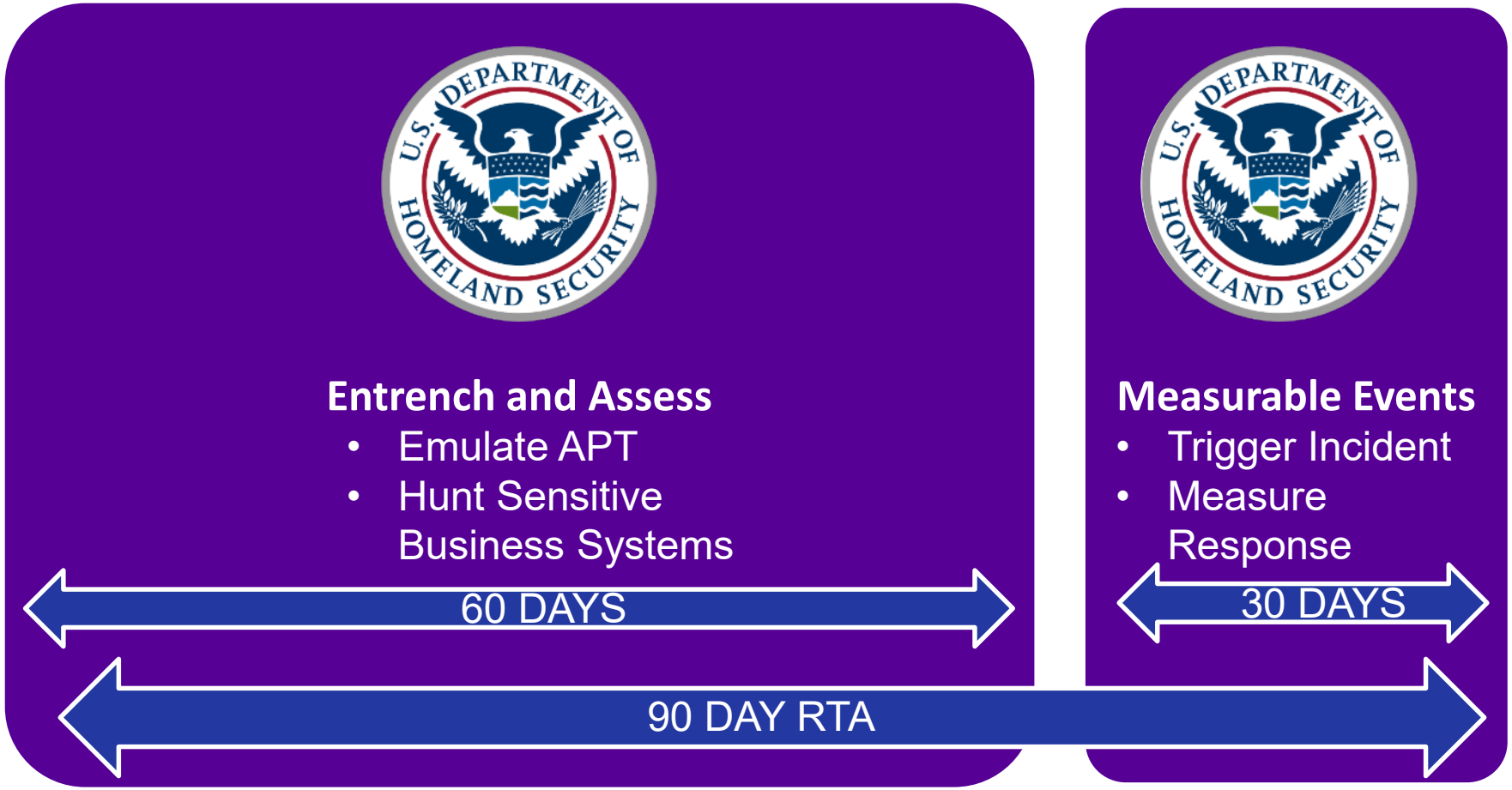
Non-work related topic, informal language, and misspellings are out of place for most office communications.

