1. **Set policies for a secure workstation.** You will do this by using a template created by National Institute of Standards & Technology (NIST), a government entity that gives guidance on cybersecurity. (Note - this will make it so that the policy requires strong passwords, etc. BUT it doesn't change existing weak passwords.)

1. Start | Run

2. type *mmc* and click OK will launch local security policy editor

3. Choose File | Add/Remove Snap-in

4. In the Add/Remove Snap-in Dialog box, click Add.

5. In the Add Standalone Snap-in dialog box, select *Security Configuration and Analysis*, click Add, and then click Close.

6. In the Add/Remove Snap-in dialog box, click OK

7. In the left pane of the MMC, right-click *Security Configuration and Analysis* and select *Open Database*.

8. In the File name box, type RBR_Template - (note: this is just a name we are giving it - you could use Disney or any other name) and click Open

9. In the Import Template dialog box, browse to where you saved the template file and select *Win7_Template.inf* and click Open (note: this is for Win7 or Win8 - use the correct template for your OS)

10. In the left pane again, right-click Security Configuration and Analysis. This time select Analyze Computer Now.

11. In the Perform Analysis dialog box, click OK. The utility will analyze the computer for security issues. When it is done, it will display the results.

12. In the left pane, expand the folders and select a few of the policies. Look to see which ones are marked with a red X. These are the items that don't conform to a securely configured PC.

13. In the left pane, right-click *Security Configuration and Analysis* and select *Configure Computer Now.*

14. On the Configure System screen, click OK

15. To check to see what changes were made →In the left pane again, right-click *Security Configuraiton and Analysis.* This time select *Analyze Computer Now.* Review to see how the Red X items are now all resolved.

Close out of the MMC - do not save the Console when asked.

General Checklist

1. Input team ID
2. Read the Read me

1.
2. Update computer and turn on automatic updates
   1. This may take quite a while. Since you will know your images ahead, it would be wise to download large, important updates such as service packs for Windows ahead of time and bring them in on a flash drive to be installed immediately- these large updates are the ones that will most likely give points. Ubuntu should upgrade to the latest version and update its software. Run updates in the background while you continue on.
3. Turn on User Account Control to the highest security setting. If you don't get points for it within a few minutes, feel free to turn it off because it gets really annoying.
4. Check users (Helpful to do through computer managements -> users and groups in Windows)
   1. Disable Guest account ya
   2. Change all passwords to something secure (8 characters, numbers, caps, symbols, ex. "R!verV13w")
   3. Make sure only accounts listed as admins in the readme are admins
   4. Remove users not listed anywhere in readme
5. Disable remote desktop/assistance (unless allowed in readme)
6. Remove unnecessary programs (add or remove programs in Windows)
   1. Remove server software, games, hacking tools, and other forbidden software (unless allowed in the readme)
7. Remove unnecessary Windows features (turn Windows features on or off)
   1. Remove games, IIS (Internet Information Services), media features, Telnet, etc. (unless allowed in the readme)
8. Remove unnecessary services (run -> services.msc)
   1. Anything "remote" except Remote Procedure Call (unless remote desktop/admin is allowed in the readme), Telnet, etc.
   2. If it doesn't have a description, then it's automatically on the chopping block. Search the name, if it's malicious or if nothing comes up then go properties -> general -> path to executable to find where it is running from. If you'll be disabling the service, you would also do well to delete the executable and probably its containing folder(s).
   3. DO NOT TOUCH DNS Client, Server, or anything else that seems essential to run the computer!
9. Change folder options
   1. Show hidden files, do not hide protected system files, do not hide extensions
10. Install useful stuff (download this beforehand)

1. Security Compliance Manager (http://technet.microsoft.com/library/cc677002.aspx) automatically sets those tedious security policies
2. Microsoft Security Essentials for basic antivirus
3. Glary Utilities (http://www.glarysoft.com/glary-utilities/download/) has some handy tools in the "advanced tools" menu including startup items, scheduled tasks, a processes list with user ratings (take with a grain of salt), and a software update checker (make sure a specific version of a program isn't required by the readme)

