CYBER NOTES

Share Drive - \\10.2.1.217 Csc password1

Never run 2 malware scanners at the same time.

<https://downloads.cisecurity.org/#/>

Checklist:

gpupdate /force

C:\Windows\System32\GroupPolicy

Backup Admin

Computer Management:

1. Task Scheduler
   1. Check for scheduled scripts
2. Event Viewer
   1. Can check for audit trips and previous events
3. Shared Folders
   1. Check for only main 3 shares (ADMIN$, C$, IPC$)
4. Local Users and Groups
   1. Enabled/Disabled users that should/shouldn’t be
   2. Check all users are in user group
   3. Check administrator group for proper admins and users that don’t belong
5. Services
   1. Scroll down

Group Policy (Computer Configuration)

Windows Settings

1. Scripts
   1. Check Startup
   2. Check Shutdown
   3. Check Logon
   4. Check Logout
2. Security Settings
   1. Account Policy
      1. Password Policy
         1. History = 5
         2. Max Age = 90
         3. Min Age = 30
         4. Min Length = 14
         5. Complexity Requirements = True
         6. Reversible encryption = False
      2. Account Lockout Policy
         1. Lockout Threshold = 5 (Yes to default others)
   2. Local Policies
      1. Audit Policy
         1. All S/F
      2. User Rights Assignment
         1. Many Things here, Use Benchmark

https://downloads.cisecurity.org/#/

* + 1. Security Options
       1. Many things here, main 2 below
       2. Interactive Logon: Do not require CTRL Alt del = Disabled
       3. Interactive Logon: Do not display last user name = Enabled
  1. Windows Firewall
     1. All Profiles:
        1. Firewall State = On (Recommended)
        2. Inbound connections = Block (default)
        3. Outbound = Allow (default)

Administrative Templates

1. All Settings has many things, so does windows components. Just use benchmarks or search for settings in response to specific issues

Group Policy (User Configuration)

1. Windows Settings
   1. Scripts
      1. Check for Logon
      2. Check for Logon
2. Administrative Templates
   1. All Settings has many things, so does windows components. Just use benchmarks or search for settings in response to specific issues

**Registry**

Run + RunOnce

-If no internet, check DNS address

-Check for Scripts

-check admins, not admins, and disabled/not accounts - computer manager

-password policy

-applications

-check windows firewall and services

-Event Viewer (if off turn on in services),

-Task Scheduler (taskschd. msc)

-Scheduled Events

-Task Manager - ALL TABS

-Updates- Windows/Firefox/Chrome/whatever else-

-CCleaner exe in downloads for no reason.

-Defender being stupid

-Services

-Finding nonwork files (\*.file-extension)

-CNTRL-DEL

-Share Permissions

-Firefox - HTML ONLY, STRICT, NO POPUPS, BLOCK KNOWN MALWARE SITES, REMOVE EXTENSIONS

- Server settings ensure newest version

-UAC Configuration

Services - Good: DNS, DHCP, BITS, Win Update, WMI, Firewall, Event Log  
Bad: Telnet, Telephony, Remote Registry, WebClient, FTP, Bluetooth Discovery, SSDP, Plug + Play,

IIS ----------------------------------------------------------------------------------------------------------

Inetpub > wwwroot

Port 80 (go figure) for http and 443 for https

IIS Manager

Create Certificate (Server Certificates)

Sites, Bindings, Add, bind to Https, remove http binding

Authentication: Disable both

Directory Browsing: Disable TOP RIGHT

Error Pages:House error reports

Logging: Log event destination (Both), Change Log Directory, APPLY BUTTON TOP RIGHT

Request Filtering: Deny(exe,bat,php,psl,py,json,js,java), Edit Feature Settings(Allow Unlisted Verbs, remove all else, Numbers are 30000000, 4096, 2048)

Configuration Editor:Sumthin

Feature Delegation: Anonymous(Read Only), Directory Browsing(Read Only), SSL Settings(Read Only)

Double check settings in individual site

SSL settings in individual site: Require SSL, require certificate, APPLY TOP RIGHT CORNER

—-----------------------------------------------------------------------------------------------------------

Task scheduler (Computer Management) + Gpedit

Active tasks will show all running scripts / tasks

Shutdown -a to abort

Shutdown -s to shutdown

Shutdown -f to force

Disable bad drivers on startup

--------------------------------------------------------------------------------------------------------------

Administrator removed from administrators

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Certutil to find hashes:

certutil -hashfile Example.txt MD5

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Filezilla Server

Server listeners

* Add
  + Loopback address
    - port : 21

Protocols settings

* Autoban
  + Ban IP address after 5 logins in 10 seconds
* Timeouts
  + Login: 20
  + Activity: 60

FTP over TLS

* Min allowed TLS version: v1.3 (or newest)
* TLS certificate
  + Use a self-signed X.509 certificate
    - Generate new
      * Hostnames: localhost
      * Distinguished name: (blank)

Logging

* Logging level
  + 5
* File rotation
  + Enabled
  + Rotate log file when its size reaches the maximum size
* Log files
  + 5

Administration:

* Connection
  + Local listening: 14148
  + Password on
  + Best to use same password as for users
* Connection security
  + Literally same thing as TLS cert rules

Updates

* Once a week
* Check for update

Rights management

* Use system user the server is running under

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Server:  
-Features: remove all those damn servers

-FTP-IIS/FileZilla

-Audits

OSI:APSTNDP-PLease Do Not Take South Park Away

Active Directory

Workstation To Domain

-Windows Features, install AD domain services role and DNS server

-Results Tab, promote server to a domain controller

Domain Share Names

C$ IPC$ Admin$

Admin%  
User%

Cis%

Default Server Shares

Netlogon

SysVol

Services:

Started and Automatic:

BITS - Background intelligence transfer service - dependency for Windows Updates

CCS Client - cyber patriot scoring client

DNS Client - Domain Name Server, Port 53 / URL name to numbers / host(s) to configure (in system32 / Drivers / Etc)

DHCP Client - Dynamic Host Configuration Protocol / Assigns Dynamic Ip Addresses / IPCONFIG in cmd to check your ip runs on port 68

Diagnostic Service Host

IP sec Policy Agent - Encrypts the traffic of what you are doing

Windows Defender Advanced Threat Protection

Windows Defender Firewall

Windows Event Collector

Windows Event Log

Windows Installer

Windows Search

Windows Time

Windows Update

WMI Performance Adapter

Stopped and Disabled

Fax

Geolocation

Infrared Monitor Service

IP Helper

Net TCP Port Sharing

Netlogon

Phone Service

Plug and Play

Print Spooler

Remote Desktop Services (README)

Remote Registry

Secondary Logon - Admins can login into a non admin account

Simple TCP/IP Services - Non needed and easily exploited / Echo (Port 6), Daytime (Port 13), QOTD (Port 17), Character Generator (Port 19), and Discard (Port 9)

Smart Card - Force you to have a key to login to stuff

SNMP Trap - Sends messages to people, grabs ip?

SSDP Discovery - Simple services discovery protocol, helps plug and play

TCP/IP NetBios Helper - Users can share files, print, and logon to the network

Telephoney - Phone support

Telnet - Two way communication to a computer

WebClient - Allows Win32 to access internet and run files

World Wide Web Publishing Service - Part of IIS, not needed

Windows Remote Management service

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

File Extensions - When searching use \*.extension

Aspx- ASP.NET Active Server Page

Bat- PC batch file

Cda- CD Audio Track

Exe- Executable program file

Gif- GIF file

Htm; html - hypertext markup language page

Jpg; jpeg- Joint Photographic Experts Group photo file

Mp3- MPEG layer 3 audio file

Mp4- MPEG 4 video

Mpeg- Moving Picture Experts Group movie file

Pdf- Portable Document Format File

Png - Portable Network Graphics file

Rtf- Rich Text Format File

Txt- unformatted text file

Vbs- VBScript

Mov- Movie

Avi- Audio video interleaved

Ps- Postscript

Wav- Waveform audio file format

Rip- Routing Information Protocol

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Hiding an application from uninstall in ctrl panel:

HKLM:\Software\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\(Application)

* Make a DWORD
  + SystemComponent
    - 1

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

IIS

* Make sure you have management tools installed
* Authentication
  + Anonymous Authentication
    - Disable
  + ASP.NET Impersonation
    - Disable
* Logging
  + One Log File Per:
    - Site
  + Format
    - W3C
  + Directory
    - %SystemDrive%\inetpub\logs\LogFiles
  + Encoding
    - UTF-8
  + Log File Rollover
    - Maximum file size
      * 100000000
    - Use Local Time for File name and Rollover
* Basic Settings
  + Make sure the name is correct
  + Physical Path
    - %SystemDrive%\inetpub\wwwroot
* Feature Delegation
  + Logging
    - Read Only

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Batch

* To copy a an output to a text file (netstat -aonb > name.txt)
* Baselines
  + Netstat
  + Process / Taskmon (powershell Get-Process)
  + Users

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Random Round 2 Things

Make sure to go through settings to get points after done other things

* Turn off autoplay
* Go through Defender exclusions

Look for Threats

* Backdoors
* Netstat -aon
* Task manager
* Malwarebytes/Defender

Smart Screen

* Reputation-based protection

Benchmarks

For RegEx Use Brackets

Control Panel

* Network and Internet
  + Internet Options
    - Security
      * Internet
        + Security level for this zone
        + High
        + Enable Protected Mode

Check box

- Trusted sites

- Security level for this zone

- high

- enable protected Mode

- Check box

- Restricted Sites

- Security level for this One

- high

- Check box

Make sure there are no startup or shutdown scripts

Validate Heap Integrity

Autoplay

What I missed

* Forensics 2 / Found on task scheduler
* DEP Enabled for all programs and services
  + Go to setting
    - go to system
      * about
        + advanced settings

setting

performance

data performance protection

turn on for all programs and services

* Windows Remote Management service has been stopped+disabled (Benchmarks)
* Internet Properties Enable Enhanced Protection Mode
  + Internet Properties
    - Advanced
      * Enable Enhanced Protection Mode

