Windows Security – Scoring, Scenario, Presentation

Rick Payne CISSP, RHCE, Security+, RHCSA

Prepared by: Rick Payne

Prepared for: The Cybersecurity Community

LinkedIn: <https://www.linkedin.com/in/rick-payne-cissp-rhce-0b953089/>

Twitter: <https://twitter.com/RickPayne929>

Email: [grep.rickp@gmail.com](mailto:grep.rickp@gmail.com)

Table of Contents

[1. Preparation 3](#_Toc517033017)

[2. CyberPatriot Scoring Engine - Installation 3](#_Toc517033018)

[3. CyberPatriot Scoring Engine - Configuration 4](#_Toc517033019)

[4. CyberPatriot Scoring Engine - Score Report 6](#_Toc517033020)

[5. Competition Scenario 7](#_Toc517033021)

[6. PowerPoint Presentation 9](#_Toc517033022)

**Background**: In 2018, one can no longer dispute the importance of cybersecurity. Successful organizations now recognize it as a business-critical function and are looking for experts to lead cybersecurity initiatives. This rising demand has many predicting over 3M open jobs by 2021! Youth cyber education programs, such as CyberPatriot and CyberCamp, focus on creating that talent at the high school level. Since 2013, I’ve been teaching and mentoring cybersecurity through these great programs. They expose our youth to important concepts using vulnerable, virtual images. I’m proud to continue this mission Summer 2018 at Florida State College of Jacksonville for 7th graders and at UCF for 9-12! The lesson is a broad Windows security course based on common denominator concepts from nearly every security framework. Looking to protect your home computer? Teach our youth? Start in cybersecurity? Get some hands-on experience? This overview will walk you through image configuration, scoring set up and testing, an example scenario, and the slides used to teach the material.

CyberPatriot: <https://www.uscyberpatriot.org/>

CyberCamp FCA: <http://www.floridacyberalliance.org/cybercamp>

CyberCamp UCF 2018: <http://cybercamp.cs.ucf.edu/>

# Preparation

This presentation assumes the reader has a basic to intermediate understanding of computing concepts. The objective is to strategically introduce vulnerabilities into a Windows 7 or 8.1 virtual machine (VM), deliver a hands-on presentation demonstrating relevant security concepts, and then have students remediate the vulnerabilities per requirements defined in the Scenario. The following preparation should be completed and/or considered when executing this content:

* Create a Windows 7 or 8.1 VM. Most schools offer free access to operating system .iso images via Microsoft Developer Network (MSDN) accounts. Once you have the .iso, you can download VMware Player free virtualization software and begin the Windows installation.
* Consider creating an image Snapshot for future lessons/testing.
* Your virtualization infrastructure will determine VM software and delivery options. Will you be sharing a zipped version through an AWS S3 Bucket, where each student will download and run a local copy? Will you be launching and configure AWS EC2 instances? Does your school or business offer other centralized delivery methods?

# CyberPatriot Scoring Engine - Installation

As of June 17, 2018, Scoring Engine Tool v3.0.1 is available from CyberPatriot here: <https://www.uscyberpatriot.org/competition/training-materials/practice-images>

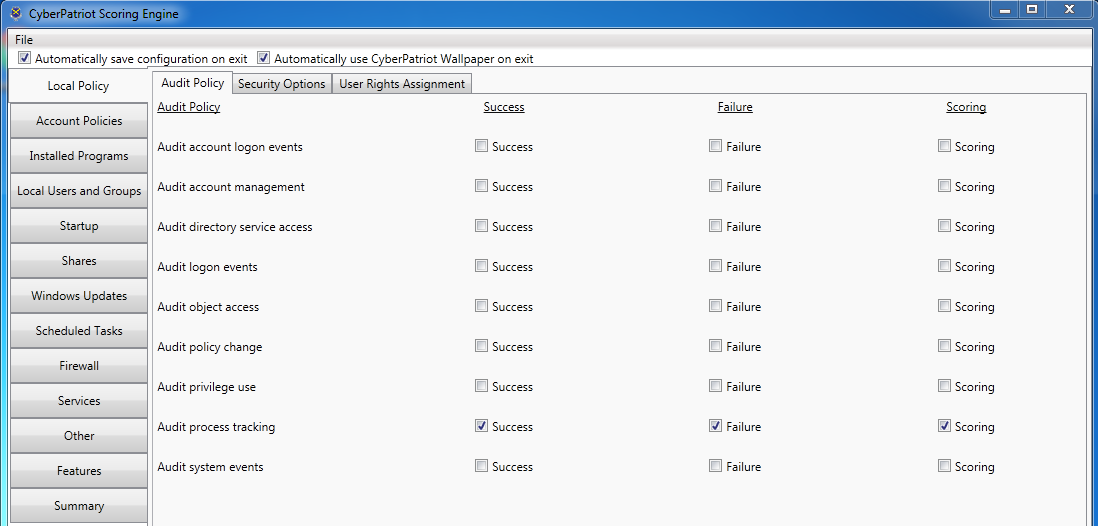
To ensure continued access, you can find it in my GitHub repository here: <https://github.com/rickpayne929/CyberCamp_Windows>

