

Blue Team Level 1 Certification
(Standard)

4 Topics

Lab and Forum Access

SECURITY FUNDAMENTALS DOMAIN

Introduction to Security Fundamentals

1 Topic

Soft Skills

7 Topics

Security Controls

5 Topics 1 Quiz

Networking 101

6 Topics 1 Quiz

Management Principles

4 Topics 1 Quiz

PHISHING ANALYSIS DOMAIN

PA1) Introduction to Emails and Phishing

7 Topics 1 Quiz

PA2) Types of Phishing Emails

10 Topics 2 Quizzes

PA3) Tactics and Techniques Used

12 Topics 2 Quizzes

PA4) Investigating a Phishing Email

8 Topics 2 Quizzes

PA5) Analysing URLs, Attachments, and Artifacts

8 Topics 1 Quiz

PA6) Taking Defensive Actions

12 Topics 1 Quiz

PA7) Report Writing

7 Topics 1 Quiz

PA8) Phishing Response Challenge

3 Topics 1 Quiz

THREAT INTELLIGENCE DOMAIN

TI1) Introduction to Threat Intelligence

7 Topics

TI2) Threat Actors & APTs

6 Topics 2 Quizzes

TI3) Operational Threat Intelligence

7 Topics 1 Quiz

TI4) Tactical Threat Intelligence

7 Topics 1 Quiz

TI5) Strategic Threat Intelligence

5 Topics 1 Quiz

TI6) Malware and Global Campaigns

6 Topics 1 Quiz

DIGITAL FORENSICS DOMAIN

DF1) Introduction to Digital Forensics

5 Topics

DF2) Forensics Fundamentals

10 Topics 5 Quizzes

DF3) Digital Evidence Collection

8 Topics 1 Quiz

Identifying and Removing Malicious Artifacts

Blue Team Level 1 Certification (Standard) > IR4) Containment, Eradication, and Recovery Phas...

IN PROGRESS

Incident Response Domain REMOVING MALICIOUS ARTIFACTS



There are a number of different actions we can take when working to identify and remove malicious artifacts, but alternatively, there are some easy 'quick wins' to completely remediate the incident or infection immediately. In this lesson we will cover the following:

- What are malicious artifacts?
- Identifying artifacts.
- Removing artifacts.

WHAT ARE MALICIOUS ARTIFACTS?

The term 'malicious artifact' is used to describe some object with malicious purposes, such as a piece of malicious software (malware) that is installed on a system, a running process, a scheduled task, a registry entry, a text file generated by a keylogger, etc. We need to ensure that we remove all malicious artifacts during the incident response process, because if we miss something, the attackers may still have some degree of control over the system. If they're using a backdoor to allow for remote access and we miss it, even if the system is patched and hardened, they have a direct route in.

IDENTIFYING ARTIFACTS

This is often a case of experience in dealing with incidents, being able to identify what items should and shouldn't be on a system. However, there are some places we can look to see if anything looks suspicious, such as active network connections, user accounts, file downloads, running processes, scheduled tasks, and registry entries.

There are some manual checks we can conduct to try and identify suspicious activity, allowing us to find and remove artifacts. Some examples include:

- Check for suspicious or unknown processes running in the system. For Windows systems, Sysinternals' [Process Explorer](#) is a very powerful task manager that can show processes that try to mask themselves as ordinary system processes.
- To determine the source of suspicious network connections, the netstat utility and Sysinternals' [Process Monitor](#) are an excellent combination to help track down malware that is attempting to "call home" or attempting to spread.
- Another tool from Sysinternals, the [Rootkit Revealer](#), is very useful in detecting Rootkits or malware that uses advanced techniques in order to mask its presence on a system.

REMOVING ARTIFACTS

Below are different methods we can use to remove malicious artifacts that we have identified during the incident response process.

DF4) Windows Investigations

3 Topics 3 Quizzes

DF5) Linux Investigations

4 Topics 2 Quizzes

DF6) Volatility

3 Topics 1 Quiz

DF7) Autopsy

4 Topics 1 Quiz

SECURITY INFORMATION AND EVENT MANAGEMENT DOMAIN

SI1) Introduction to SIEM

7 Topics 1 Quiz

SI2) Logging

6 Topics 2 Quizzes

SI3) Aggregation

2 Topics 1 Quiz

SI4) Correlation

6 Topics 1 Quiz

SI5) Using Splunk

5 Topics 2 Quizzes

INCIDENT RESPONSE DOMAIN

IR1) Introduction to Incident Response

8 Topics 1 Quiz

IR2) Preparation Phase

10 Topics 2 Quizzes

IR3) Detection and Analysis Phase

7 Topics 4 Quizzes

IR4) Containment, Eradication, and Recovery Phase

5 Topics 1 Quiz

Section Introduction, CER

Incident Containment

Taking Forensics Images

Identifying and Removing Malicious Artifacts

Identifying Root Cause and Recovery

Activity) End of Section Review, CER

IR5) Lessons Learned and Reporting

7 Topics

IR6) MITRE ATT&CK

13 Topics 2 Quizzes

BTL1 EXAM

Exam Preparation

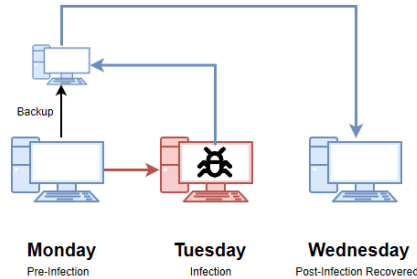
Using RDP and SSH

How to Start Your Exam

Response process

Reimaging Affected Systems

One of the easiest ways to completely recover a system from any kind of infection is to reimage it from a backup. In the below diagram, we've demonstrated how incident responders can remove **all** malicious artifacts in one go, ensuring the system is completely clean, provided there is a backup before the infection occurs. The downside with this method is that all data after the pre-infection backup was taken will be lost.



Anti-Malware Solutions

We can scan affected systems with a high-grade Antivirus solution, preferably a Next-Generation Antivirus solution, to ensure that malicious artifacts are identified and removed from the system. This may not always be a good solution, in the event of a malware infection, if the antivirus didn't detect the malware to start with it may struggle to find associated malicious artifacts. Next-Generation AV might be more useful here, as it doesn't take the same approach of traditional antivirus methods that are often beaten by knowledgeable attackers, but what's the difference? It goes beyond known file-based malware signatures and heuristics and can utilize predictive analytics powered by machine learning and artificial intelligence to detect file-less malware that hides in memory, and respond to new threats that would normally go undetected. In all cases we should ensure the endpoint solution is enabled, properly configured, and has the latest updates and signatures to increase the chance of successful detection. In the case of an advanced malware infection, it is likely better to proceed with the re-imaging method of removing artifacts.

Bootable Tools

Some antimalware vendors offer tools or versions of their products that don't require installation and can be run from a CD or USB drive in order to prevent them from being affected by malware residing on the system. For example:

- McAfee provides the stand-alone [Stinger Malware removal tool](#) and Microsoft has the [Malicious Software Removal Tool](#), for detecting and removing specific malware.
- Avira offers the "[Avira Rescue System](#)", designed to be booted and run from a CD or USB drive.

< Previous Topic

Mark Complete ✓

Back to Lesson

Next Topic >

Privacy & Cookies Policy

