This could even lead to a total compromise of the system. Limiting network access to only critical
network services and essential system functions is an important part in mitigating the attack surface available to and adversary.

2) Forensics Question 2 Correct

• How do I find this problem?

When you open an image, please read all the "Forensics Questions" thoroughly before modifying
the image as you may change something that prevents you from answering the question correctly.
There is a file on the Desktop here named "Forensics Question 2”.

• How do I solve this problem?

This question asks you to find the SHA256 sum of the file on the desktop named jarlsberg.png. While holding down the Shift key, right-click on the Desktop in an empty space and select Open PowerShell window here. In the PowerShell window type Get-FileHash -Algorithm SHA256 .\jarlsberg.png and press Enter.
The answer to this question is located under Hash. Remember to Save and close the file.

• Why is fixing this problem important?

It’s important to know what hash functions are and how they can be used. Hash functions, when used correctly, can be used to verify the integrity of files, ensuring they have not been modified by an adversary. Hash functions are one-way functions that rely on 4 main properties for security:
pre-image resistance, second pre-image resistance, collision resistance, and pseudo-randomness.
Hash functions have many uses in cryptography including playing an important role in digital signatures and encryption algorithms.

3) Removed unauthorized user ancano

• How do I find this problem?

One of the first things you should do when starting an image during a competition is check the README file on the desktop. The authorized administrators and users listed in the README are
the only users that should exist on the system (aside from legitimate built-in system accounts and
those used for services). All unauthorized user accounts should be removed.

• How do I solve this problem?

Press the Windows key + R to open the Run dialog. In the Run dialog type lusrmgr.msc and press Enter to open the Local Users and Groups. Click Users on the left side of the window. Rightclick on anacano and select Delete. In the resulting dialog box click Yes to confirm that you want to delete the user.

• Why is fixing this problem important?

Computer access should be limited to just those who need to use it to complete their tasks. By leaving unauthorized user accounts on the image, unauthorized individuals may be able to log on
to the computer and make changes that could affect the safety and security of legitimate users.

Unauthorized user accounts also give adversaries a greater attack surface. For example, unauthorized user accounts increase the risk of having a user account compromised via password
cracking.
4) Removed unauthorized user tolfdir
• How do I find this problem?
One of the first things you should do when starting an image during a competition is check the README file on the desktop. The authorized administrators and users listed in the README are
the only users that should exist on the system (aside from legitimate built-in system accounts and
those used for services). All unauthorized user accounts should be removed.
• How do I solve this problem?
Press the Windows key + R to open the Run dialog. In the Run dialog type lusrmgr.msc and press Enter to open the Local Users and Groups manager. Click Users on the left side of the window. Right click on tolfdir and select Delete. In the resulting dialog box click Yes to confirm that
you want to delete the user.
• Why is fixing this problem important?
Computer access should be limited to just those who need to use it to complete their tasks. By leaving unauthorized user accounts on the image, unauthorized individuals may be able to log on
to the computer and make changes that could affect the safety and security of legitimate users. Unauthorized user accounts also give adversaries a greater attack surface. For example, unauthorized user accounts increase the risk of having a user account compromised via password
cracking.
5) User lydia is not an administrator
• How do I find this problem?
One of the first things you should do when starting an image during a competition is check the README file on the desktop. The authorized administrators listed in the README are the only users that are authorized have administrator level access. All users not in the list of authorized administrators should have their administrator level access removed.
• How do I solve this problem?
Press the Windows key + R to open the Run dialog. In the Run dialog type lusrmgr.msc and press Enter to open the Local Users and Groups manager. Click Groups on the left side of the window. Double-click on Administrators to open a Properties window. Select lydia and click Remove, then click OK to apply the changes and close the Properties window.
• Why is fixing this problem important?
Administrator level access gives individuals the ability to modify critical system files and functions
and should be limited to authorized individuals only. The more users with administrator level access, the higher your risk, since compromising an account with administrator level access gives

