FINAL PROJECT REPORT

Introduction

The primary objective of this exercise was to gain insights into the critical aspects of Red Team and Blue Team methodologies, focusing on securing systems through measures such as hardening, vulnerability assessment, system configuration, and SIEM (Security Information and Event Management) installation. We were presented with a scenario wherein we assumed the roles of employees at GDG, Inc., a global distribution syndicate. We were informed that a recently terminated IT Director had accessed Facebook from the corporate network and engaged in activities such as participating in a quiz titled 'How safe is my work password?'. Such actions were deemed potential pathways for malicious activities to infiltrate the system.

We were provided access to four virtual systems: SIEM, Ubuntu Server, Domain Controller, and Windows 10 Workstation. Our objective was to fortify the systems against potential attacks and ensure that unauthorized individuals did not gain control over them.

SIEM Installation and Configuration

Our initial step was setting up the SIEM. Following instructions, we commenced the installation of Wazuh, an Open-Source Security Platform offering Unified XDR (Extended Detection and Response) and SIEM protection for endpoints [1]. Referring to the guidelines provided at the URL: https://documentation.wazuh.com/current/installation-guide/index.html, I initiated the installation of Wazuh Indexer, Server, and Dashboard on our SIEM system. Adhering to the initial configurations, we downloaded the Wazuh installation assistant along with the necessary configurations. Upon receiving static IPs from the instructors, we configured our SIEM accordingly and designated the systems G4DC, G4Windows10, and G4UbuntuServer as agents for our Wazuh Server. This action enabled us to monitor the logs, file integrity, ensure malware detection, and activate responses for these systems.

System Hardening

Before the initiation of the live attack, we received instructions to harden all our virtual systems to the best of our abilities. Within our team, we divided the hardening process across different machines.

Commencing with the Linux server, our first step involved verifying all MAC addresses. Subsequently, we focused on fortifying the 'SSH Configuration Files' by updating Password Authentication, Root Login Access, and Public Key Authentication. Following this, we hardened FTP configurations, encompassing the hiding of IDS, disabling anonymous users, and updating

paths to the root user. Concluding our actions on the Linux server, we deleted the passwords of terminated employees and those granted unauthorized access to administrator privileges.

While our SIEM was not as rigorously hardened as the server, we ensured that all unnecessary processes were disabled, and services such as Apache2 and MySQL were halted.

Recognizing the potential impact the Domain Controller could face, I assumed responsibility for its hardening. Initially, I disabled unwanted services on the DC, including Internet Information Services, Remote Desktop Services, and unused network protocols. Subsequently, I updated Group Policy Object (GPO) policies for Account Policies (Password Policy, Account Lockout Policy), Local Policies (Audit Policy, Security Options), Event Logs (Retain System, Security, and Application Logs), Windows Defender Firewall, and System Admin Policies (Logon, Remote Procedure Call, User Profiles). These actions significantly aided in controlling network traffic, protecting systems from unauthorized access, and prioritizing critical security events and alerts. Additionally, our team disabled remote shell access and modified security administrative template policies on the DC.

Despite the Windows Workstation being connected to the hardened DC, our team emphasized the necessity to independently harden the workstation. Measures included disabling the spooler subsystem application and other unnecessary Windows services.

Vulnerability Management

Our initial step involved downloading Nessus [2] to conduct a comprehensive scan of the corporate network, enabling us to prioritize risk mitigation based on the severity of identified vulnerabilities. Additionally, our team installed 'nmap' to execute an SMB script scan, aiming to pinpoint vulnerabilities, misconfigurations, or potential risks linked to SMB services within the corporate network.

Subsequently, we integrated our Windows workstation (G4Windows10) into the AD domain (G4DC). Since Wazuh relied on static IP addresses for its setup and operation, we encountered issues with dynamically changing IP addresses initially. To address this, we reinstalled Wazuh and monitored the issue closely to ensure the stability of our SIEM system.

We diligently identified and eliminated suspicious directories and files across all systems. Upon analyzing logs that indicated multiple successful and unsuccessful attempts on our DC, we traced the root cause to a Kerberos attack. Consequently, we disabled the Kerberos Distribution Center and the associated Kerberos user on the system to mitigate the threat.

List of Changes made

Domain Controller:

The SMBv1 and SMBv2 protocols were disabled, and the hostname of the DC was changed to G4DC. Services such as Netlogon, Audit, Remote Procedure Call, Windows Time service were kept active on the DC. While investigating, I came across a program named 'nothing_suspicious_here'. Upon inspection, it became apparent that this program was causing the Windows firewall to fail. Referring to the provided user list, I proceeded to update the Domain Controller's user roster by removing entries for non-employees or recently fired individuals such as Rebecca Armstrong, Stephen Mixon, Dale Monsen, and John Beeson. Additionally, upon receiving complaints from the user 'adams' regarding login issues, the user was prompted to log in with a new password. Elena Curtis, who had been terminated, was consequently removed from the user profile list. During the live defense session, we were instructed to audit the user list on the controller, resulting in the following updated list.

AD user	Permissions
lewis	Admin user, Domain user
adams	Admin user, Domain user
soto	Admin user, Domain user
jones	Admin user, Domain user
atkinson	Admin user, Domain user
martin	Domain user
florian	Domain user
james	Admin user, Domain user
summerfield	Domain user
stokes	Domain user
helms	Admin user, Domain user
cason	Domain user
pagan	Domain user
saucedo	Domain user

student	Admin user, Domain user, Domain Admin, Enterprise Admin, Group Policy Creator Owners, Schema Admin

Ubuntu Server:

The hostname had been updated to G4UbuntuServer. In addition to the hardening measures implemented, a few system changes were made. Initially, Apache and MySQL were disabled as they were deemed non-essential services. However, subsequent instructions required us to maintain the LAMP stack, so we opted to enable them accordingly.

SIEM:

The hostname had been revised to G4SIEM. We resolved the issue of dynamically changing IPs for our SIEM and ensured stable operation. Monitoring the logs of all agents through the SIEM dashboard, we meticulously audited the changes made across these systems.

Windows 10 Workstation:

The hostname was updated to G4Windows10. Similar to the domain controller, the workstation underwent comparable changes. However, particular emphasis was placed on ensuring Windows Defender was active. Unwanted processes and services were disabled, with most adjustments focusing on GPO policies. Modifications were made for Logon, Remote Procedure Call, User Profiles, Auditing Policies, and Security and Application Logs, among others. Additionally, vigilant monitoring via the task manager allowed prompt removal of any 'mimikatz' files detected on the local disk.

Conclusion

The exercise gave us valuable insights into potential vulnerabilities and exploits of a network system. The post discussion session with the instructors helped us to understand the effectiveness of our implemented approaches to secure the systems as well as different methods that could have been used to protect the systems in a better way.

References

1. https://wazuh.com/
2. https://www.tenable.com/products/nessus