1. Download **Scoring\_Engine\_Tool\_v3.0.1** from either location above.
2. Start your Windows VM and log in.
3. Copy **Scoring\_Engine\_Tool\_v3.0.1** from your host machine to your **VM** **Desktop**. VMware Player with VMware Tools installed allows easy host <-> VM transfers.
4. Click: Start -> Type: Features -> Click: **Programs and Features**
   1. **Uninstall** any previously installed instance. 
   2. Select the default options and **Reboot** when complete.
5. Open the **Scoring\_Engine\_Tool\_v3.0.1** folder -> Run **CyberPatriot+Scoring+Engine+3.0.1.exe** -> Select: All default options.
6. Once the installation is complete, two new icons will be added to the user's Desktop: Coach Configuration Tool and Score Report. 

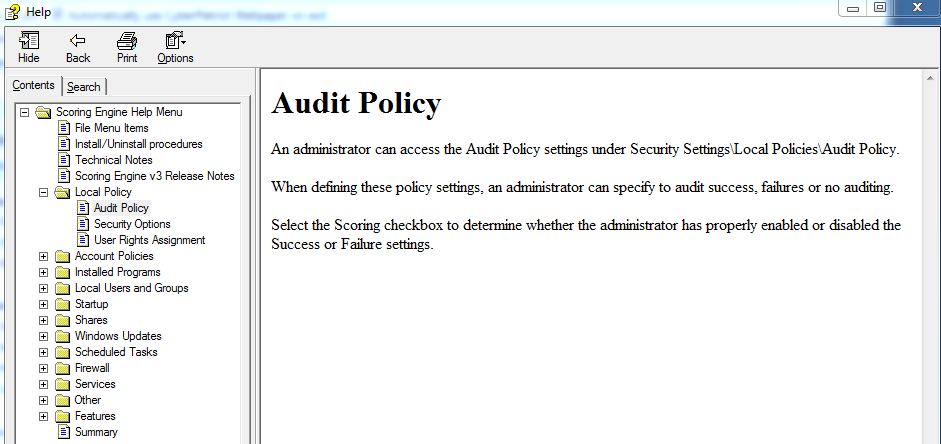
# CyberPatriot Scoring Engine - Configuration

The below options were designed as an introductory lesson. Please tailor your content and lessons per student ability.