To make a secure operating system hidden file, type in **attrib +s +h full folder path to cmd**

**—--------------------------------------------------------------------------------------------**

**REGEDIT (Yay)**

H stands for hive

Hives → Keys

General Keys

* **Run (Make sure “VMware” and “(Default)” are the only keys in here)**
  + Computer
    - HKEY\_LOCAL\_MACHINE
      * SOFTWARE
        + Microsoft

Windows

Current Version

Run

* Run Once
  + Computer
    - HKEY\_LOCAL\_MACHINE
      * ASOFTWARE
        + Microsoft

Windows

Current Version

Run

* AutoAdminLogon (Make sure it is OFF)
  + Computer
    - HKEY\_LOCAL\_MACHINE
      * Software
        + Microsoft

Windows NT

Current Version

Winlogon

* Dhcp thingy
  + HKEY\_LOCAL\_MACHINE
    - SYSTEM
      * CurrentControlSet
        + Services

DHCP

Right click the key for permissions to start the service

TCP/IP

Right click the key for permissions to start the service

NT Service

DHCP should have full permission

**—--------------------------------------------------------------------------------------------**

**AD (even mor yay!)**

**Disable these Internet Properties**

* Control Panel
  + Network and Internet
    - Network and Sharing Center
      * Click on Ethernet
        + Properties

Link-Layer Topology Discovery Mapper I/O Driver

IPV6

LLDP Protocol Driver

Link-Layer Topology Discovery Responder

Microsoft Network Adapter Multiplexor Protocol

IPV4 Settings

* Control Panel
  + Network and Internet
    - Network and Sharing Center
      * Click on Ethernet
        + Properties

IPV4

Properties

Advanced

WINS

Disable NetBIOS over TCPIP

Disable TCP/IP netBios helper

**—---------------------------------------------------------------------------------------------**

Configure auto updates enabled

Hide specific control panel items disabled

Prohibit access to Control Panel and Pc settings disabled

Hide and disable all items on the desktop disabled

Netcat backdoor deleted

Netcat task on task scheduler deleted

Delete a task disabled on task scheduler

Script execution for powershell disabled

Startup script deleted

Require lowercase letters disabled

Pokemon DarkFlame Deleted

Internet options security tab configured

TLS 1.2 enabled all disabled

SSL 3.0 enabled rest disabled

Enable Enhanced Protected Mode

HTTP 2 Enabled all disabled

Check for signatures on downloaded programs

Check for server certificate revocation enabled

Check for publisher’s certificate revocation enabled

Send Do Not Track requests to sites you visit in Internet Explorer enabled

Warn if changing between secure and not secure mode

Enabled SmartScreen Filter

Never allow websites to request your physical location enabled

Virus.exe.txt deleted

Deleted desktop.png / Control Panel.bat

Allow font downloads enabled

Hide windows marketplace disabled

Hide Network Tab disabled

Audit Policies set to Success, Failure

Password Policies set

Autoplay turned off

Turn off InPrivate Browsing Disabled

Turn off InPrivate Filtering Disabled

Web sites in less privileged Web content zones can navigate into this zone disabled

Allow scriptlets disabled

Point and Print Restrictions enabled

Enable alternative codecs in HTML 5 media elements disabled

Enable automatic image resizing disabled

Do not save encrypted pages to disk enabled

Enable temporary internet files folder when browser is closed

Im a Malware.txt deleted

Control panel.png deleted

All shortcuts on the desktop deleted

Make sure to check d e p folder during comp

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

UAC Turned On

Removed access to the context menus for the taskbar disabled

Remove Task Manager Disabled

Tiny Server Removed

FQ 3 - System Shutdown

Netstat fixed

Fake “FireFox Updater” Event deleted - Had shutdown /s in it

HOST FILE C:\Windows\System32\drivers\etc

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Round 4 Practice Image

* Hacker Script File deleted from the documents folder
* Goodware deleted from the downloads folder
* Disabled prohibit access to control panel and PC settings
* Hide specific control panel items disabled
* IPV6 Disabled
* Deleted Goodware registry in Run (Regedit)
* Disable Anti Spyware disabled in (Regedit)
* Hacker Website Deleted
* Forensic Question 1 Complete, Windows Da Goat
* Google removed from host file
* “Windows Update” Shutdown -s Task scheduler Deleted
* Turned off file and printer share
* Remove startup script “Hacker.Script.ps1”

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

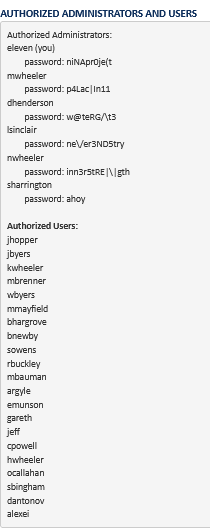
Round 4

* xAdministrator Disabled
* FTP Disabled
* Created group ftpadmins
* Added users to ftpadmins
* Ftpadmins can write
* Filezilla configured
* Deleted SecurityHealth Key in

IF I GET STUCK TRY TO FIND FRETS ON FIRe

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Round 3 Garbage



A million GPEDIT things congifured

FQ 1: HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp\PortNumber

Removed Windows Defender exclusions

User ocallahan no longer disabled

User two disabled

Mmayfield removed from admins

Forced user sharrington to change pass

My script was used, got points for passes and i think audits

Removed TeamViewer

Chromium download

Burp Removed

Pass policies set

Thunderbird upgraded

Tiled updated

Infrared monitor service disabled

`

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

XAMPP

X - Cross Platform (Ie. Windows, Linux, MacOS)

A - Apache (81) (open source IIS)

M - MySQL (SQL Server / Database)

P - Php (Programing Language)

P - Perl (Programing Language)

Apps That You Can Install With It

* FileZilla - FTP Server
* Mercury - Mail Server
* Tomcat - Java
* Webalizer - Web Analytics
* Open SSL - HTTPS certificates

(80) HTTP - Hypertext transfer protocol

(443) HTTPS - Hypertext transfer protocol SSL

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Features - Turn On

.NET framework 4.8

Work folder client

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Ports to know

Anything above 1029 - unknown

1900: SSDP discovery

3389: RDP

43: WhoIs

53: DNS

123: NTP/ Windows time

67 + 68: DHCP Server

23: Telnet

80: HTTP

443: HTTPS

445: SMB

69: TFTP

7: Echo

13: Daytime

17: QOTD

19: Character generator

88: Kerberos

25: SMTP

22: SSH

81: Apache management

139: netBios

20 + 21: FTP

1306: SQL

25565: minecraft

5800 / 5900: VNC

389: LDAP

3478-3841: Ms Teams

636: LDAPS

990: FTPS

110: POP3/POP

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Goose Extermination

* May just sit in a file path
  + EVEN IF IT IS NOT NAMED THE SAME THING

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Good applications or websites to use during comp

Rumkin

Cyber Chef

dCode

Malwarebytes

CVE.mitre.org

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

PORTS

Ssh:22-Ftp:21-Cupsd:162/3-Http:80-Https:443-Telnet:23-Minecraft:25565-Smdb:139-TfptTrivialFilePrintingProtocol:69-Smtp:25=clienttoserver-Somba/Smb:445-Imap4:143-Pop3:110=email-Bind9:5234>DNS:53-RDP:3389-Netbios:139-MySQL:3306/1639-SQLServer:1433ExcelSpreadsheetServerMicrosoftSpecific-NTP:123NetworkTimeProtocol-DHCP=DynamicHostControlProtocol:67client/68server-Kerbenos:88-Apache:8080AdministratorPort-7:echo,13,15-simpleTCP/IPFeaturesToRemove-RPC:135RemoteProcedureCall-SNMP:161/162(trap)SimpleNetworkMessagingProtocol-

ICMP:

SSl-SecureSocketLayer-encrypts stuff for other services

>TLS

Server: configured by admins. If using all server networks, server gets slower.F

User Computer: Connects to the server.

Least Privilege, Give people the least permissions they need to keep them in line.

2k16 Server-

gpmc.msc=Group Policy Management->Make Group Policy->

Domains>h.com>Group Policy Objects>new, name, right click, edit,

>shows normal gpedit policies, set to image specifications>you can force something on> and apply to all below your domain editor.

Right click on h.com, link your GPO, right click to enforce it.

4 things, configure, put in settings, enable, link it, enforce it, [in relevant prompt] open command prompt, gpupdate /force

Features,

DNS-> URLs to IPs/text to computer garbage

>Structure

> . Root Server (TLD)

>.com, .net, .gov, .edu, country specific and smaller stuff.

[EX.]looking for engineering.mit.edu - google asks .com server who asks root who asks .edu who sends to .mit who sends to engineering

>Domain Specific- \*DOMAIN HIERARCHY\*

>DNS->TLD/PDC=Primary Domain Controller

>RODS=for storage

>DC-accounting >Different perms from other DCs

>Workstations

>Individual people

>DC=domain controller

>Mail

>HTTP

>SQL

> Don’t kill

>AD

>requires DNS

>Manages other computers

>Port SB

>Records

>types

>A

>IPV4 -standard IP addresses /old and outdated

>AAAA

>IPV6 -

>Base16 [0-9=base10] and first 6 letters of the internet

>Fe80:: = loopback

>MX

>Mail Exchange=Email

>SMTP-25

>POP3-

>IMAP-

>CNAME

>DNS

Group Policy Trumps Local Policy.

FTP - Port 21

Term Service - RDP - Remote Desktop Protocol - 3389

W3SVC - World Wide Web - IIS - 80 (HTTP) or 443 (HTTPS)

LanManServer - Local Area Network Manager - Network TCP/IP

BITS - Background Intelligent Transfer Service - Download and Update Between Servers

DNSCache - Domain Name System - Changes Domain Names to IP address.