an adversary complete control of the system.
6) User balgruuf has a password
• How do I find this problem?
Ensuring users have strong passwords is an important principle of cybersecurity. Users with no passwords can be found by looking at User Accounts under the Control Panel.
• How do I solve this problem?
Press the Windows key + R to open the Run dialog. In the Run dialog type control and press Enter to open the Control Panel. In the Control Panel, click User Accounts, then click Manage another account. Note that the description under balgruuf does not say Password protected. Click balgruuf, then click Create a password. Choose a secure password and type it into the New
password and Confirm new password text boxes, and click Create password.
• Why is fixing this problem important?
Not having a password on an account will allow an adversary with physical access to the machine
to log in without a password. In some cases, this can also allow an adversary to log in over the network without a password.
7) A secure maximum password age exists
• How do I find this problem?
Enforcing industry recommended password policies is good cybersecurity practice.
• How do I solve this problem?
Press the Windows key + R to open the Run dialog. In the Run dialog type secpol.msc and press Enter to open the Local Security Policy. Navigate to Security Settings Account Policies Password Policy. Double-click on Maximum password age. Set the password to expire in 90 days.
• Why is fixing this problem important?
Setting a maximum password age limits your risk of having a password compromised and can help
mitigate the damage if a password is compromised. When an adversary obtains password hashes
or performs a brute force attack, they can obtain your password given enough time.
Changing your passwords regularly can limit the risk of an adversary obtaining your password.
8) Store passwords using reversible encryption [Disabled]
• How do I find this problem?
Enforcing industry recommended password policies is good cybersecurity practice.
• How do I solve this problem?
Press the Windows key + R to open the Run dialog. In the Run dialog type secpol.msc and press Enter to open the Local Security Policy. Navigate to Security Settings Account Policies Password Policy. Double-click on Store passwords using reversible encryption and click Disabled and Apply .
• Why is fixing this problem important?
Storing passwords on the system with reversible encryption could allow an attacker to obtain the encrypted hash value and decrypt it to obtain your actual password.
9) A secure lockout threshold exists

• How do I find this problem?
Enforcing industry recommended account lockout policies is good cybersecurity practice.
• How do I solve this problem?
Press the Windows key + R to open the Run dialog. In the Run dialog type secpol.msc and press Enter to open the Local Security Policy. Navigate to Security Settings Account Policies Account Lockout Policy. Double click on Account lockout threshold. Set the account lockout threshold to 10 invalid logon attempts.
• Why is fixing this problem important?
Setting secure account lockout policies limits your risk of having a password compromised. When
an adversary performs a brute force attack this will stop or slow down their attack, greatly increasing the time required to compromise a user account.
10) A secure account lockout observation window exists
How do I find this problem?
Enforcing industry recommended account lockout policies is good cybersecurity practice.
How do I solve this problem?
Press the Windows key + R to open the Run dialog. In the Run dialog type secpol.msc and press Enter to open the Local Security Policy. Navigate to Security Settings Account Policies Account Lockout Policy. Select Account Lockout Duration click on the arrow to set the number of minutes. At least 4 minutes is recommended.
Why is fixing this problem important?
Setting secure account lockout policies limits your risk of having a password compromised. When
an adversary performs a brute force attack this will stop or slow down their attack, greatly increasing the time required to compromise a user account.
11) Limit local use of blank passwords to console only [enabled]
• How do I find this problem?
Enforcing industry recommended security options is good cybersecurity practice.
• How do I solve this problem?
Press the Windows key + R to open the Run dialog. In the Run dialog type secpol.msc and press Enter to open the Local Security Policy. Navigate to Security Settings Local Policies Security Options. Double-click on Accounts: Limit local account use of black passwords to console logon only to bring up a Properties menu. Select Enabled and click OK to apply the setting and close the Properties window.
• Why is fixing this problem important?
Allowing users without a password to log in over the network is a severe security risk. Any users that do not have a password will immediately have their account compromised by an adversary attempting to log in over the network.
12) Do not allow anonymous enumeration of SAM accounts and shares [enabled]
• How do I find this problem?
Baseline hardening is the process of applying a standard set of security configurations and best practices to a system. Security practices such as baseline hardening requires you to review security policies on the system to ensure that they are set to the industry standard.
• How do I solve this problem?

Press the Windows key + R to open the Run dialog. In the Run dialog type secpol.msc and press Enter to open the Local Security Policy. Navigate to Security Settings Local Policies Security Options. Double-click on Network access: Do not allow anonymous enumeration of SAM accounts and shares to bring up a Properties menu. Select Enabled and click OK to apply
the setting and close the Properties window.

• Why is fixing this problem important?

Preventing anonymous enumeration of SAM accounts and shares prevents attackers from easily
learning about user accounts and resources on your system such as usernames and contents of
shared folders.

13) Audit Security State Change [Success]

• How do I find this problem?

I Baseline hardening is the process of applying a standard set of security configurations and best
practices to a system. Security practices such as baseline hardening requires you to review local
policies on the system to ensure that they are set to the industry standard.

