Preparation Stage (Part 2)

Another part of the preparation stage is to protect against incidents. While protection is not necessarily the responsibility of an incident handling team, any protection-related activities should be known to them to better understand the type and sophistication of an incident and know where to look for artifacts/evidence, that could aid the investigation.

Let us now look at some of the highly recommended protective measures, which have a high mitigation impact against the majority of threats.

DMARC

DMARC is an email protection against phishing built on top of the already existing SPF and DKIM. The idea behind DMARC is to reject emails that 'pretend' to originate from your organization. Therefore, if an adversary is spoofing an email pretending to be an employee asking for an invoice to be paid, the system will reject the email before it reaches the intended recipient. DMARC is easy and inexpensive to implement, however, I cannot stress enough that thorough testing is mandatory; otherwise (and this is oftentimes the case), you risk blocking legitimate emails with no ability to recover them.

With email filtering rules, you may be able to take DMARC to the 'next' level and apply additional protection against emails failing DMARC from domains you do not own. This is possible because some email systems will perform a DMARC check and include a header stating whether DMARC passed or failed in the message headers. While this can be incredibly powerful to detect phishing emails from any domain, it requires extensive testing before it can be introduced in a production environment. High false-positives here are emails that are sent 'on behalf of' via some email sending service, since they tend to fail DMARC due to domain mismatch.

Endpoint Hardening (& EDR)

Endpoint devices (workstations, laptops, etc.) are the entry points for most of the attacks that we are facing on a daily basis. If we consider the fact that most threats will originate from the internet and will target users who are browsing websites, opening attachments, or running malicious executables, a percentage of this activity will occur from their corporate endpoints.

There are a few widely recognized endpoint hardening standards by now, with CIS and Microsoft baselines being the most popular, and these should really be the building blocks for your organization's hardening baselines. Some highly important actions (that actually work) to note and do something about are:

- Disable LLMNR/NetBIOS
- Implement LAPS and remove administrative privileges from regular users
- Disable or configure PowerShell in "ConstrainedLanguage" mode
- Enable Attack Surface Reduction (ASR) rules if using Microsoft Defender
- Implement whitelisting. We know this is nearly impossible to implement. Consider at least blocking execution from user-writable folders (Downloads, Desktop, AppData, etc.). These are the locations where exploits and malicious payloads will initially find themselves. Remember to also block script types such as .hta, .vbs, .cmd, .bat, .js, and similar. Please pay attention to LOLBin files while implementing whitelisting. Do not overlook them; they are really used in the wild as initial access to bypass whitelisting.
- Utilize host-based firewalls. As a bare minimum, block workstation-to-workstation communication and block outbound traffic to LOLBins
- Deploy an EDR product. At this point in time, AMSI provides great visibility into obfuscated scripts for antimalware products to inspect the content before it gets executed. It is highly recommended that you only choose products that integrate with AMSI.

When it comes to hardening, Don't let perfect be the enemy of good.

Network Protection

Network segmentation is a powerful technique to avoid having a breach spread across the entire organization.

? Go to Questions

Table of Contents

Introduction

Incident Handling

Cyber Kill Chain

The Incident Handling Process

Incident Handling Process Overview

Preparation Stage (Part 1)

Preparation Stage (Part 2)

Detection & Analysis Stage (Part 1)

Detection & Analysis Stage (Part 2)

Containment, Eradication, & Recovery Stage

Post-Incident Activity Stage

Business-critical systems must be isolated, and connections should be allowed only as the business requires. Internal resources should really not be facing the Internet directly (unless placed in a DMZ).

Additionally, when speaking of network protection you should consider IDS/IPS systems. Their power really shines when SSL/TLS interception is performed so that they can identify malicious traffic based on content on the wire and not based on reputation of IP addresses, which is a traditional and very inefficient way of detecting malicious traffic.

Additionally, ensure that only organization-approved devices can get on the network. Solutions such as 802.1x can be utilized to reduce the risk of bring your own device (BYOD) or malicious devices connecting to the corporate network. If you are a cloud-only company using, for example, Azure/Azure AD, then you can achieve similar protection with Conditional Access policies that will allow access to organization resources only if you are connecting from a company-managed device.

Privilege Identity Management / MFA / Passwords

At this point in time, stealing privileged user credentials is the most common escalation path in Active Directory environments. Additionally, a common mistake is that admin users either have a weak (but often complex) password or a shared password with their regular user account (which can be obtained via multiple attack vectors such as keylogging). For reference, a weak but complex password is "Password1!". It includes uppercase, lowercase, numerical, and special characters, but despite this, it's easily predictable and can be found in many password lists that adversaries employ in their attacks. It is recommended to teach employees to use pass phrases because they are harder to guess and difficult to brute force. An example of a password phrase that is easy to remember yet long and complex is "i LIK3 my coffeE warm". If one knows a second language, they can mix up words from multiple languages for additional protection.

Multi-factor authentication (MFA) is another identity-protecting solution that should be implemented at least for any type of administrative access to **ALL** applications and devices.

Vulnerability Scanning

Perform continuous vulnerability scans of your environment and remediate at least the "high" and "critical" vulnerabilities that are discovered. While the scanning can be automated, the fixes usually require manual involvement. If you can't apply patches for some reason, definitely segment the systems that are vulnerable!

User Awareness Training

Training users to recognize suspicious behavior and report it when discovered is a big win for us. While it is unlikely to reach 100% success on this task, these trainings are known to significantly reduce the number of successful compromises. Periodic "surprise" testing should also be part of this training, including, for example, monthly phishing emails, dropped USB sticks in the office building, etc.