WUAUServ - Windows Updates

FAX - Open Port - Fax has to run crap code in INF files.

Remote Registry - People can change stuff from anywhere

Seclogon - Secondary Logon - allows multiple people on at once.

RIP - Routing Information Protocol

Telnet - Bad old and outdated - Remote Access

**Registry**

hkcu: registry

HKCU:\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3’ - zones for restricted sites

“Hives” 5 of them

Run and RunOnce are major check spots. They run on startup and otherwise.

Computer/{hKEY LOCAL MACHINE/}/SOFTWARE/MICROSOFT/WINDOWS/CURRENTVERSION/{RUN/RUNONCE}

hKEY LOCAL MACHINE/}/SOFTWARE/MICROSOFT/WINDOWSNT/CURRENTVERSION/WINLOGON/AUTOADMINLOGON

File Types -

.Bat - Batch (cmd)

.Ps - Powershell, .Ps[1] - designates what script is \*.Ps[1] \*=Wildcard

.Vbs - Visual Basic Script => Macros

.Js - Java script => Browser Based

Java => Platform Agnostic (Any platform can run it. => bad and slow

.Py - Python

.Rb - Ruby

Find Scripts -

Search for Filetype - show hiddens, can be turned off.

Schedule Tasks

Registry - Local Machine - Software - Microsoft - Windows - CurrentVersion - Run/Runonce

Task Manager - Startups

Group Policies - administrative Templates - lists - Windows Settings

Wuauserv - windows updates

netsh advfirewall - always says firewall is on even when off.

CCleaner

Legitimate software that they try to sell, adware.

PCoptimizer

Toolbars - Bad and Annoying - malware/adware

Languages for Windows

Powershell

Batch - original language for windows. Get to it via cmd - type cmd in the search bar (Ipconfig(network information) /all netstat/netstat -aon(active connections/ -aon shows all ports))

Secpol in windows search - lies about firewall configuration with no reason

POWERSHELL NOTES OVERALL.

20 years younger than batch, batch for dummies with a lot more utility

A few new commands from linux and a few new ones.

Used for scripting in powershell ISE simply allows writing and running scripts.

Also shows all powershell specific commands.

List services - get-services

Variables always start with $ (Dollar signs)

Lt - less than

Loops:

$i=1

$iList = {1, 2, 3, 4, 5}

Foreach($i in $iList)

$i++

} echo $iList

Will display 23456 because it replaces the number with the variable each time

Forever loop - while($true)

For loop - for ($i=0; $i -lt 3; $i++)

[Command]

} - end of loop

Set to 0, until it is 3, loop. At end of loop add 1. Loops 3 times

Define variable - $[VARIABLE]=[NUMBER]

Not equal to - -not([VARIABLE]=[NUMBER])

= - set to [number]

-eq - check for equal

-lt - check for less than

-gt - check for greater than

Checks for true/not true - If [(-not]($i -eq $true)[)] {

sc start WinDefend

} Else {

sc stop Windefend

Net user - list users

Select-String -Pattern “[variable]” - look for variable in list of selected thing in parameters (ex. “ ”)

Usage:

foreach ($i in $goodUsers) {

if (-Not $(net user | Select-String -Pattern "$i")) {

$score-=2

}

}

Try/catch - Try [this] if that doesn’t work do catch [this]

Usage:

foreach ($i in $requiredServices) {

try {

if (-Not $($(Get-Service -Name "$i").Status | Select-String -Pattern "running")) {

$score-=3

}

} catch {

$score-=3

}

}

.status - running/stopped

Usage:

foreach ($i in $goodServices) {

if (-Not $($(Get-Service -Name "$i").Status | Select-String -Pattern "stopped")) {

$score+=3

$vulns++

}

$totalVulns++

}

Test-Path - existing/not signal/not on path check

Get-SmbShareAccess - port445 file sharing service

ConsentPromptBehaviorAdmin - asks for consent to do anything - should be set to 3

Prompt for credentials - in user account control.

BATCH NOTES OVERALL.

Program=

Netstat -aon >> C:\Users\User\Desktop\baseline.txt

{Also works in powershell}

Command prompt - cmd

see folder - ls

See all - dir

Go into folder - cd [Folder name]

Run .exe - start

Spit message back at me - echo

Background running script in batch - @echo off

Computer Management - compmgmt

stop /start/ get information from services - sc stop/start/query (ex.) WinDefender

Screw with settings of services - sc config [NAME] start=auto/disable

See all users [shows info on user] {add user with name given} - net user {/add} [username]

Change password - net User [Username] [Password]

Delete user - net user /delete [name]

enable /disable user - net user [User] /active no/yes

Show info on groups - net localgroup

Add user to group - net localgroup [group name] /add/delete [username]

Info on firewall - net sh advfirewall show allprofiles

Massive list of tasks running/tasks to run - tasklist

Shows running tasks - tasklist fi “status eq running”

Scheduled tasks - schtasks

Find DNS server - nslookup

Security policy - secpol

Task manager - taskmgr

Local users and groups - lusrmgr

Computer manager - compmgmt

Local group policy - gpedit

Useful command to find running applications

tasklist /v /fi "windowtitle eq Administrator: Command Prompt"

To stop a automatic shutdown, use shutdown /a

MALWARE - unwanted program

CCleaner-NetCat-Mimikatz-Nbirdshell-TightNVC\_Server-BitTornado-John\_the\_Ripper-Advanced\_Port\_Scanner-Brutus-ChickenInvaders-KNCTR-Beware\_IRC\_server-HashCat-Tini-Fgdump-Vstumbler-Ophcrack-Tx-Netbus\_Pro-VirtualDJ\_8-Wireshark-RainbowCrack

Task\_Scheduler-Registry-Services-Task\_Manager-WinDefender[settings]-MalwareBytes

Check Ports-PID+port

Random Notes:

FTP- uses port number 20 and 21, IIS can host FTP but not primary function

IP address #.#.#.# all need to be within (0-255)

Loopback address- is an address that sends back itself, its how you check your machine. Its either (127.0.0.0.1, or 0.0.0.0

Add Roles and Features

Role based Features Click it

Based on scenario which server roles you should click

If no one ask for them make sure the are unchecked, and check the one they want =

SMB- server message block runs on port 345

New stuff that should show up in round 3:

Servers - IIS->FTP 21 Win10

‘->HTTP 80 Server

IIS management

-Authentication-Enable All? [check] anonymous authentication off/on dependent on scenario(off by default)

-eh-logging

-SSL -Certificates-Encryption, Authentication, integrity - Certificate required for SSL Certificate

-FB Setup Mid-Right-

1Site is C:\inetpub\wwwroot

2Loopback-127.0.0.1-255

3Explore button in top right corner

Group Policy

Winsettings\_>Scripts

BitLocker Backs Up Files(not for competition)/encryption

>Control Panel(normally)

>>Group Policy for without flashdrive (google it) !VERY LAST THING! It likes to shut itself off

Group Policy administrative policy, bottom, sort by state, take ethan’s list

Autoplay off (Control panel, settings, group policy/administrative Template/windowscomponents/autoplaypolicy) Turn it off on all 3 for garunteed points

Task Scheduler, Run/Runonce, Administrative Template, Task Scheduler, Task manager scripts, scripts in group policy

Network and internet, internet options, properties, Security, protected mode on always, Medium Low, Medium Low, Medium, High, Check the sites, Privacy, on/high prob doesn’t matter, advanced, Multimedia off, Security/Block Check enhancedprotectedmode.on useall warnon enablesmartscreen and do not allow

Server manager blue button IEESC ON

Group policy scripts delete real file

Advanced Audits not configured

Admin templates/autoplay/turnoffautoplay/ALL DRIVES

All settings not configured

Do the entire list twice in both top and bottom

Firefox, update and privacy and security settings

https://geekflare.com/apache-web-server-hardening-security/

CRAPPY APACHE THINGS

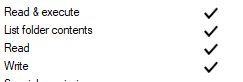
WHAT I DID

Enabled control panel

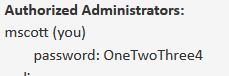
Enabled all smb features

IIS Disabled

Removed everyone from sales sharing tab



All passes set to Th!s!sAG00dP@SS



CHECK PVANCE LATER WHEN STUCK WEIRD USER

Dwallace disabled

Removed an administrator

7-zip and GnuCash updated

Disabled allow surf game

Many Gpe edit things changes

Firewall configured

Deleted Totalcmd

Moved Bcastdvr - From Windows Folder to Deskotp

Moved Digital locker - From windows Folder to desktop

Configured Edge

Moved Nirsoft - Program Files to desktop

Moved L2schemes - Windows to Desktop

Edge configuredVersion Header

Directory Browser Listing

Forbidden Page

ETag

Run Apache form Non-Privileged account  
Change Permissions of Bin and Conf folders

Round 1: RDP - control panel->system and security->System-allow remote access, FTP - control panel programs and features, IIS FTP[21]/HTTP[421] server

Give users new passwords

Prohibited MP3 Files

File Sharing Disabled for C: Control panel $C $Admin $IPC,

In server - World Wide Web Publishing Service - Ports - cmd netstat -aon - port 80 IIS,

Beware IRC Server - displayed as open port,

Round 3 win 10 practice that i will put in proper place later

Free MD5 Hash Search to reverse search MD5 Hashes

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Please read the entire README thoroughly before modifying anything on this computer.

UNIQUE IDENTIFIER

If you have not yet entered a valid Unique Identifier, please do so immediately by double clicking on the "CyberPatriot Set Unique Identifier" icon on the desktop. If you do not enter a valid Unique Identifier this VM may stop functioning after a short period of time.

FORENSICS QUESTIONS

If there are "Forensics Questions" on your Desktop, you will receive points for answering these questions correctly. Valid (scored) "Forensics Questions" will only be located directly on your Desktop. Please read all "Forensics Questions" thoroughly before modifying this computer, as you may change something that prevents you from answering the question correctly.