11. Turn on the firewall
    1. Specific ports to block or keep can be found on the ports page.
12. Remove unnecessary shares (computer management- IPC$, C$, and ADMIN$ cannot be removed)
13. Snoop through user files for prohibited files (programs, pictures, videos, music, etc.)
    1. Use wildcard searches to speed up this process- for example, searching for "*.mp3" will show all mp3 files on the computer. Make sure hidden files are shown in folder options, and make sure "search hidden files and folders" is enabled in the search menu!
    2. One way to find hacking tools such as John the Ripper or netcat is to search for "readme" as these tools usually come packed with one, and it is otherwise an uncommon file name. Searching for .exe's is less viable because of the sheer number included in Windows.
    3. Right click -> open containing folder is your friend!
    4. If all else fails, just manually look through all folders in a user's account folder.
14. Look at the file system in general. The temp folder, program files, and users folders are great places to find unnecessary or malicious files.

Retrieved from "http://riverview-cyberpatriot.wikia.com/wiki/General_Checklist?oldid=4121"

Categories: Add category

Great Shortcut: (info about computer)

Windows Button + Pause

Computer → Right mouse click → manage → shared folders → shares

should be 3:
Admin$
C$
IPC$

Ctrl + R

or

Windows button → search bar → Secpol.msc

Set policy use directions ("Set policies for a secure workstation")

If you kill a service with an "automatic" startup type.

↳ if you restart your computer it will just start up again

↳ then change its properties and startup type to disabled

Read the Read Me File — Usernames in the Read Me File are the ONLY valid usernames

Forensics Questions 2x points

turn on firewall easy points (kind of)

Do everything in the action center

Turn on User ~~Account~~ Account Control

Uninstall unnecessary software

Folder Icon → CyberPatriot → tools

helps

tools → Policy Template - run it = points

Make sure anti virus is installed and all

- Microsoft Security Essentials
  - After antivirus run malware bytes

To Firewall

- Control Panel
- Action Center
- Want to make everything green

(has to be on in competition)

+cyberpatriot

$af3tylst

Max

Mae
Anri
Di ane
Lyle
Ken
Luke

CyberPatriot - Vulnerabilities List - Found in past competitions		
Removed backdoor inside Winamp		W2k3 CP5 Rd3.5
Removed plaintext file with social security number, credit card numbers, TOP SECRET		W2K8Rd3
Removed prohibited media file (or prohibited video files) (avi, wmv, jpg, gif, bmp, mp3, mp4, wav,		Vista CP6 Rd2
Removed tinibackdoor running as svchost	Malware Bytes	
Removed Tinyweb web server running as svchost	Process Hacker	
ResEdit		CP7_Win8_Rd2
Sam Spade web crawler		CP7_Vista_Rd3
Search Protect browser hijacker removed		Win7 CP6 Rd1
Spy keylogger		
Superscan scanning tool		W2K8CP6State
VAF Music toolbar removed		Win7 CP6 Rd1
VNC Software		
Wireshark network monitor		CP7_Vista_Rd2
Zoomify PUP app		CP7_Win8_Rd2

Account/Local Security Policies

Issue	Notes
<Name> is no longer an Administrator	W2K8 / Vista /Ubuntu CP6 Rd2
<Name> password expires	CP7_Vista_Rd2
A minimum password length is required in the account policy	Vista Cp6 Rd2, Win8CP6Rd3
A password history is being kept for user accounts; A sufficient password history is being kept	W2k3 CP6 Rd1, W2K8&Win8Cp6Rd3
A secure maximum password age is sent	Win8CP6State
Allow system to be shut down without having to log on disabled	W2K3CP6Rd3
An account lockout threshold has been set	
Anonymous enumeration of SAM accounts and shares is disabled	W2k3 CP6 Rd1, Win8CP6Rd3
Autoplay has been completely disabled	Win8CP6Rd3
Ctl-Alt-Del set at login	
Everyone permissions no longer include anonymous users	Vista CP6 Rd2
File sharing disabled for the <name> folder	W2K8&Win8CP6Rd3
Former employee <name> account has been removed	

