Product: MegaCorp One

Report: Offensive Security network

PEN-DOC-202108140857

Pentest company,
https://github.com/1modm/petereport

14-08-2021

Contents

1 Project Overview

1.1 Description

Sample Penetration report – Megacorp One

https://www.offensive-security.com/reports/sample-penetration-testing-report.pdf

2 Executive Summary

Offensive Security was contracted by MegaCorp One to conduct a penetration test in order to determine its exposure to a targeted attack. All activities were conducted in a manner that simulated a malicious actor engaged in a targeted attack against MegaCorp One with the goals of:

- Identifying if a remote attacker could penetrate MegaCorp One's defenses
- Determining the impact of a security breach on:
  - Confidentiality of the company's private data
  - Internal infrastructure and availability of MegaCorp One's information systems

Efforts were placed on the identification and exploitation of security weaknesses that could allow a remote attacker to gain unauthorized access to organizational data. The attacks were conducted with the level of access that a general Internet user would have. The assessment was conducted in accordance with the recommendations outlined in NIST SP 800-1151 with all tests and actions being conducted under controlled conditions.

Initial reconnaissance of the MegaCorp One network resulted in the discovery of a misconfigured DNS server that allowed a DNS zone transfer. The results provided us with a listing of specific hosts to target for this assessment. An examination of these hosts revealed a password-protected administrative webserver interface. After creating a custom wordlist using terms identified on the MegaCorp One 's website we were able to gain access to this interface by uncovering the password via brute-force. An examination of the administrative interface revealed that it was vulnerable to a remote code injection vulnerability, which was used to obtain interactive access to the underlying operating system.

This initial compromise was escalated to administrative access due to a lack of appropriate system updates on the webserver. After a closer examination, we discovered that the compromised webserver utilizes a Java applet for administrative users. We added a malicious payload to this applet, which gave us interactive access to workstations used by MegaCorp One's administrators.

Using the compromised webserver as a pivot point along with passwords recovered from it, we were able to target previously inaccessible internal resources. This resulted in Local Administrator access to numerous internal Windows hosts, complete compromise of a Citrix server, and full administrative control of the Windows Active Directory infrastructure. Existing network traffic controls were bypassed through encapsulation of malicious traffic into allowed protocols.