COMPETITION SCENARIO

You work for Always Fresh Aqua (AFA), a new water production & distribution company.

This company's security policies require that all user accounts be password protected. Employees are required to choose secure passwords, however this policy may not be currently enforced on this computer. The presence of any non-work related media files and "hacking tools" on any computers is strictly prohibited.

This company currently does not use any centralized maintenance or polling tools to manage their IT equipment. This computer is for official business use only by authorized users. Your job is to secure this computer, within the guidelines of the scenario, while ensuring the availability of authorized business critical software and services.

Company policy states that Windows Action Center should be enabled and monitoring the security status of desktop Windows operating systems at all times.

This is a critical computer in a production environment. Please do NOT attempt to install Windows "Feature Updates" or "Insider Preview Builds." Please do NOT attempt to use the Windows recovery options "Reset this PC" or "Go back to an earlier build".

WINDOWS 10

It is company policy to use only Windows 10 on this computer. Management has decided that the default web browser for all users on this computer should be the latest stable version of Google Chrome.

Policy also states that the Guest account on the computer must be disabled.

Your company just hired a new employee. Make a new account for this employee named "tonraq".

Management has been informed that the IT team has been unable to update the Windows operating system. The error code points towards the Windows Update service being disabled. Please re-enable this service and install all necessary Windows updates.

There is a drive being shared on this computer that can be risky because anyone who has access to that drive can access all the files and folders on the shared drive. ​

While removing unauthorized tools from this computer, please note: Some applications must be uninstalled in order to be successfully removed. Other applications can be removed by simply deleting the application file.

This is a standalone workstation machine and does not have any business critical services.

Critical Services:

(None)

AUTHORIZED ADMINISTRATORS AND USERS

Authorized Administrators:

korra (you)

password: (blank/none)

mako

password: fir3FeRr3t$!

bolin

password: p4buisTh3Be$t

asami

password: fu7ur3indu$tr!es

tenzin

password: pema

lin

password: be!f0ng123$

Authorized Users:

jinora

ikki

meelo

opal

kai

bumi

kya

suyin

pema

tarrlok

varrick

iroh

wu

raava

gommu

yung

raiko

desna

eska

COMPETITION GUIDELINES

In order to provide a better competition experience, you are NOT required to change the password of the primary, auto-login, user account. Changing the password of a user that is set to automatically log in may lock you out of your computer.

Authorized administrator passwords were correct the last time you did a password audit, but are not guaranteed to be currently accurate.

Do not stop or disable the CCS Client service or process.

Do not remove any authorized users or their home directories.

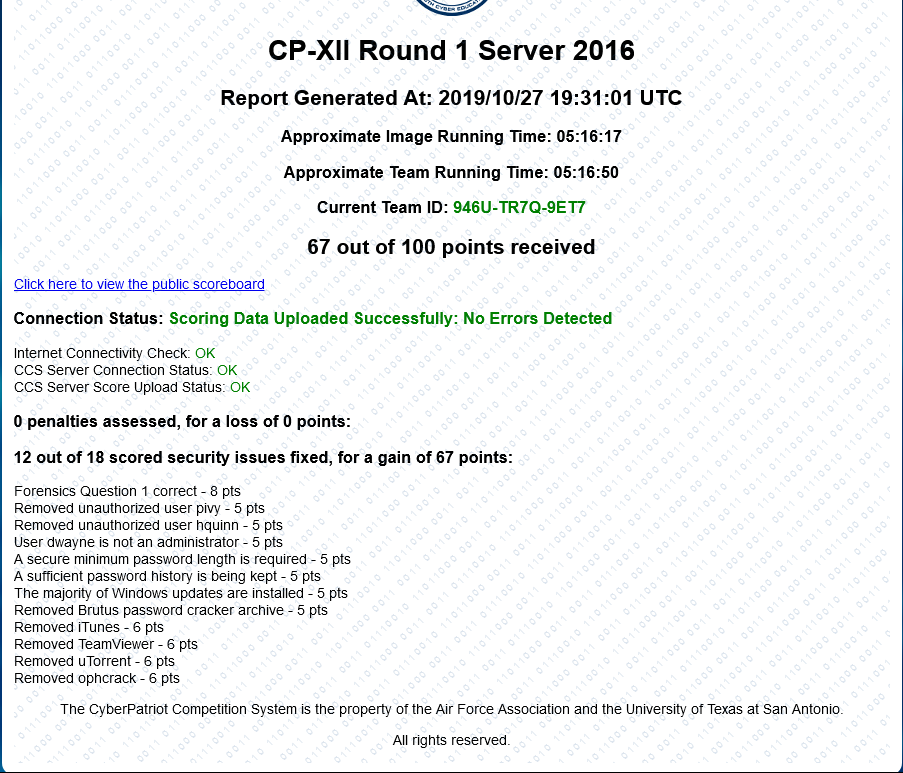
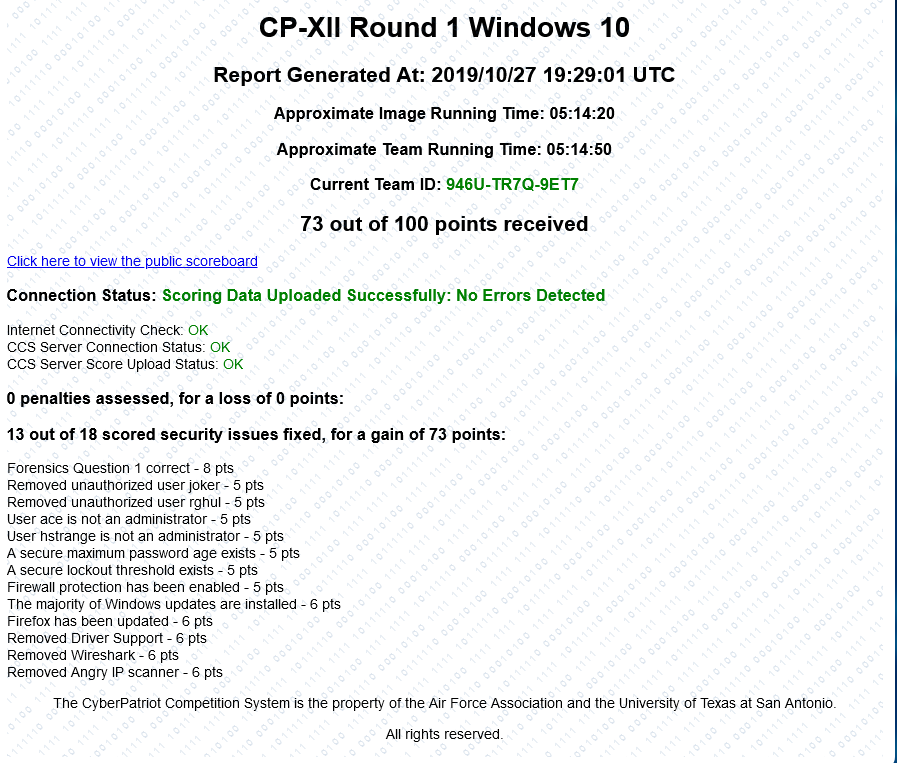
The time zone of this image is set to UTC. Please do not change the time zone, date, or time on this image.

You can view your current scoring report by double-clicking the "CyberPatriot Scoring Report" desktop icon.

JavaScript is required for some error messages that appear on the "CyberPatriot Scoring Report." To ensure that you only receive correct error messages, please do not disable JavaScript.

Some security settings may prevent the Stop Scoring application from running. If this happens, the safest way to stop scoring is to suspend the virtual machine. You should NOT power on the VM again before deleting.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_



Linux/Windows Combined Lesson

Configuration FIles - SSH-RDP clone, SWD = files the computer relies on to be its settings

Bad shit, delete

Shifting from passive to active - Netcat listeners, reverse shells, Unauthorized users, Unauthorized services, Time is of the essence

Baselining - take stock, take note of open ports, all users, installed services, backup databases, websites, and special custom files

Access through authorized services

[22]SSH - PASSWORDS! - change them = Secure Shell- Remote logon protocol[RDP Clone]

[23]Telnet - (OLD) Throws traffic between computers very loosely and badly made, easy to compromise

[]Samba - File sharing service- can steal all of your files, like passwords.txt

VSFTP - Samba clone

news:x:9:9:news:/var/spool/news:/usr/sbin/nologin

Hacked = news:x:0:0

00 = superuser

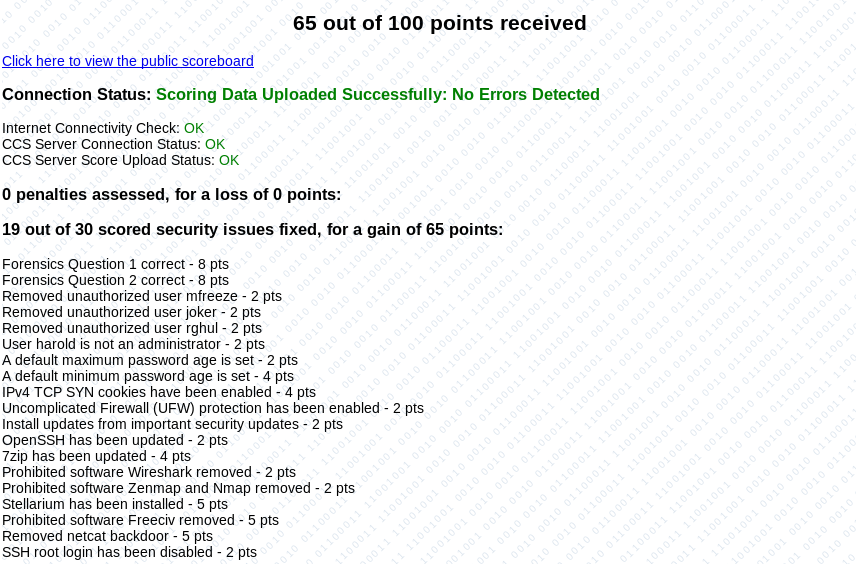
Hacked = sbin/nologon

Encryption should be $6

Skim==/etc/crontab, crontab, /etc/rc.local, /etc/bash.bashrc - runs stuff for you, ~/bashrc, /etc/init.d/\*