CyberPatriot - Vulnerabilities List - Found in past competitions

- Check program files directory
- control panel
add/remove software

Malware / Prohibited Software

Issue	**Tool used**	**Notes**
Abyss Web Server		
Advanced Port Scanner		
Aircrack sniffing tool		W2K8CP6State
AKProg keylogger (hidden process)		W2k3 CP6 Rd1
Angry IP Scanner		CP7_Win7_Rd3
Application Network Helper backdoor	Malware bytes	W2K8CP6 Rd3
Backdoor software		
cmd Autorun listener malware		CP7_Vista_Rd3
Cryptcat backdoor has been removed		W2K8 CP6 Rd2
Dark Comet RAT		CP7_Win8_Rd2
DealPly Adware removed		Win7 CP6 Rd1
Free Key Logger		
Http Web server software removed		Win8CP6Rd3
Hydra password cracker		UbuCP7Rd3
Java Update backdoor		CP7_Vista_Rd3
John the Ripper .POT = usually John the Ripper		
Keylogger = rvlkl.exe		Win8CP6Rd3
Metasploit Exploit Tool	Forensic Question	W2K8CP6State
Nectar toolbar		CP7_Win7_Rd3
Netbus Backdoor / Spyware		CP7_W2K8_Rd1
netcat backdoor (hidden in crss.exe for W2K3 image)	Ubuntu CP6 Rd2, W2k3 CP6 Rd1	
Nikto scanning software archive removed		Vista CP6 Rd2
Nmap setup file		W2K8Rd3
Nmap software archive removed		Vista CP6 Rd2
ntbindshell.exe backdoor	Malware bytes	W2k8 CP5 Rd2
Open TFTP server		CP7_Win7_Rd1
ophcrack password cracker		CP7_W2K8_Rd1
Password sniffer has been removed		W2K8 CP6 Rd2
Premier Opinion Service spyware		CP7_Vista_Rd2
PS3 Media Server		Win8CP6State

★ = get rid of 100% unless says keep

CyberPatriot - Vulnerabilities List - Found in past competitions

? = maybe get rid of.

Unnecessary Services & Applications

Issue	Notes
Abyss Web Server	CP7_W2K8_Rd1
? Apache Web server web server	Ubuntu CP6 Rd2
DNS Server	
Free SSD Service	Ubuntu CP6 Rd2
★ FTP Service	*suggested
ICS	aka - Web Server
? IIS (Internet Information Service)	
? InetPub	Win7 CP6 Rd1
IRC server has been removed (chatting)	CP7_Win7_Rd3
LPD service	UbuCP6Rd3
NFS server	CP7_Win7_Rd1
Open TFTP Server	W2K8 CP6 Rd2
RDP network level authentication enabled	CP7_Win7_Rd1
Remote Desktop sharing	Win7 CP6 Rd1
Remote registry services has been disabled	
RIP Listener Service	CP7_Win8_Rd2
RPC Locator	W2K8CP6State
Simple TCP/IP Services	UbuCP6Rd3
SMB server	
? SMTP for mail servers	Vista CP6 Rd2
SNMP Trap Service	*suggested
SSDP discover	Vista CP6 Rd2, Win7 CP6 Rd1
★ Telnet	
Terminal Services	W2K8 CP6 Rd2
TFTP server has been removed	*suggested
UPnP Device Host	UbuCP6Rd3
VNC server	CP7_Win7_Rd3
? Web Client service	*suggested
? WWW Publishing Service	

CyberPatriot - Vulnerabilities List - Found in past competitions

OS / Application Patching

Issue	Notes
Apache has been updated	Ubu CP6 Rd2&Rd3, W2k3 CP6 Rd1
Firefox has been updated	Win8CP6Rd3
Install updates from important security updates	Ubu CP6 Rd2
Majority of windows updates have been applied	W2K8 CP6 Rd2
MySQL has been updated	UbuCP6Rd3
OS check for updates daily	Ubu CP6 Rd2&Rd3
Windows automatically checks for updates	Vista CP6 Rd2
Windows Service Pack (#) is installed	W2K8/Vista CP6 Rd2, W2k3 CP6 Rd1
Windows Update Service is enabled and running	Win7 CP6 Rd1