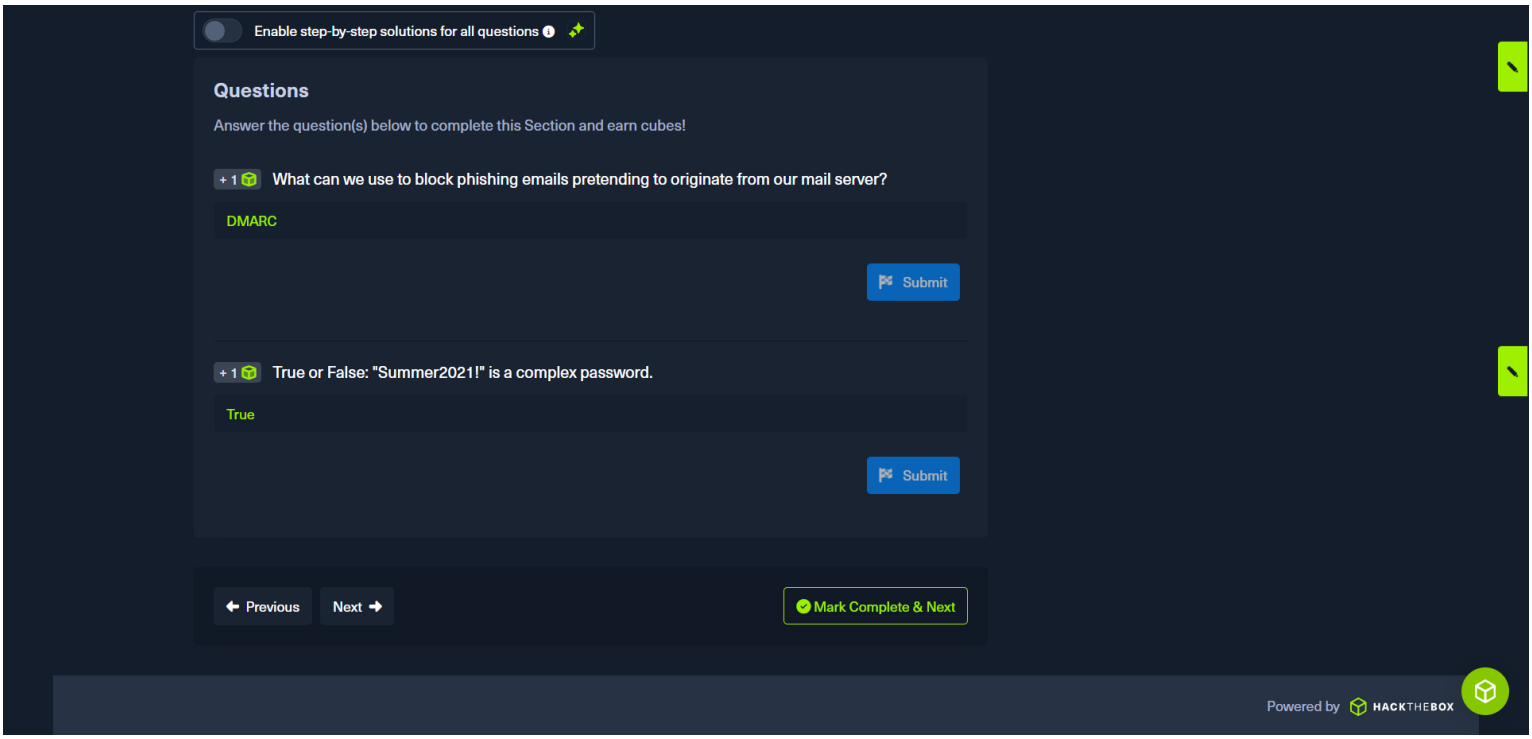
Active Directory Security Assessment

The best way to detect security misconfigurations or exposed critical vulnerabilities is by looking for them from the perspective of an attacker. Doing your own reviews (or hiring a third party if the skillset is missing from the organization) will ensure that when an endpoint device is compromised, the attacker will not have a one-step escalation possibility to high privileges on the network. The more additional tools and activity an attacker is generating, the higher the likelihood of you detecting them, so try to eliminate easy wins and low-hanging fruits as much as possible.

Active Directory has a few known and unique escalation paths/bugs. New ones are quite often discovered too. Active Directory security assessments are crucial for the security posture of the environment as a whole. Don't assume that your system administrators are aware of all discovered or published bugs, because in reality they probably aren't.

Purple Team Exercises

We need to train incident handlers and keep them engaged. There is no question about that, and the best place to do it is inside an organization's own environment. Purple team exercises are essentially security assessments by a red team that either continuously or eventually inform the blue team about their actions, findings, any visibility/security shortcomings, etc. Such exercises will help in identifying vulnerabilities in an organization while testing the blue team's defensive capability in terms of logging, monitoring, detection, and responsiveness. If a threat goes unnoticed, there is an opportunity to improve. For those that are detected, the blue team can test any playbooks and incident handling procedures to ensure they are robust and the expected result has been achieved.


Enable step-by-step solutions for all questions
Questions
Answer the question(s) below to complete this Section and earn cubes!
+ 1
What can we use to block phishing emails pretending to originate from our mail server?
DMARC
Submit
+ 1
True or False: "Summer2021!" is a complex password.
True
Submit
Previous
Next
Mark Complete & Next
Powered by HACKTHEBOX