• How do I solve this problem?

Press the Windows key + R to open the Run dialog. In the Run dialog type secpol.msc and press Enter to open the Local Security Policy. Navigate to Security Settings Local Policies > Advanced Audit Policy Configuration > System Audit Policies – Local Group Policy Object > Policy
Change > System . Double-click Audit Security State Change. Check the boxes Configure the following audit events: and Success. Click Apply.

• Why is fixing this problem important?

Auditing security state changes on the system allow the security team to investigate after an attack and use the information to better secure the system in the future.

14) Firewall protection has been enabled

• How do I find this problem?

In the search bar, search “Control Panel” and select the Control Panel Desktop app option that appears. In the control panel, select Windows Defender Firewall to view the status of the firewall.

If you select the arrow to open the drop-down under Private networks or Guest or public networks, “Windows Defender Firewall state: Off” will be showing as one of the fields.

• How do I solve this problem?

In Windows Defender Firewall, select “Turn Windows Defender Firewall on or off”. You will see that the firewall is turned off in both the Private and Public network settings. Select “Turn on Windows Firewall” under Private network settings. Select the same option under Public network settings. Select “OK” to save the changes.

• Why is fixing this problem important?

Windows Defender Firewall is a security feature that protects your computer from threats that come from outside of your organization’s network. Enabling and properly configuring a firewall is

critical to ensuring that you are only allowing known, authorized traffic in and out of your computer.

15) Windows automatically checks for updates

• How do I find this problem?

It is important to keep your operating system updated to receive the latest security improvements. Search “update” in the search bar and select the option “Check for updates”. Select “Advanced Options” and “View configured update policies”. Under “Policies set on your device”, you will notice the policy “Disable automatic updates”.

• How do I solve this problem?

Press the Windows key + R to open the Run dialog. In the Run dialog type gpedit.msc and press Enter to open the Local Group Policy Editor. Under computer configuration, select the “Administrative Templates” folder and then the “Windows Components” folder. Under the “Windows Components” folder, scroll down to find the “Windows Update” folder. In the settings that appear on the right panel, you will see the setting “Configure Automatic Updates” set as Disabled. Double-click on the setting and select “Enabled”. Then, select “Apply” and “OK”.

• Why is fixing this problem important?

Keeping your operating system updated allows you to have the newest security features on your system. Updates also contain patches for vulnerabilities on your operating system.

16) File share greybeard disabled

• How do I find this problem?

It’s important to know what files and directories are being shared over the network.

• How do I solve this problem?

Press the Windows key + R to open the Run dialog. In the Run dialog type fsmgmt.msc and press Enter to open Shared Folders. Click Shares on the left side of Shared Folders. Right-click on
greybeard and select Stop Sharing. Click Yes to confirm that you want to stop sharing greybeard.

• Why is fixing this problem important?

Unauthorized file shares are a security vulnerability. The C$, ADMIN$, and IPC$ shares are default
administrative shares created automatically by Windows. Microsoft does not recommend disabling the administrative shares.

17) File share disabled for C drive

• How do I find this problem?

It’s important to know what files and directories are being shared over the network.

• How do I solve this problem?

Open File Explorer and right-click on Local Disk (C:). Navigate to Properties > Sharing > Advanced
Sharing. Uncheck the box that says Share this folder and click Apply.

• Why is fixing this problem important?

Unauthorized file shares are a security vulnerability. The C$, ADMIN$, and IPC$ shares are default
administrative shares created automatically by Windows. Microsoft does not recommend disabling the administrative shares.

18) Simple Mail Transfer Protocol (SMTP) service has been stopped and disabled

• How do I find this problem?

It is important to know which services are running on your computer. You can see the status of all
of the services on your computer by checking the services app.

• How do I solve this problem?

Press the Windows key + R to open the Run dialog. In the Run dialog type services.msc and press
Enter to open the Services app. Scroll down to find the Simple Mail Transfer Protocol (SMTP) service. Double click on the service to open the service Properties. The Startup type is currently set to Automatic. In the drop-down menu, select Disabled. Select Apply, Start, then OK.

• Why is fixing this problem important?

It is best practice to turn off SMTP if you don't need it. Since SMTP sends email, leaving it on gives
attackers another possible way to use your server to send spam or access information.

19) FTP service has been stopped and disabled

How do I find this problem?