2.1 Summary of Findings Identified

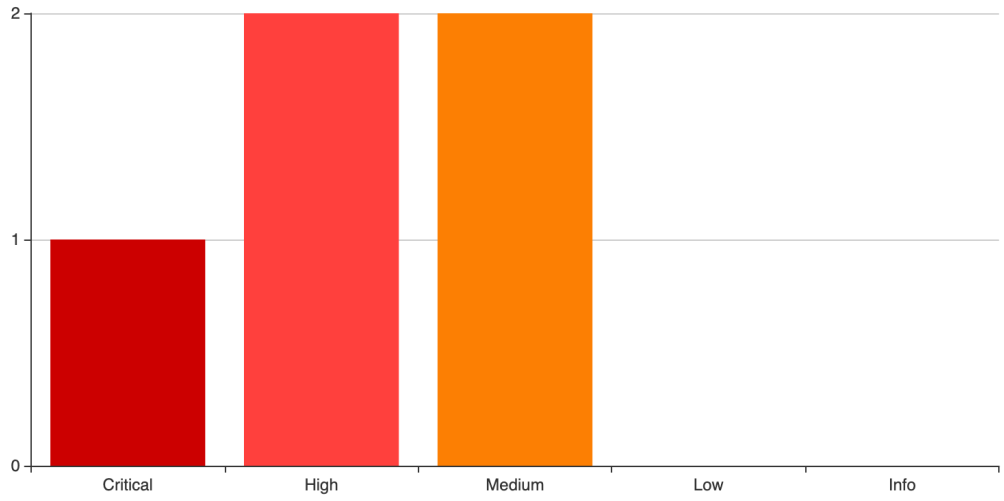

Figure 1: Executive Summary

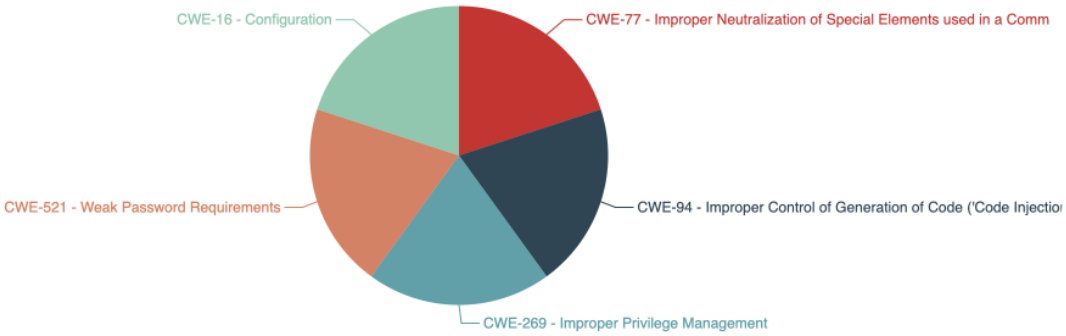

Figure 2: Breakdown by Categories

 # 1 Critical Administrative Privilege Escalation

 # 2 High Interactive Shell to Admin Server

 # 3 High Password Reuse

 # 4 Medium Admin Webserver Interface Compromise

 # 5 Medium Citrix Environment Compromise

2.2 Scope

2.2.1 In Scope

MegaCorp One network

2.2.2 Out of Scope

- DoS
- OSINT

2.3 Methodology

OSSTMM

The OSSTMM framework, one of the most recognized standards in the industry, provides a scientific methodology for network penetration testing and vulnerability assessment.

2.4 Recommendations

Due to the impact to the overall organization as uncovered by this penetration test, appropriate resources should be allocated to ensure that remediation efforts are accomplished in a timely manner. While a comprehensive list of items that should be implemented is beyond the scope of this engagement, some high level items are important to mention .

Offensive Security recommends the following:

1. Ensure that strong credentials are use everywhere in the organization. The compromise of MegaCorp One system as drastically impacted by the use of weak passwords as well as the reuse of passwords across systems of differing security levels. NIST SP 800-119 is recommended for guidelines on operating an enterprise password policy. While this issue was not widespread within MegaCorp One, it was still an issue and should be addressed.
2. Establish trust boundaries. Create logical boundaries of trust where appropriate on the internal network. Each logical trust segment should be able to be compromised without the breach easily cascading to other segments. This should include the use of unique administrative accounts so that a compromised system in one segment cannot be used in other locations.
3. Implement and enforce implementation of change control across all systems: Misconfiguration and insecure deployment issues were discovered across the various systems. The vulnerabilities that arose can be mitigated through the use of change control processes on all server systems.
4. Implement a patch management program: Operating a consistent patch management program per the guidelines outlined in NIST SP 800-4010 is an important component in maintaining good security posture. This will help to limit the attack surface that results from running unpatched internal services.
5. Conduct regular vulnerability assessments. As part of an effective organizational risk management strategy, vulnerability assessments should be conducted on a regular basis. Doing so will allow the organization to determine if the installed security controls are properly installed, operating as intended, and producing the desired outcome. Please consult NIST SP 800-3011 for guidelines on operating an effective risk management program.

3 Findings and Risk Analysis

3.1 Administrative Privilege Escalation

Severity: Critical
CVSS Score: 9.9 (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H)

CWE

77 - Improper Neutralization of Special Elements used in a Command (‘Command Injection’)

Description

With interactive access to the underlying operating system of the administrative webserver obtained, we continued with the examination of the system searching for ways to escalate privileges to the administrative level. We found that the system was vulnerable to a local privilege escalation exploit4, which we were able to utilize successfully. Please see Appendix A for more information.

