



CIS Top 20 #20

Penetration Tests and Red Team Exercises

Lisa Niles: CISSP, Director of Solutions Integration



CIS Top 20 Critical Security Controls

CSC # 20

Test the overall strength of an organization's defenses (the technology, the processes, and the people) by simulating the objectives and actions of an attacker.



CIS Top 20 Critical Security Controls

Why Is This Control Critical?

Basic

1 Inventory and Control of Hardware Assets

2 Inventory and Control of Software Assets

3 Continuous Vulnerability Management

4 Controlled Use of Administrative Privileges

5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

6 Maintenance, Monitoring and Analysis of Audit Logs

Foundational

7 Email and Web Browser Protections

8 Malware Defenses

9 Limitation and Control of Network Ports, Protocols, and Services

10 Data Recovery Capabilities

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

12 Boundary Defense

13 Data Protection

14 Controlled Access Based on the Need to Know

15 Wireless Access Control

16 Account Monitoring and Control

Organizational

17 Implement a Security Awareness and Training Program

18 Application Software Security

19 Incident Response and Management

20 Penetration Tests and Red Team Exercises

Understanding
the
Control types

ICS Cyber Security Control Framework

Procedural Security Controls

Operational
Security Controls

Technological
Security Controls

Physical Security
Controls

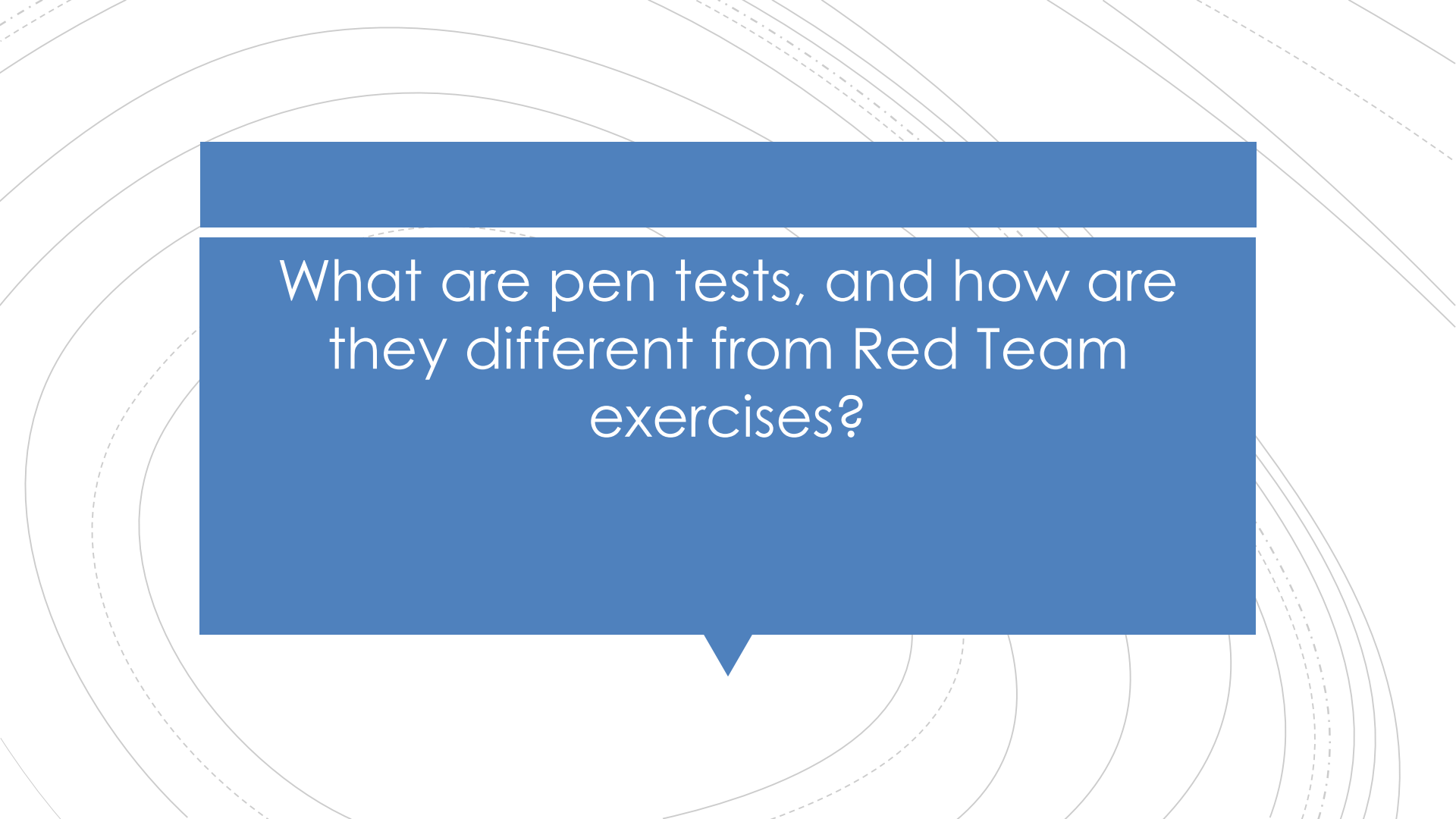
Regulatory &
Compliance
Controls

CIS Top 20 Critical Security Controls

- 1ST AND FOREMOST
- Penetration testing and Red Teaming only provide significant value when basic defensive measures have already been put into place, and when they are performed as part of a comprehensive, ongoing program of security management and improvement.

CIS Top 20 Critical Security Controls

This is much more than just vulnerability scanning using [Nessus](#) or [OpenVAS](#). This includes attempting to exploit the vulnerabilities found by these systems.

The background features several concentric circles, some solid and some dashed, in a light gray color. A large blue speech bubble is centered on the page, containing the text. The speech bubble has a white border and a small white triangle pointing downwards at its bottom center.

What are pen tests, and how are they different from Red Team exercises?

The background features several concentric circles, some solid and some dashed, in a light gray color. A large blue speech bubble is centered on the page, containing the text 'Planning for a pen test'.

Planning for a pen test

The background features several concentric circles of varying radii, some solid and some dashed, creating a ripple effect. A large blue callout box is centered on the page, containing the text "Other considerations".

Other considerations



CIS Top 20 Critical Security Controls

- **Key Takeaways from Control 20**
 - Rely on the previous controls.
 - Where's the remediation?



CIS Top 20 Critical Security Controls

- Many organizations fail to perform pen tests for many reasons, mainly out of fear