Overall Security

Issue	Notes
Action Center items have all been configured	
Antivirus protection is enabled	
Applications may not bypass the secure desktop	Win8CP6State
Bitlocker drive encryption service is running	CP7_Win8_Rd2
DNS Zone transfers to any server is disabled	W2K8CP6State
Event log service is running (needed to turn it back on)	Vista CP6 Rd2
File sharing has been disabled	Win7 CP6 Rd1
Firewall has been enabled	Win8CP6 Rd3
Hosts file - bad entries have been removed	CP7_Vista_Rd3
Internet Explorer - Disabled download of unsigned Active X controls form restricted sites (update will set this OR go into Options - advanced)	CP7_Vista_Rd2
Remote Desktop sharing has been turned off	W2k3 CP6 Rd1
UAC escalation prompt has been enabled through action center/ -control panel [illegible] in the [illegible]	CP7_Win7_Rd1
UAC has been enabled	Win8CP6State
Unencrypted file containing users and passwords	W2k3 CP5 Rd3.5
Windows Server Backup has been installed	CP7_W2K8_Rd1

CyberPatriot - Vulnerabilities List - Found in past competitions

Guest account has been disabled	
Guest account has been secured	W2K8 / Vista CP6 Rd2
Last user name is no longer displayed when logging in	Vista CP6 Rd2
Limit use of blank passwords to console only	Vista CP6 Rd2
Logon required for system shutdown	CP7_W2K8_Rd1
No longer automatically logged in as administrator on recovery console	
NTLM hash is no longer stored on next password change	W2k3 CP6 Rd1
Password for user account <name> has been changed from default	
Remote access to CD Device is disabled	W2k3 CP6 Rd1
Removed unauthorized user <name>	W2K8 /Ubuntu /Vista CP6 Rd2
Restrict anonymous access to Named Pipes and Shares enabled	W2K8 CP6 Rd2, W2K8CP6Rd3
System can no longer be shutdown without logging in	W2K8 CP6 Rd2
UAC detect application installation and prompt for elevation setting enabled	Win8CP6Rd3
User <name>'s account is now password protected	W2K8/Vista CP6 Rd2
Users are no longer allowed to install print drivers	W2K8CP6Rd3
Users must type CTRL+ ALT + DEL before logging	CP7_W2K8_Rd1

Forensic Questions

Issue	**Notes**
A php backdoor has been installed on your system. What is the full path?	UbuntuCP6 Rd3
A reverse shell has been installed - it initiates an outgoing connection every minute. What IP address is the reverse shell attempting to communicate with?	Win8CP6 Rd3
A reverse shell is installed - what remote port number is it attempting to communicate with?	Win8CP6State
Character Encodings - identify types	CP7_Vista_Round2
Decrypt message using gpg4win application	CP7_Win7_Round3
Email - examine email.txt source file to find IP address of sender - then determine City	CP7_Win7_Round1
Find fingerprint for users public key	CP7_Win7_Round3
List the users allowed to configure printers	UbuCP6State
Someone was trying to guess their way into a user's account. Which user account were they trying to guess their way into?	W2K8 CP6 Rd3
Steganography using Open Puff	CP7_Vista_Round2
Using pictures, determine what city was visited	Win8CP6 Rd3
What port is backdoor listening on	CP7_Win7_Round3

Which user put the <malware file> in the <username> 's directory?	W2K8CP6State
Who deleted one of <username>'s files?	W2K8 CP6 Rd3

UBUNTU specific items

Issue	**Notes**
PHP has been updated	UbuCP6Rd3
The Linux kernel has been updated	UbuCP6Rd3
SSH root login has been disabled	UbuCP6State
SSH LolginGraceTime reduced to prevent DoS attacks	UbuCP6State
Automatic login is disabled	UbuCP6Rd3
MySQL remote access is disabled	UbuCP6Rd3
Inetd is disabled or removed	UbuCP7Exhibition
SYN cookies have been enabled	UbuCP7Exhibition
Anonymous samba access is disabled	UbuCP7Exhibition
Insecure root password has been changed	Ubuntu CP6 Rd2
Open SSL has been updated	UbuCP7Rd2
System is not vulnerable to shellshock	UbuCP7Rd2
Insecure sudo configuration has been fixed	UbuCP7Rd3
FTP anonymous upload disabled	UbuCP7Rd3
What groups is <name> a member of?	UbuCP7Rd3
What is IP address that an anonymous upload to the FTP server came from?	UbuCP7Rd3

Network:

Local Network:

- Lowest level of data is 1 bit.