Startup, Run, Runonce, Service Register, Group Policy

Bad Tricks - Renaming Binaries = SVChost, Renaming Services

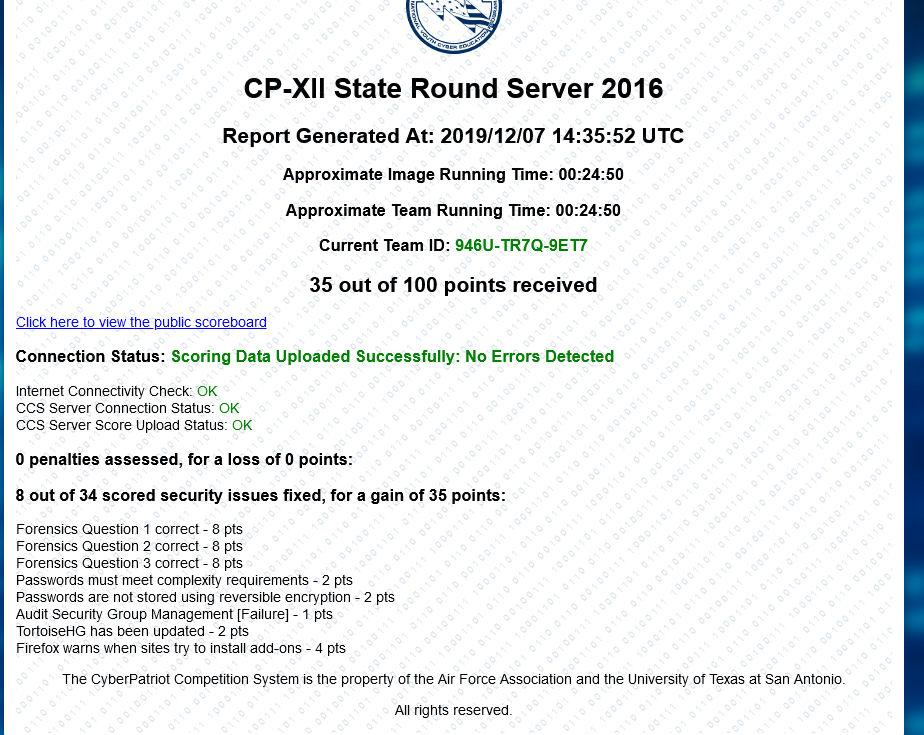
****

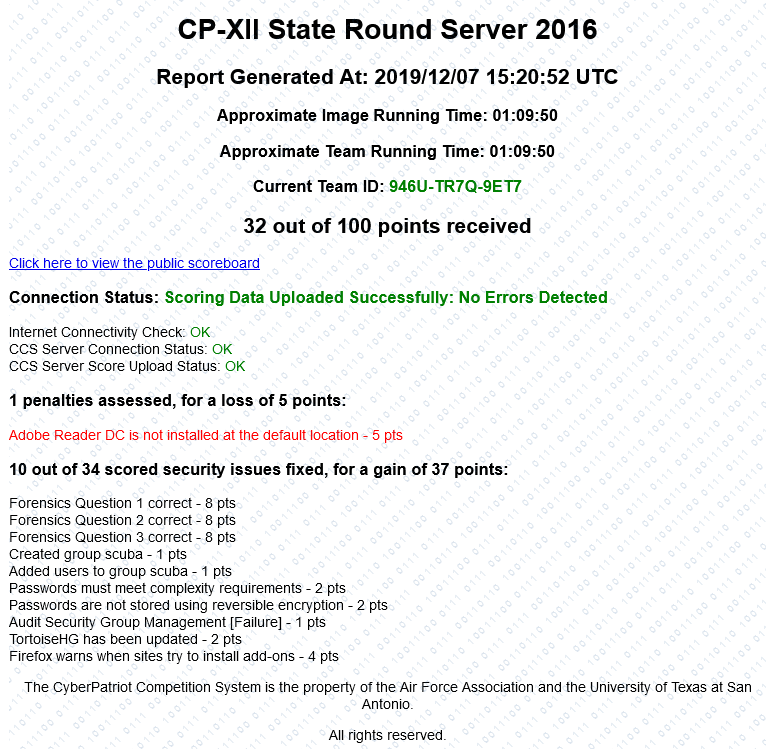
Firefox Pop-up Blocker Block dangerous downloads, MP3 Files, Thunderbird updated, Local use of blank passwords to consol only?, FTP service, Don’t display last user?=Win10 Real hiddenfiles

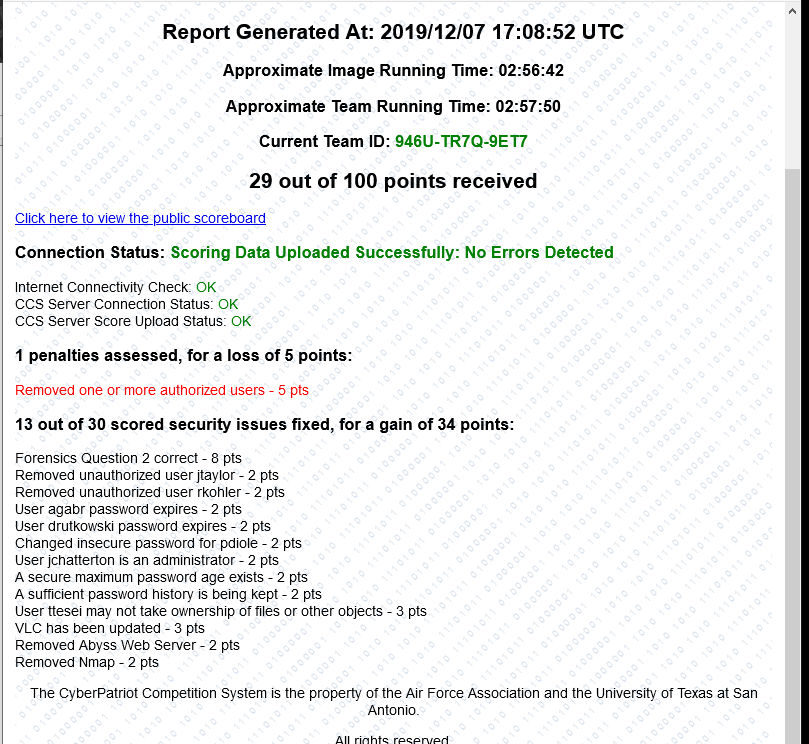
****

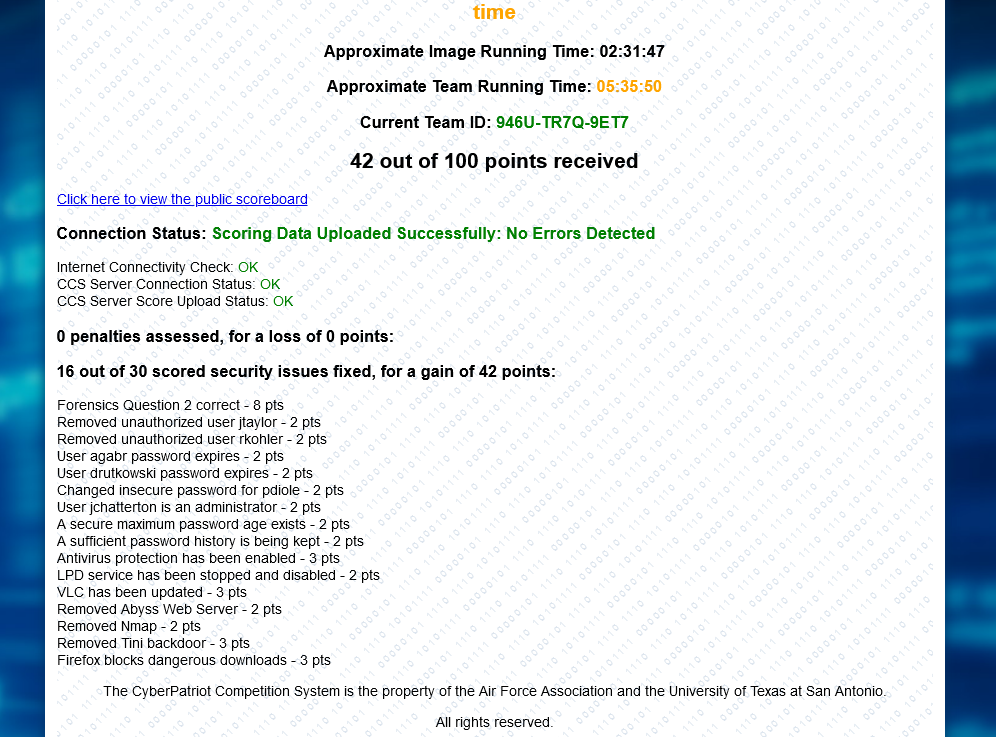
Local Blank Passwords Consol only, Brutus Password archive, Event Log,stopGCPDsharedfolder