CIS Top 20 Critical Security Controls

How to Get Started

- Step 1. Gap Assessment.
2. Implementation Roadmap
3. Implement the First Phase of Controls
4. Integrate Controls into Operations
5. Report and Manage Progress





CIS Top 20
Critical
Security
Controls
CSC # 18

- [Sample Gap questions](#)
 1. Has the organization documented a detailed standard for penetration testing (including the how and when aspects)?
 2. Are only appropriate users authorized to perform penetration tests on the organization's systems?
 3. Are penetration tests being performed on a regular basis from both inside and outside of the organization's network?
 4. Has a metric or scoring system been implemented for penetration testing to help prioritize remediation efforts?
 5. Are the results of penetration tests integrated into the organization's overall risk management program?

CIS Top 20 Critical Security Controls

20.1	Conduct regular external and internal penetration tests to identify vulnerabilities and attack vectors that can be used to exploit enterprise systems successfully. Penetration testing should occur from outside the network perimeter (i.e., the Internet or wireless frequencies around an organization) as well as from within its boundaries (i.e., on the internal network) to simulate both outsider and insider attacks.
20.2	Any user or system accounts used to perform penetration testing should be controlled and monitored to make sure they are only being used for legitimate purposes, and are removed or restored to normal function after testing is over.
20.3	Perform periodic Red Team exercises to test organizational readiness to identify and stop attacks or to respond quickly and effectively.
20.4	Include tests for the presence of unprotected system information and artifacts that would be useful to attackers, including network diagrams, configuration files, older penetration test reports, e-mails or documents containing passwords or other information critical to system operation.
20.5	Plan clear goals of the penetration test itself with blended attacks in mind, identifying the goal machine or target asset. Many APT-style attacks deploy multiple vectors—often social engineering combined with web or network exploitation. Red Team manual or automated testing that captures pivoted and multi-vector attacks offers a more realistic assessment of security posture and risk to critical assets.
20.6	Use vulnerability scanning and penetration testing tools in concert. The results of vulnerability scanning assessments should be used as a starting point to guide and focus penetration testing efforts.
20.7	Whenever possible, ensure that Red Teams results are documented using open, machine-readable standards (e.g., SCAP). Devise a scoring method for determining the results of Red Team exercises so that results can be compared over time.
20.8	Create a test bed that mimics a production environment for specific penetration tests and Red Team attacks against elements that are not typically tested in production, such as attacks against supervisory control and data acquisition and other control systems.