- clients talk to servers

- end devices
  - phone etc,

- peer to peer networking
  - connected by one cable.

Router Configuration – commands needed for 10/11/2016 practice

NOTES FOR INSTRUCTIONS:

- This symbol < > means that it needs to be replaced with YOUR information. Do NOT type in those < > or what is inside them.
- There are examples - Do NOT type that information in, you must use the information specific to the lab you are working on.
- READ all the instructions before applying them to your lab

1. Log into router

-enable
-config t

Privileged EXEC mode–aka enable mode

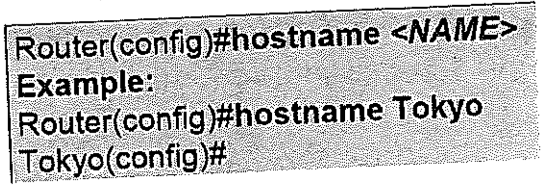
- access to all commands and sublevels
- to enter EXEC mode, use the ***enable*** command
- prompt = **Router#**

Configuration mode – aka config mode

- configure settings on router
- to enter config mode, use the **config t** command
- prompt = **Router(config)#**

2. Give the router a name (aka hostname)

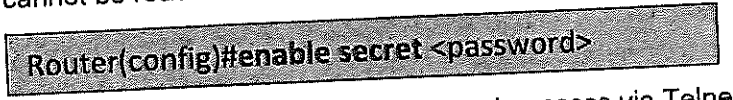
- default router name = Router
- giving router a unique name will help with network management and make router easy to identify remotely.



```
Router(config)#hostname <NAME>
Example:
Router(config)#hostname Tokyo
Tokyo(config)#
```

3. Put a passwords on the router

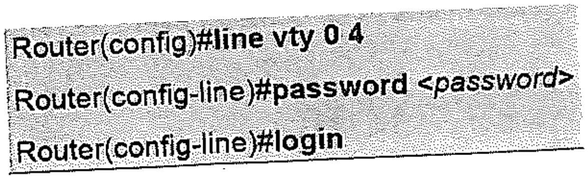
- Login password: use the ***enable secret*** command to set a login password that is encrypted and cannot be read or converted back to plain text.



```
Router(config)#enable secret <password>
```

(must use ***class*** as password for lab)

- Set password **vty lines** to restrict remote access via Telnet. WHAT IS A VTY?(Virtual TeletYpe) = Telnet sessions are known as virtual terminals -typically Older Cisco routers supported 5 VTY lines numbered 0 - 4, now they support 16 **numbered 0-15**



```
Router(config)#line vty 0 4
Router(config-line)#password <password>
Router(config-line)#login
```

4. Configure the Ethernet interfaces

Must have an IP address and subnet mask

1. Enter interface configuration mode
2. Specify the ipaddress and subnet mask **(use the info from the topology picture in the lab)**
3. Enable the interface

```
Router(config)#interface <interface nickname>
Router(config-if)#ip address  <ipaddress for that interface>  <subnet mask>
Router(config-if)#no shutdown
```

Type exit to get back to config mode

EXAMPLE:

```
Router(config)#interface e0
Router(config-if)#ip address 183.8.126.2  255.255.255.128
Router(config-if)#no shutdown
```

5. Set a login banner / Message of the Day

- This will post a message to anyone who logs onto your router
- Often used to post a "Keep Out" message
- Text of message must be enclosed by a # or ? sign on each end.

```
Router(config)# banner motd # Stay out – This means you! #
```

6. Configure a routing protocol

Use the command below **ONCE** on the router to tell it which routing protocol to use:

```
Router(config)# router rip
```

Then use the command below to tell it which interfaces that will participate in this routing – need to enter the **NETWORK ID** address for each network represented on your router.

```
Router(config-router)#network <network ID address>
```

← This MUST end in 0 !!!!