Stopping and disabling insecure or unnecessary services is an important principle of good cybersecurity. Many services need to be running to ensure normal and secure operation of computer systems. Reading about the services on your system and doing research can help you
determine the importance of a service and if it is necessary for normal operation. Additionally, business critical services listed in the README should remain running at all times. The Services management console lists all services, their startup type, and their current status.

• How do I solve this problem?

Press the Windows key + R to open the Run dialog. In the Run dialog type services.msc and press Enter to open Services. Scroll down and double-click on Microsoft FTP Service to open a Properties window. Change the Startup type to Disabled to prevent the service from starting automatically, then click Stop to stop the service. Click OK to apply the changes and close the Properties window.

• Why is fixing this problem important?

Disabling unnecessary services can limit your attack surface. The fewer services an adversary has to
attack and potentially exploit, the lower your risk. Adversaries may attack known or unknown vulnerabilities in services to obtain information, escalate privileges, or gain unauthorized access.

20) Firefox has been updated

• How do I find this problem?

Updating installed applications and services to fix security vulnerabilities is an important principle
of good cybersecurity.

• How do I solve this problem?

Open Firefox and click the menu button near the upper right corner of the Firefox window. Click Help, then About Firefox. Click Update to update Firefox.

• Why is fixing this problem important?

When security vulnerabilities are found in software, the software vendor publishes updates that patch the security vulnerabilities. Adversaries can more easily compromise your system if software is present that has known security vulnerabilities. Ensuring software is up to date removes known security vulnerabilities.

21) Removed BitTorrent

• How do I find this problem?

Removing unauthorized and potentially unwanted programs from a computer is an important cybersecurity principle. Third party software installed on the system should be limited to the software listed in the README, and software required for normal operation of the operating system and services.

• How do I solve this problem?

Press the Windows key + R to open the Run dialog. In the Run dialog type control and press Enter to open the Control Panel. In the Control panel click Programs and Features. Click BitTorrent, then click Uninstall. Follow the prompts to ensure that BitTorrent is completely uninstalled.

• Why is fixing this problem important?

Removing unauthorized software from your system is important for limiting your risk and reducing
your attack surface. Unauthorized programs may leak confidential information, interfere with business-critical software and services, contain various malware and security vulnerabilities, or could introduce unwanted legal and regulatory issues.

22) Removed Wireshark

• How do I find this problem?

Removing unauthorized and potentially unwanted programs from a computer is an important cybersecurity principle. Third party software installed on the system should be limited to the software listed in the README, and software required for normal operation of the operating system, and services and software listed in the README.

• How do I solve this problem?

Press the Windows key + R to open the Run dialog. In the Run dialog type control and press Enter to open the Control Panel. In the Control panel click Programs and Features. Click Wireshark, then click Uninstall. Follow the prompts to ensure that Wireshark is completely uninstalled.

• Why is fixing this problem important?

Removing unauthorized software from your system is important for limiting your risk and reducing
your attack surface. Unauthorized programs may leak confidential information, interfere with business-critical software and services, contain various malware and security vulnerabilities, or could introduce unwanted legal and regulatory issues.

23) Removed Brutus password cracker archive

• How do I find this problem?

Removing unauthorized and potentially unwanted files and software from a computer is an important cybersecurity principle. Third party software installed on the system should be limited to the software listed in the README, and software required for normal operation of the operating system, and services and software listed in the README.

• How do I solve this problem?
Open File Explorer from the bottom task bar. Navigate to Local Disk (C:) > Users > Public > Public
Downloads. Right-click the file names brutus-aet2-darknet.zip file and select Delete from the drop-down menu.
• Why is fixing this problem important?
Removing unauthorized files and software from your system is important for limiting your risk and
reducing your attack surface. Unauthorized programs may leak confidential information, interfere
with business-critical software and services, contain various malware and security vulnerabilities,
or could introduce unwanted legal and regulatory issues.
Penalties
1) Account lockout policy less than 5 is deprecated: -4 pts.
• Why is this a penalty?
Setting the account lockout threshold is an important security precaution to prevent brute force password cracking. The threshold should be set between 5 and 50 failed logon attempts. A threshold of under 5 is too few and may result in valid users accidentally locking themselves out of their accounts, or adversaries easily being able to perform a denial-of-service attack and locking
users out of their accounts.
2) Remote Desktop is disabled: -5 pts.
• Why is this a penalty?
The README states that Remote Desktop is a critical service.
3) Firefox is not installed at the default location: -5 pts.
• Why is this a penalty?
The README states that Firefox is required software.