CIS Top 20 Critical Security Controls

- *20-1* - Conduct regular external and internal penetration tests to identify vulnerabilities and attack vectors that can be used to exploit enterprise systems successfully. Penetration testing should occur from outside the network perimeter (i.e., the Internet or wireless frequencies around an organization) as well as from within its boundaries (i.e., on the internal network) to simulate both outsider and insider attacks.
- **Free Tools**
- Free Tools
 - [Backbox Linux](#) - Pentesting distro built on Ubuntu. DOES NOT REQUIRE RUNNING AS ROOT!
 - [Kali Linux](#) – Kind of the defacto pentesting distro out there. Most schools teach from this distro in security classes. Requires you to run as root all the time.
 - [PenTesters Framework \(PTF\)](#) - Framework of tools that can be installed and updated on any distro (currently only limited to Kali, Debian, and Ubuntu)
- **Commercial Tools/Services**
 - SynerComm

CIS Top 20 Critical Security Controls

- *20-2* - Any user or system accounts used to perform penetration testing should be controlled and monitored to make sure they are only being used for legitimate purposes, and are removed or restored to normal function after testing is over.
- Tools
 - This is just common sense

CIS Top 20 Critical Security Controls

- 20-3 - Perform periodic Red Team exercises to test organizational readiness to identify and stop attacks or to respond quickly and effectively.

CIS Top 20 Critical Security Controls

- *20-4* - Include tests for the presence of unprotected system information and artifacts that would be useful to attackers, including network diagrams, configuration files, older penetration test reports, e-mails or documents containing passwords or other information critical to system operation.
- Tools
 - This is more procedure than tools.

CIS Top 20 Critical Security Controls

- 20-5 - Plan clear goals of the penetration test itself with blended attacks in mind, identifying the goal machine or target asset. Many APT-style attacks deploy multiple vectors—often social engineering combined with web or network exploitation. Red Team manual or automated testing that captures pivoted and multi-vector attacks offers a more realistic assessment of security posture and risk to critical assets.
 - Again, libraries are written on this topic. I could list tools here, but it would be a million lines long, and still people would be offended because I left off some obscure DNS fuzzer that they enjoy using... HOWEVER, there is one tool I can absolutely recommend...
 - [Penetration Testing Framework](#) - a treasure trove of information.

CIS Top 20 Critical Security Controls

- 20-6 - Use vulnerability scanning and penetration testing tools in concert. The results of vulnerability scanning assessments should be used as a starting point to guide and focus penetration testing efforts.

CIS Top 20 Critical Security Controls

- 20-7 - Wherever possible, ensure that Red Teams results are documented using open, machine-readable standards (e.g., SCAP). Devise a scoring method for determining the results of Red Team exercises so that results can be compared over time.
- Free Tools
 - This might help:
 - [DREAD Scoring Template](#) - I have attached a template that helps me organize vulnerabilities found based on criticality. This helps me focus my efforts where they are needed most.

CIS Top 20 Critical Security Controls

- 20-8 - Create a test bed that mimics a production environment for specific penetration tests and Red Team attacks against elements that are not typically tested in production, such as attacks against supervisory control and data acquisition and other control systems.
 - Because, you know...having your Red Team take down your main website in the middle of the day is never a good thing.

CIS Top 20 Critical Security Controls

- 20-x – Additional things...
- CONTROL AND MONITOR ACCOUNTS ASSOCIATED WITH PENETRATION TESTING
 - **Description:** Any use or system accounts used to perform penetration testing should be controlled and monitored to make sure they are only being used for legitimate purposes and are removed or restored to normal function after testing is over.
 - **Notes:** This is part of the clean-up that happens after each engagement by the red team.

CIS Top 20 Critical Security Controls



• You are invited!!

- SynerComm IT Summit
- October 22-23rd
- Milwaukee @ Potawatomi
- Enabling Secure Digital Transformation
- [Registration](#)

CIS Top 20 Critical Security Controls

Thank you for Attending.

Hope you can join us for the Complete CIS Top 20 CSC

Tuesday October 30th

CIC CSC # 15

Wireless Access Control