****

****

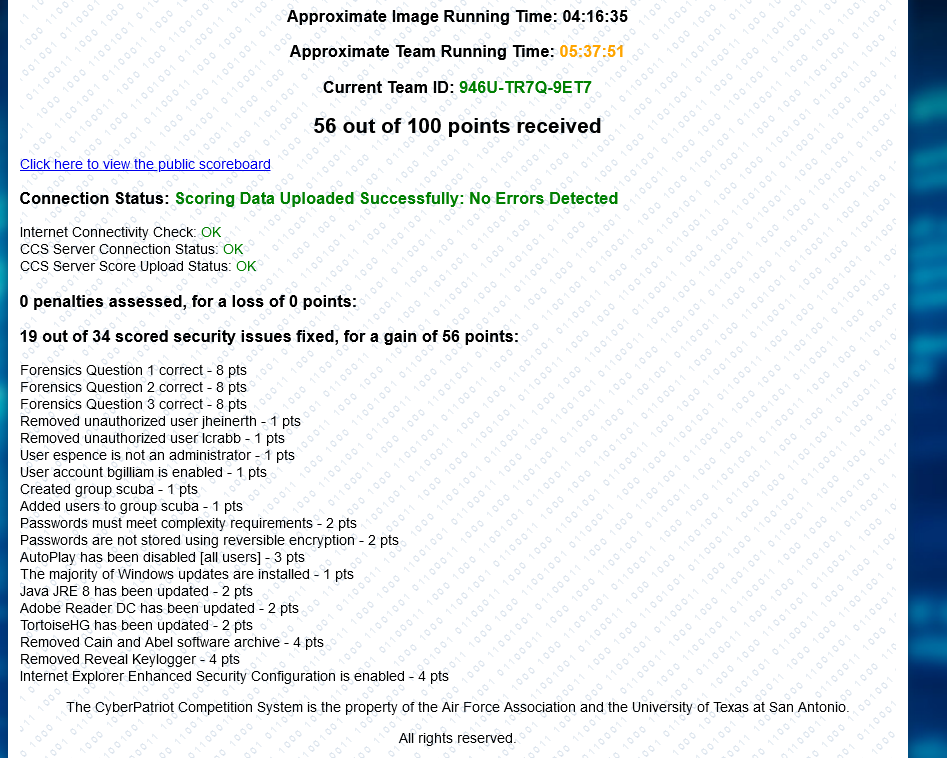
****

****

****

**Blank passwords console only, prevent installing of printer drivers, File sharing, Webclient, screw you ethan, Hashcat windows 10 in program files, Tini Backdoor, Interned explorer, RPC, RPC connection, encryption High, Autorun commands have been disabled, ttesei ownership?, Nikto scanning software archive**

**Group Policy**

****

**Google How to secure IIS-OWASP IIs default web browsing disabled- IIS manager, open TFTP server, John the ripper Program Files, TightVNC Program files and registry, Next TCP port sharing service, Audits after reset, Firefox, dont share lan hash value, Rempote Registry off, Net.tcp port sharing is bad, everyone may not access computer from network**

ballen (you)

password: (blank/none)

iwest

password: JiTTerS

pspivot

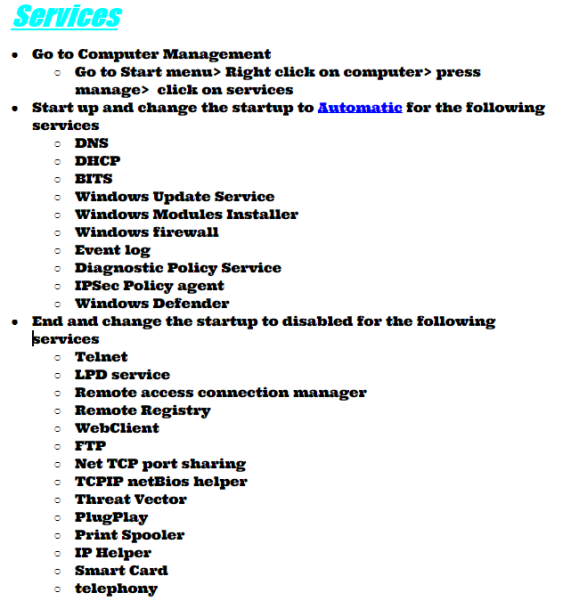
password: thawne25

grodd

password: ZoLomOn

jwells

password: quick



2021/22/1

**REG add HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System /v DisableRegistryTools /t REG\_DWORD /d 0 /f  
Run in Run ^**

**Run cmd as different user - WORKS FUCK YOU**

**Find service kdc, use services to find dependencies**

**Fixed Firefox Settings 1**

**Started gpedit in gpmane**

**User rights assignment fully blank**

**Benchmarks**

**Windefender - turn on in settings \*\*\*APPARENTLY FUCK\*\*\***

**Remove the alphabet of exclusions 1**

**Control flow guard Default on**

**Remove unwanted software**

**Removed Amartin from admins**

**Changed share permissions**

**Enforced GPO**

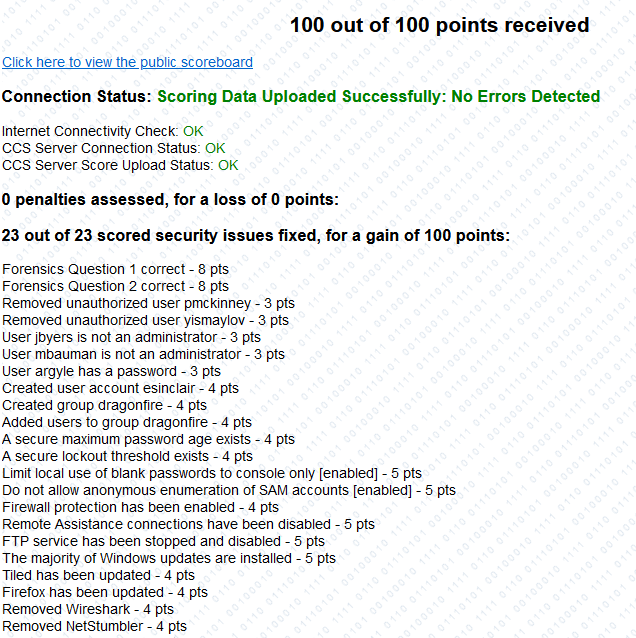
**Did services**

**IEEE**

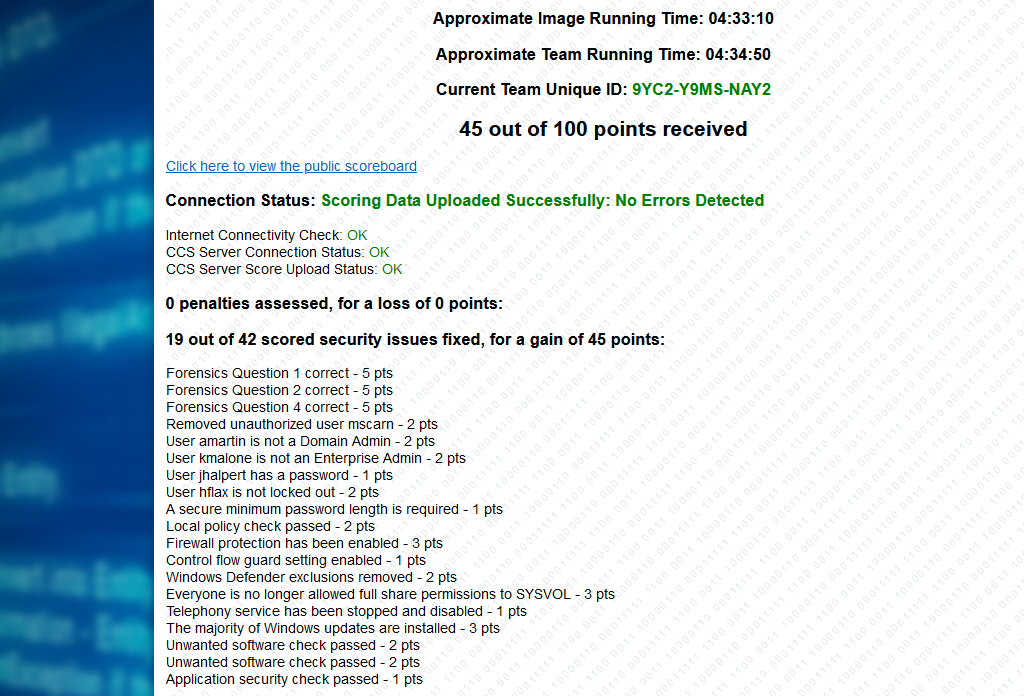
**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