Hovering over link would show underlying URL to be http://mail.[ncats-domain].tld/tweet?=%TOKEN%

Phishing Legal Issues

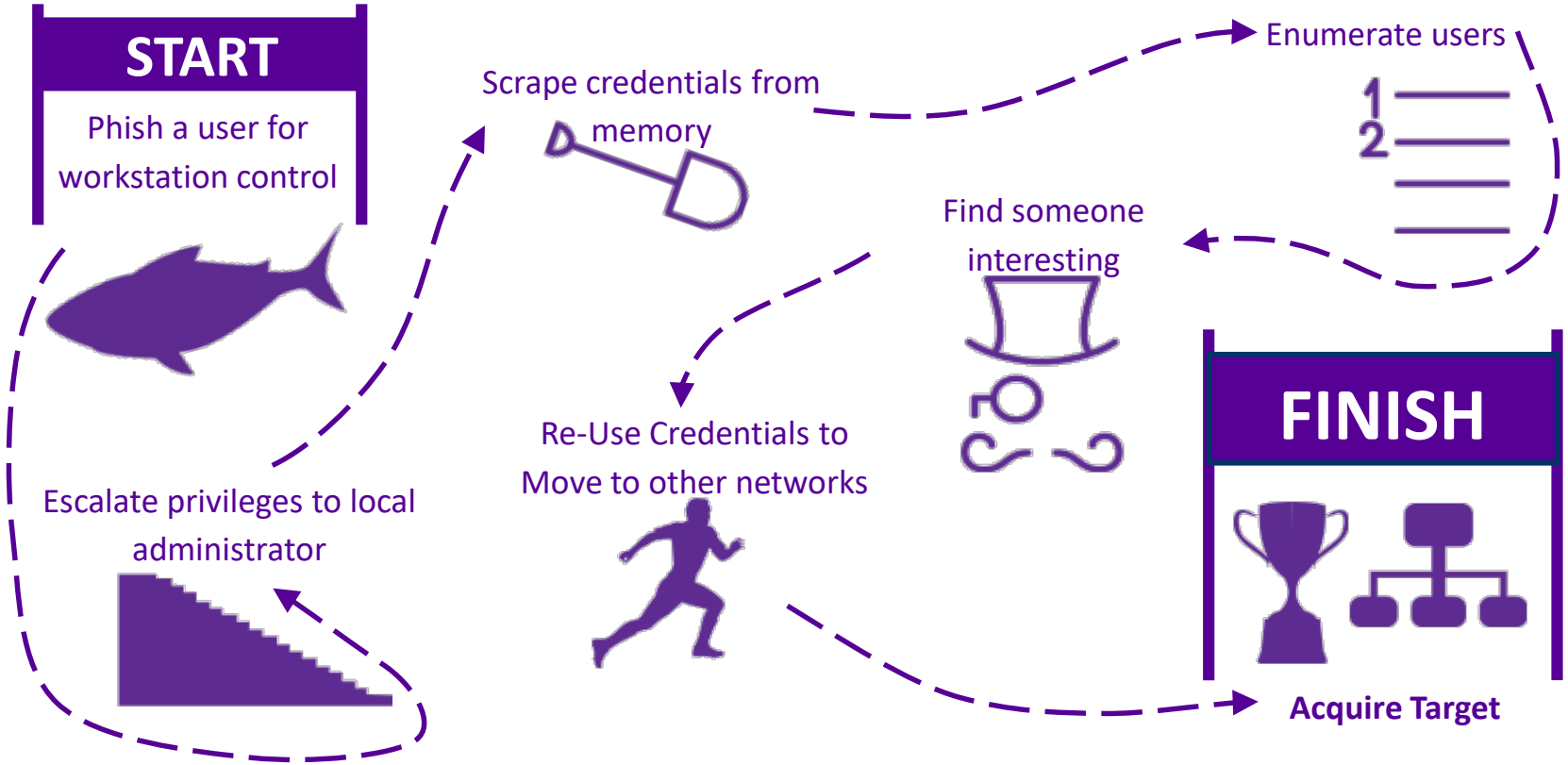
- IP issues
  - Use of agency seal
  - Customer marks in phishing emails
- Adverse actions against phished employees