That means a command like the example below needs to be done for every NETWORK on your router.

```
Router(config-router)#network 172.16.0.0
```

To save your configuration work on the Router:

```
RBR# copy running-config startup-config
```

OR

RBR# copy run start

y (yes)

To Use telnet

- used for remote connection for configuration and management
- maximum of 5 simultaneous Telnet sessions on one router
- also used to test connectivity

```
To start a Telnet session, any of these can be used:
Router>telnet Net2
Router>Net2
Router>connect Net2
Router>131.109.100.152

*need a host table or DNS server to use a name
```

Disconnect from Telnet

- if inactive for 10 minutes, will terminate automatically
- To disconnect:
  - **Router>disconnect Net2**

To check on your router try these commands

- View of what you have configured on the device

RBR# show run

- Quick view of interface IP settings and status

RBR# show ip interface brief

The 'show' command will help you if you ask. Just type ? after show -- it will give a list of words that can come after. Then keep adding to the command and put a ? afterwards, it will keep giving you tips as to what can come next.

RBR# show ?
RBR# show ip ?
RBR# show ip arp

Carter

CyberPatriot Competition Checklist

Manual	Automated
☑ Read the Read Me file – highlight, take notes	□ User Rights – update registry
☑ Answer Forensics Question(s)	□ MalwareBytes for malware
☑ Turn on Firewall	□ Automatic Updates – download and install
☑ Action Center	□ AV scan
☑ User Account Control	
☑ Secure Users and Groups (Guest/Admin, etc.)	
☑ Passwords for accounts	
□ Password Policies	
□ Remove/Disable Insecure Services	
□ Local Security Policy (if not by .inf file)	
□ Update appropriate software	
☑ Uninstall unnecessary software	
□ Search for inappropriate files – media, hack tools, etc.	
□ Secure File and Directory shares	
□ Check Open Ports	
□ Check for Anti-Virus Program	
□ Check for abnormal behavior	

Ensure you are not rebooting the machine for updates with less than an hour to go!

Document each and every action you perform – whether the setting works or not.

Trying to open ReadMe

Turned on firewall in action center
Deleted Public and another invalid user

Users

ascott ✓
ballen ✓
bwayne ✓
dgarret ✓
enatchios ✓
mmurdock ✓
pparker ✓
ssummers ✓
tstark ✓

Admins

cxavier
Windows p - (blank/none)
Linux p: ~~mutants51;fe~~
mutants51;fe

diana
p: Justice7

password: ZQ74DL829KOW38

Kerberos Policy

Max lifetime for user ticket = 16
Enfore user ligon restrictions = Enabled
Max lifetime for user ticket renewal = 7 days
Maximum tolerance for computer clock sync = 5 min

→ mmc
→ add snap in Security Template
→ New template
  → Name it
→ Configure
→ Save as

→ See CP worksheet

.inf additional parts (System Services)

Disabled	Enabled
SSDP Discovery	Windows Defender Service + Network I.S.
UPnP Device Host	Firewall
Windows Remote Management	
SNMP	
RPC Endpoint Mapper	
RPC Locator	
RPC	

*If CP with RDP service, be prepared to make manual adjustments *

Changed in Security Options

Restrict CD-ROM access → Enabled
Floppy → Enabled

Display user info → display name only

Didn't do (Other services that weren't listed)

RDS
net.TCP Port Sharing

RBR 6

Team number: 11-4438	**Team Unique ID: 47M3-3VX5-C4MK**
Cisco Login: 114438cp	**Cisco Password: 47M3-3VX5-C4MKcp**

Steps for Competition opening

1. Righclick on the zipped image file. Select 7zip --> extract files to "name_of_image"
2. The password to extract the images is: on the other paper I handed you
3. When the image is unzipped, go into folder and find the file that ends with .vmx -- it will have 3 blue overlapping squares as an icon. Doubleclick to start opening.
4. When asked selected "I copied it". If there are any other prompts, just say yes or ok EXCEPT for updating Vmware. Say later or never or no - just don't update.
5. Once the image is open, enter your team unique identifier.
6. Open the scoring report to make sure you can access the score server
7. Open the README file and find out the details of the image
8. Read the Forensics questions and try to answer first.
9. Start entering information in the Documentation Server so that you will have a record of the steps you took.
10. START WINNING!