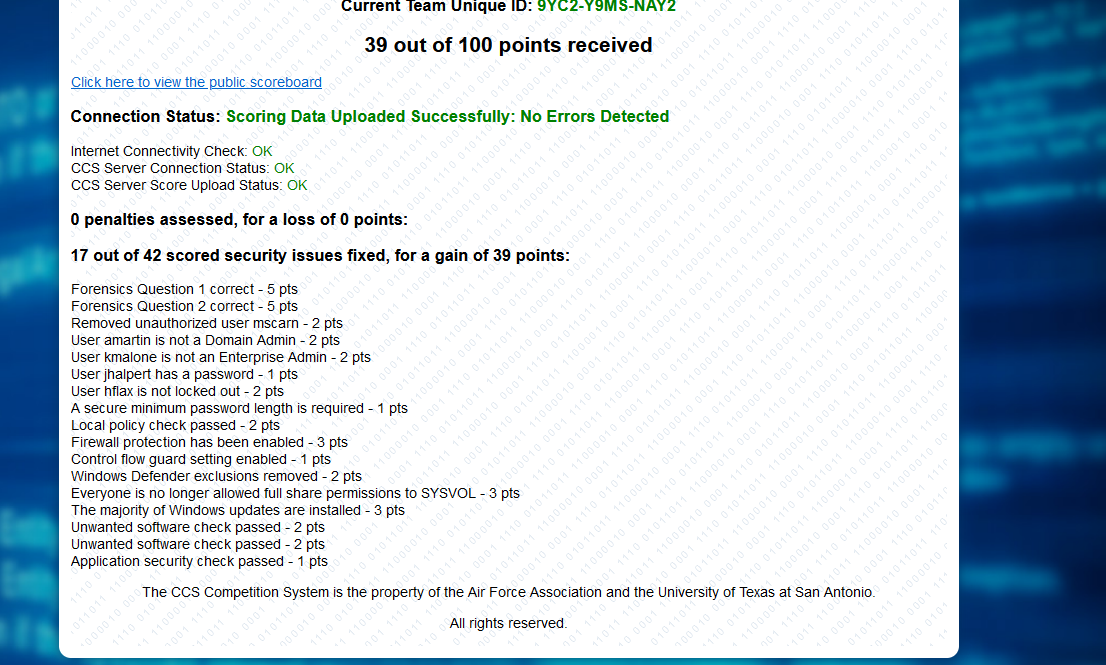
**Round 1 Notes**

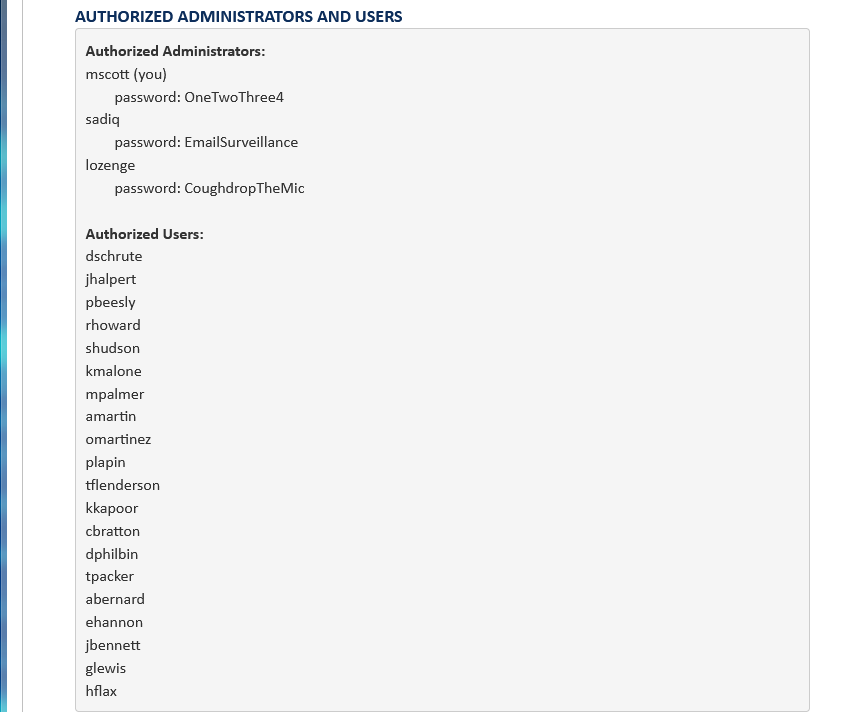
* **Firewall Turned On**
* **Removed pmckinney, yismaylov**
* **Created account sinclair**
* **Greated group dragonfire**
* **Added users to group dragonfire**
* **Firefox was updated**
* **Removed Wireshark, NetStumbler, and PC Cleaner**
* **Set all passes to Th!s!s@G00dP@ss**
* **User Passes configured**
* **Password Policies**
* **FQ 2 = 56F722195D4B249BA6764BEB8906B4DDD401BE66**