Red Team Assessment



Phishing Campaign Assessment

- From Phish to Finish

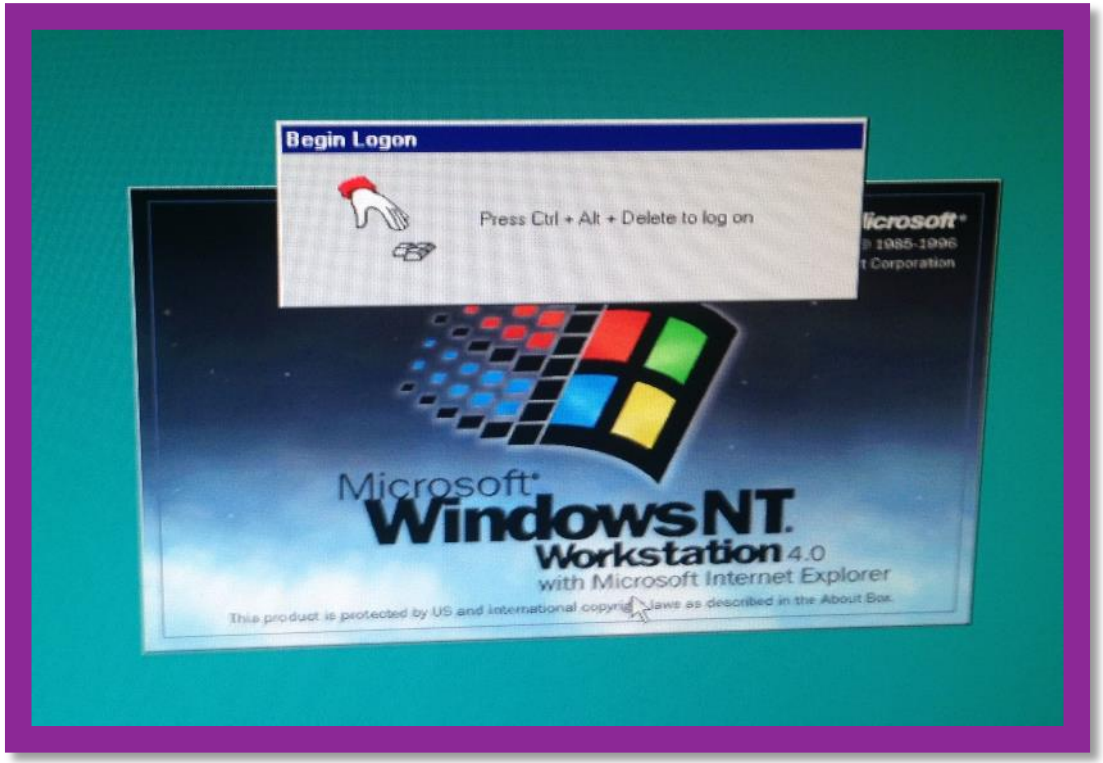


Red Team Assessment Legal Issues

- Legal Authorization
  - Use of Payloads
  - Pivots to other systems
  - 3rd party Cloud-providers
- Liability and scope of Customer/User consent in Rules of Engagement
  - Criminal and Constitutional Law Issues
- Legal Authorization
  - 3rd party and cloud systems and environments
- Data Sensitivity and State Breach Laws
- Data Protections in Rules of Engagement

Emerging Issues

- Red Teaming on Mobile devices and apps
- IoT
- Shared Resources: Cloud
- “Long-Game” Phishing
- Physical Security
- Industrial Control Systems



Next steps

- Document and understand your network and IP space
- Determine date of your last Risk and Vulnerability Assessment
- Examine any contracts with 3rd party of Cloud Service providers
- Explore any potential issues with other appropriate legal SMEs
  - Employment law, contract law

Contact Info and Q&A

- Questions? NCATS@hq.dhs.gov
- Q&A in time remaining