Steps for CISCO quiz and Packet Tracer

-- Instructions are in our CyberPatriot Google Classroom

Steps for Competition closing

1. **Full Screen Capture of the Scoring Page.** If the screen capture of the scoring page is cut off or modified, it will not be considered in the appeal. The screen capture must be easily readable and include:

- CyberPatriot Logo - Report Generated Time - Current Unique Identifier
- Known Issues Fixed - Penalties Assessed - Score
- Copyright Information - Connection Status

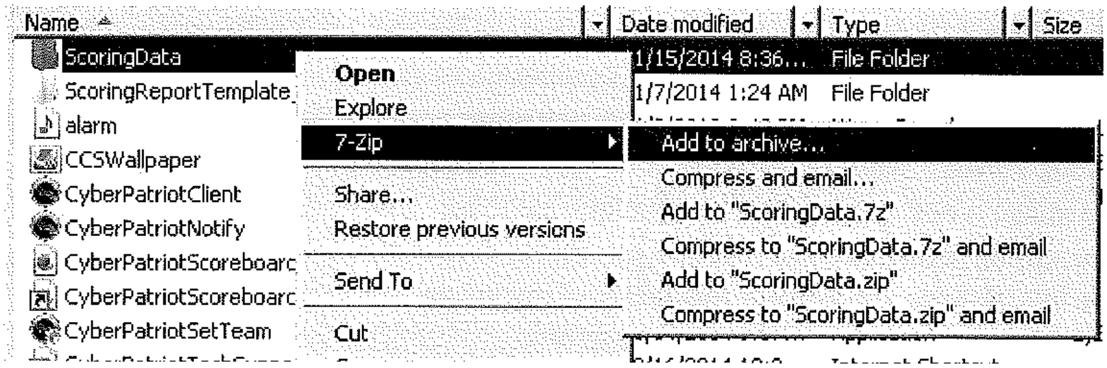
Save this labeled as <TeamName>ScoreReport.jpg – Uploaded to Google Classroom

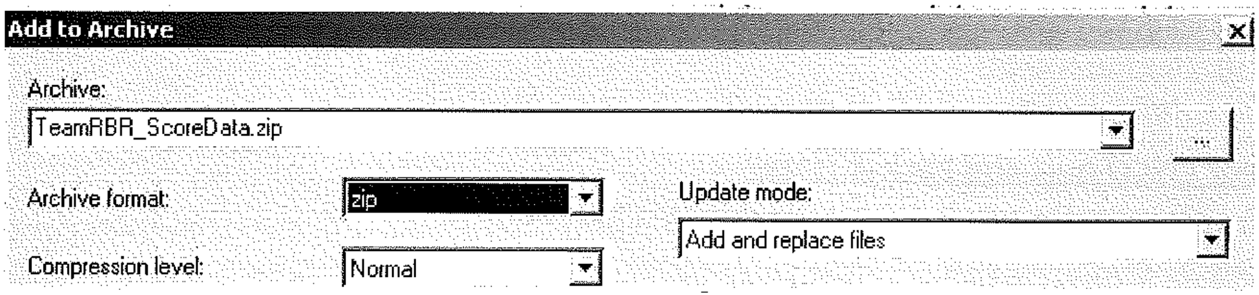
2. **Word document copy of score report data** - go into the score report and copy all the text - easiest to do by click Ctrl-A - then rightclick Copy. On your host laptop, open a Word document and paste the score report into that document. **Save as <TeamName>ScoreReport.doc - Uploaded to Google Classroom**

3. Backing Up Scoring Data

To back up scoring data on a Windows image:

- In the image, navigate to C:\CyberPatriot\ScoringData
- Right click on the folder - from the menu, select 7Zip
- From the menu, select "Add to archive" - label
- Copy the ENTIRE contents and compress copied files to a .zip file labeled as <TeamName>ScoreData.zip
- **Copy .zip file to your host machine desktop AND Uploaded to Google Classroom**





Archive: TeamRBR_ScoreData.zip

Archive format: zip

Compression level: Normal

Update mode: Add and replace files

To back up scoring data on an Ubuntu image:

- Navigate to \opt\CyberPatriot\ScoringData.
- Copy the ENTIRE contents of this directory to your host desktop
- Use 7Zip on the host machine (see above) to compress the folder into a .zip file labeled as <TeamName>ScoreData.zip
- **Copy the .zip file to your host machine desktop AND Uploaded to Google Classroom**