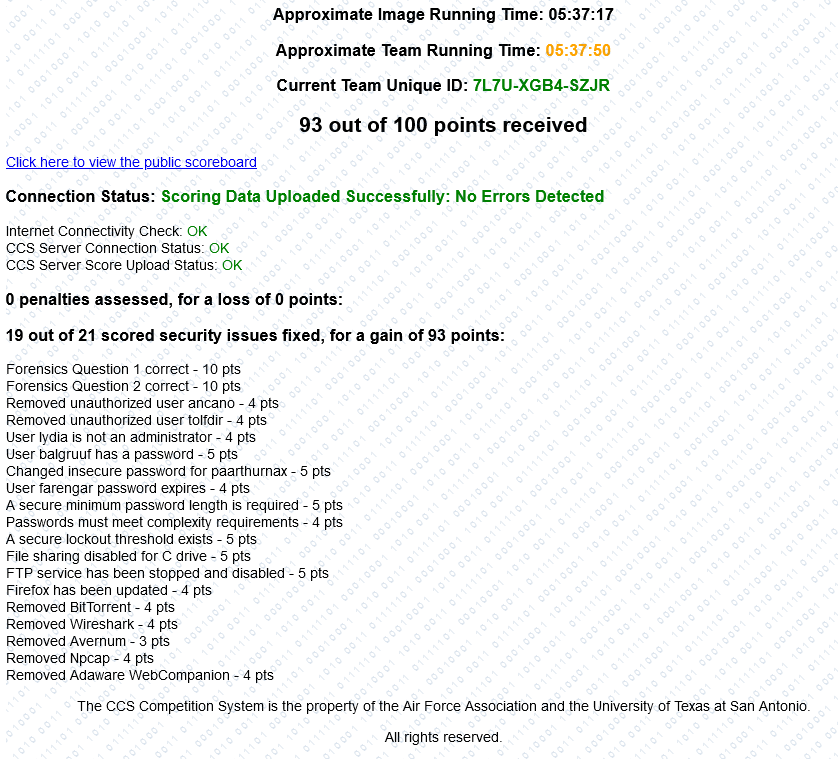
****

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

****

****

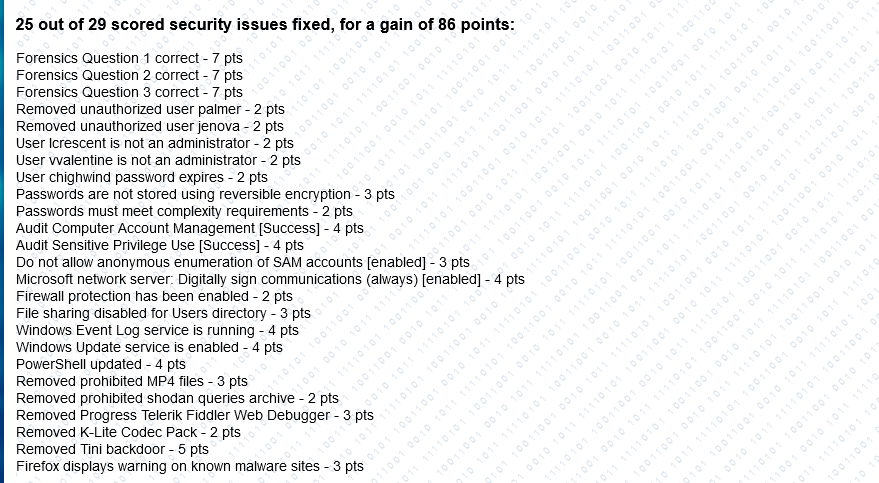
****



All Settings - limit use of blank passwords to console only

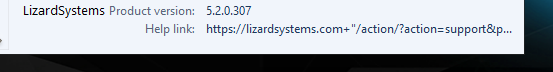
Firefox auto-updates

Cntrlaltdel not required to login

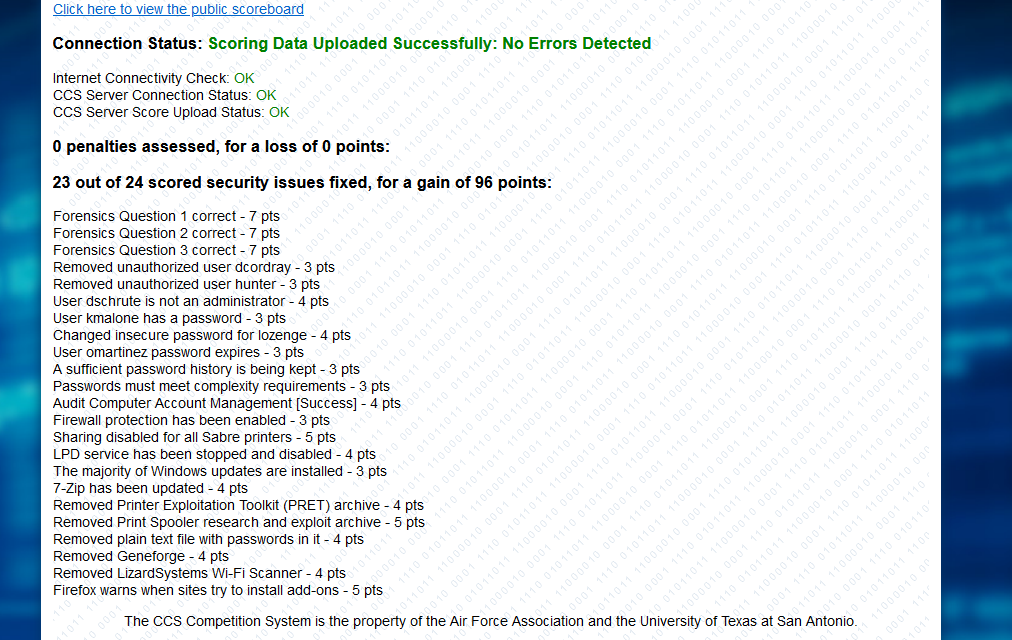


FIREWALL STOP SHUTTING YOURSELF OFF

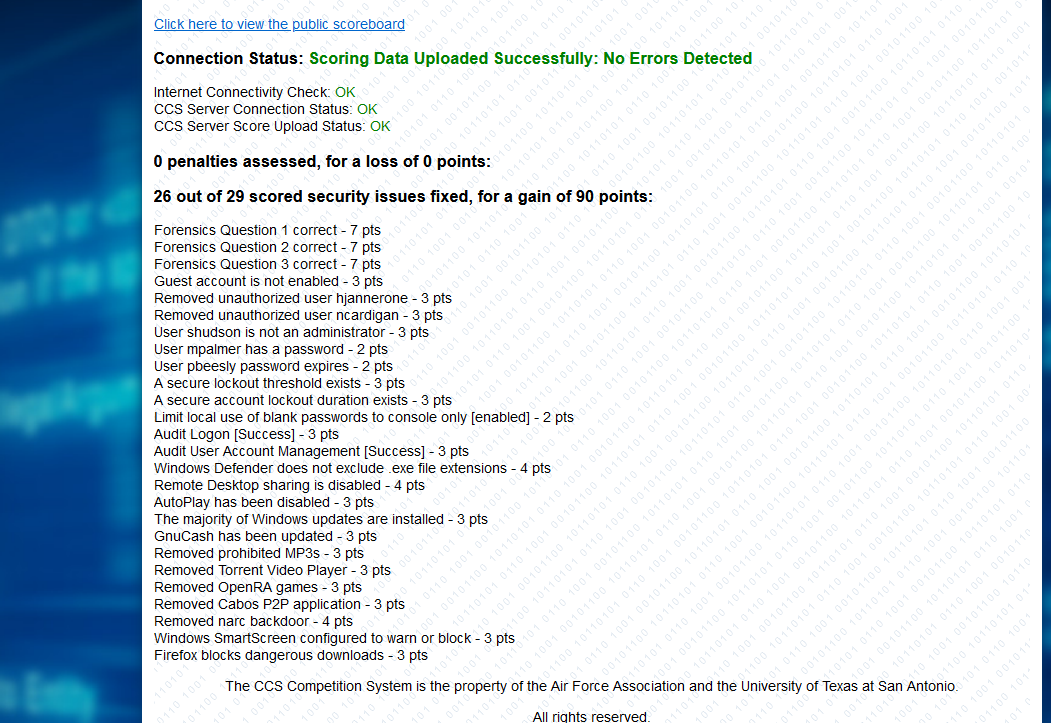
**Hell round 2021**



System32\spool\drivers



Users cannot uninstall printer drivers [enabled]



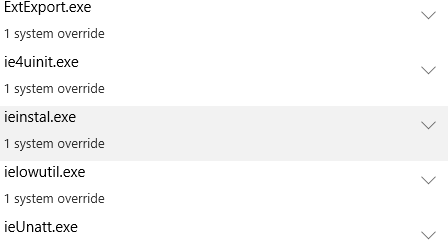
\_\_\_\_\_\_\_Did Not Get\_\_\_\_\_\_\_

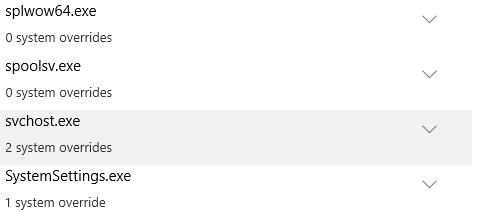
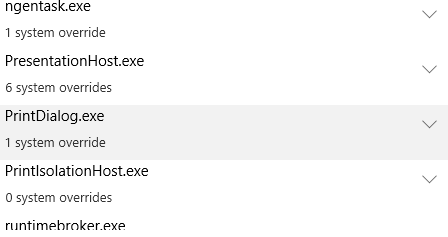
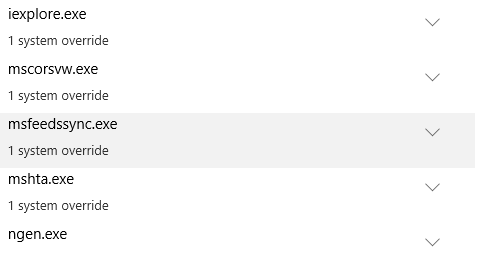
Validate heap integrity -App + Browser Control - Exploit Protection

Recovery Console: Allow automatic administrative logon [diabled] - 3pts

Infrared monitor service has been stopped and disabled

States Stuff Win 10





Google works, fixed DNS rerouting

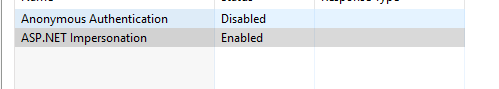
Deleted tiny

Deleted Server

Turned task manager back on

grouppol/network/etc/etc/firewall

Windows defender enabled



Disabled Powershell Environment task due to typo in description

Turned on all audits in a desperate bid for control

Killed scoring

Found weird bad server page on inetpub with funky if statements

Disabled Defrag Partner

THINGS I LEARNED:

Check my server ports, should be normal ports for Protocol

Check for secondary, bad sites.

Shutdown /a (in CMD) aborts shutdown

POC-Activity-211104.log is Forensics 1

Ncrack 0.7

Osquery 5.0.1

Ieinstal.exe

Ielowutil.exe

IeUnatt

Iexplore

InetMgr

Mscorsvw

Msfeedssync

Mshta

Ngen

Ngentask

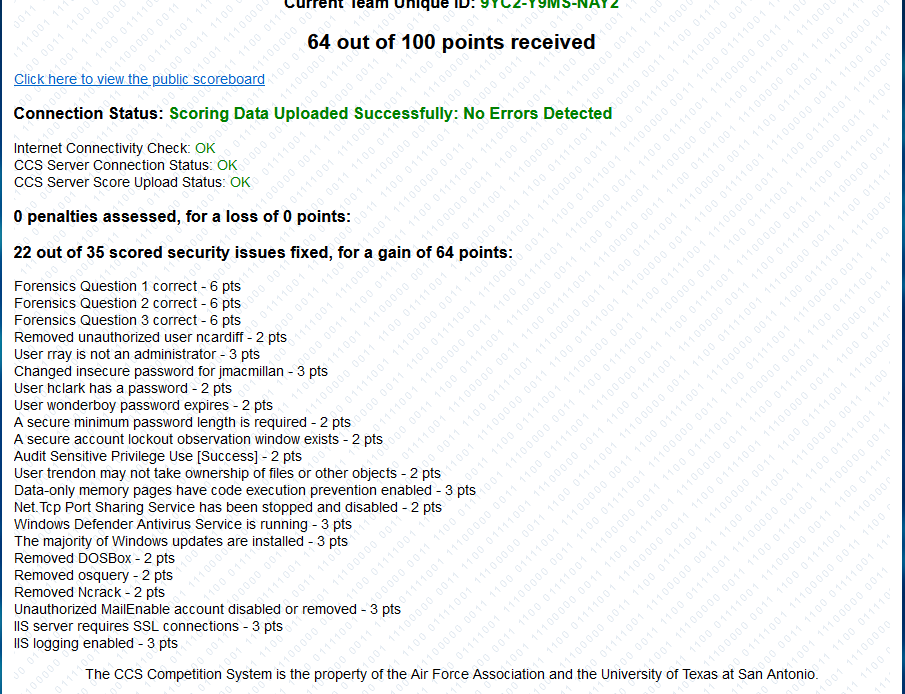
Presentationhost

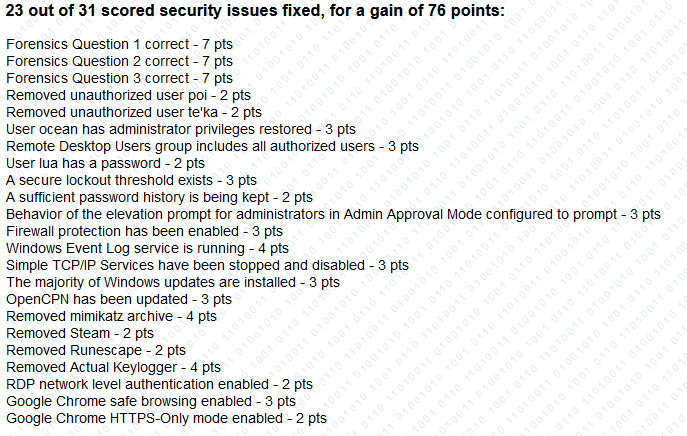
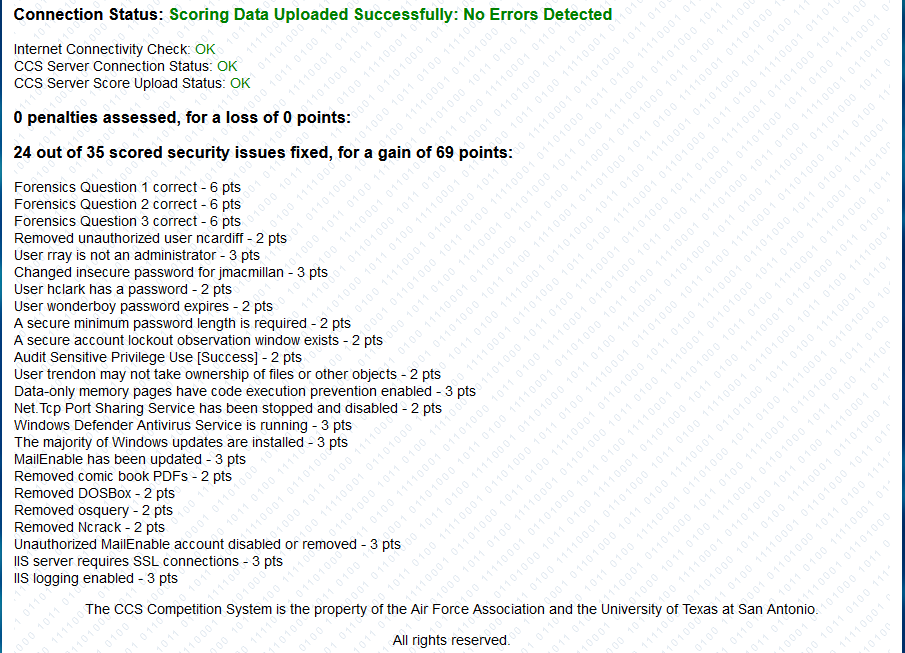
Printdialog.exe

Runtimebroker.exe

Svchost

Systemsettings





How to do andrew thing: Go into internet properties, disable all old TLS, and enable the newest

Allowed admins to go through RDP

Limit Local use of Blank Passwords to Console only