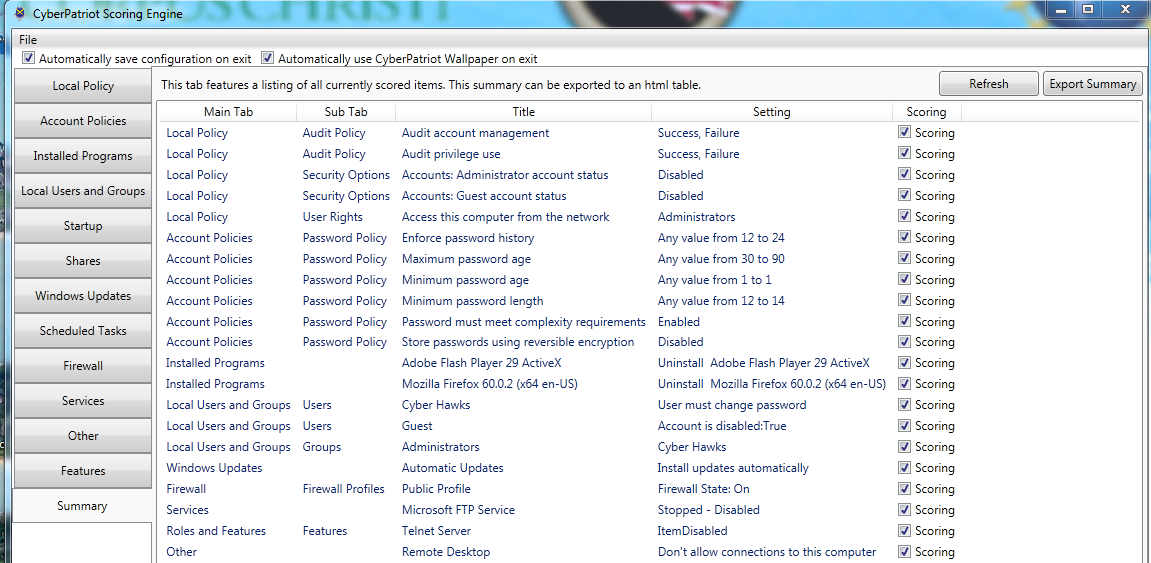
1. Double click the **Coach Configuration Tool** icon  to start configuring settings the Scoring Engine will monitor.



1. For Scoring Help, Open the **Scoring\_Engine\_Tool\_v3.0.1\SEHelpv3** folder -> Run **SEHelp.chm**
   1. Expand the **Scoring Engine Help Menu** to access configuration details on each tab.



1. Here are some example Scoring Configurations used in this lesson:
   1. Group Policy scoring: Security Options, User Rights Assignment, Basic auditing, Password and Account Lockout Policy
      1. Audit Policy: Audit privilege use: Success, Failure
      2. Audit Policy: Audit account management: Success, Failure
      3. SO -> Disabled Guest & Admin account
      4. URA -> Access this computer from the network: Administrators only
      5. PP -> Max age 30-90 days, Min age, 1, History 12-24, Length 12-14, Complexity enabled, Reversible encryption disabled
      6. ALP: Duration 60, Threshold 3, Counter 60
   2. Installed Programs: Remove Adobe Flash and Firefox
   3. Local Users & Groups: Cyber Hawks password change, disable all other users, Administrators Group: Cyber Hawks and <choose a user> only
   4. Folder shares: Delete <choose a share to remove>
   5. Windows updates: Install updates automatically
   6. Public Firewall: On
   7. Services: Microsoft FTP Service: Stopped, Disabled
   8. Files to be removed: <choose a prohibited file to remove>
   9. Features: Telnet server: Disabled
2. Click the **Summary** tab to review your configurations

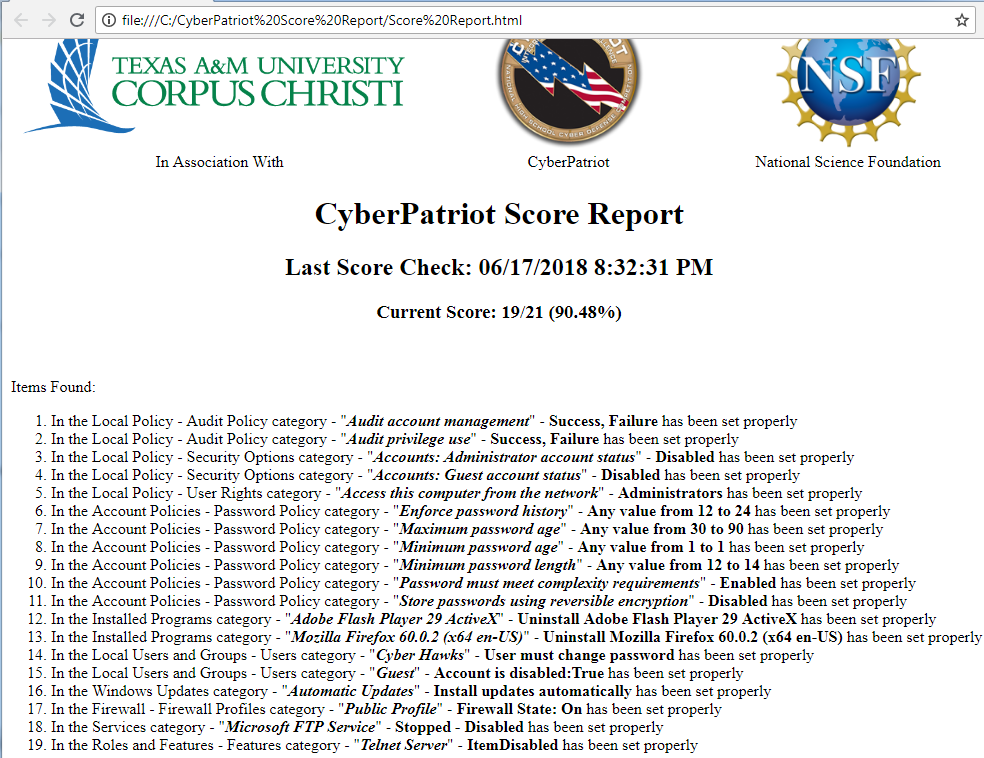


1. Use the **Export Summary** button to generate an .html version to use when reviewing student progress during the Scenario. Located in GitHub, this example was exported as ScoringEngineExport\_2018-06-17\_201346.html.
2. Click: File -> **Save As** to save your current configuration to a .dat file. This can be imported later through File -> Load Saved Configuration. Located in GitHub, this example was saved as ScoringEngineConfiguration\_2018-06-17\_201445.dat.
3. **Note**: Release to Students is the final step and will require reinstallation for changes. Click: File -> **Release to Students** to prepare the image for scoring.

# CyberPatriot Scoring Engine - Score Report

Use the Score Report to test each setting after being finalized.

1. Double click the **Score Report** icon  on the Desktop to review the current score.
2. Step through the exported .html summary list to confirm all options score as expected.



# Competition Scenario

The below scenario was designed as an introductory lesson. Please tailor your content and lessons per student ability.



You are supporting a Department of Defense(DoD) program that requires robust security. This machine must be securely configured to align with DoD, federal, and industry standards such as the Principle of Least Privilege and Least Functionality. To get started, your manager has requested you ensure the below configurations are in place. Also, your predecessor may have been up to no good. Confirm all user accounts match the list below, and ensure the system does not contain prohibited files.

Access Control - Account Management:

-<User> and Cyber Hawks should be the only active users. All others can be disabled.

-<User> and Cyber Hawks should be the only members of the Users and Administrators Groups. All others can be removed.

-Only members of the Administrators group should be able to access this computer from the network

-<User>'s and Cyber Hawks password's should be reset to CyberCamp2018

Access Control - Account Lockout Policy:

-Duration: 60

-Threshold: 3

-Counter reset: 60

Auditing:

-The system should audit account management and privileged events.

Firewalls:

-Domain, Private, and Public firewall should be On.

Identification and Authentication - Password Policy:

-Password history: 24

-Maximum age: 60

-Minimum age: 1

-Minimum length: 14

-Complexity requirements: Enabled

-Reversible encryption: Disabled

Least Functionality - Features:

-The Telnet server feature should be removed.

Least Functionality - Services:

-The FTP service should be Stopped and Disabled.

Least Functionality - Sharing:

-The system should not have any shared folders.

Patching - Application:

-Rather than patching, unnecessary or unused support applications, such as Flash and Firefox, should be removed.

Patching - System:

-The system should be configured to Install updates automatically

Prohibited files:

-The system should not contain any videos such as .avi or .mpeg files.

# PowerPoint Presentation

The lesson is a broad Windows security course based on common denominator concepts from nearly every security framework. Each concept is introduced with an excerpt from an authoritative source, such as a Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG), to help understand why the configuration is required. For example, this text is paraphrased from the Windows 7 STIG “Audit logs are necessary to provide a trail of evidence to help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred as well as detecting attacks.” to tie the concept and configuration together.

Here is the course overview:

* Access Control - Account Management
* Access Control - Account Lockout Policy
* Auditing
* Firewall
* Identification and Authentication - Password Policy
* Least Functionality – Features, Services, Sharing
* Patching – Application, System
* Prohibited file identification