Figure 3: Exploit.png

Location

administrative webserver

Impact

The use of this exploit was partially made possible due to the inclusion of developer tools on the vulnerable system. If these tools were not present on the system, it woul d have still been possible to successfully exploit, although the difficulty in doing so would have been increased. In its current configuration, the webserver represents an internal attack platform for a malicious party.

With the ability to gain full administrative access, a malicious party could utilize this vulnerable system for a multitude of purposes, ranging from attacks against MegaCorp One itself, to attacks against its customers. It's highly likely that the attackers would leverage this system for both purposes.

Recommendation

All corporate assets should be kept current with latest vendor-supplied security patches. This can be achieved with vendor-native tools or third-party applications, which can provide an overview of all missing patches. In many instances, third-party tools can also be used for patch deployment throughout a heterogeneous environment

References

http://www.exploit-db.com/exploits/18411/

https://www.offensive-security.com/reports/sample-penetration-testing-report.pdf

Additional notes

Appendix A: About Offensive Security

3.2 Interactive Shell to Admin Server

Severity: High
CVSS Score: 8.2 (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:N)

CWE

94 - Improper Control of Generation of Code (‘Code Injection’)

Description

The previously discovered SQLite Manager software was found to be vulnerable to a well-known code injection vulnerability. Successful exploitation of this vulnerability results in shell access to the underlying system in the context of the webserver user. Using a modified public exploit, we were able to obtain limited interactive access to the admin.megacorpone.com webserver. Please see Appendix A for more information.

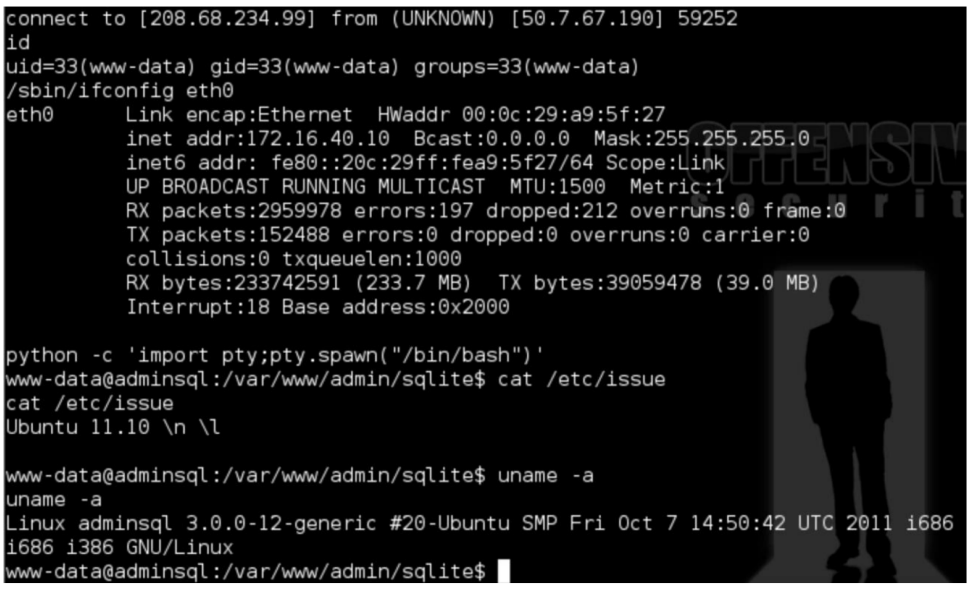

Figure 4: ShellAccess.png

The public version of the exploit targets a slightly different version of the SQLite Manager than the one deployed by MegaCorp One. Although the deployed version of the software is vulnerable to the same underlying issues, the exploit does not successfully run without modifi cation. We were able to extend the original exploit to support HTTP authentication and customize it for the updated version. A copy of this updated exploit will be provided separately from this report.

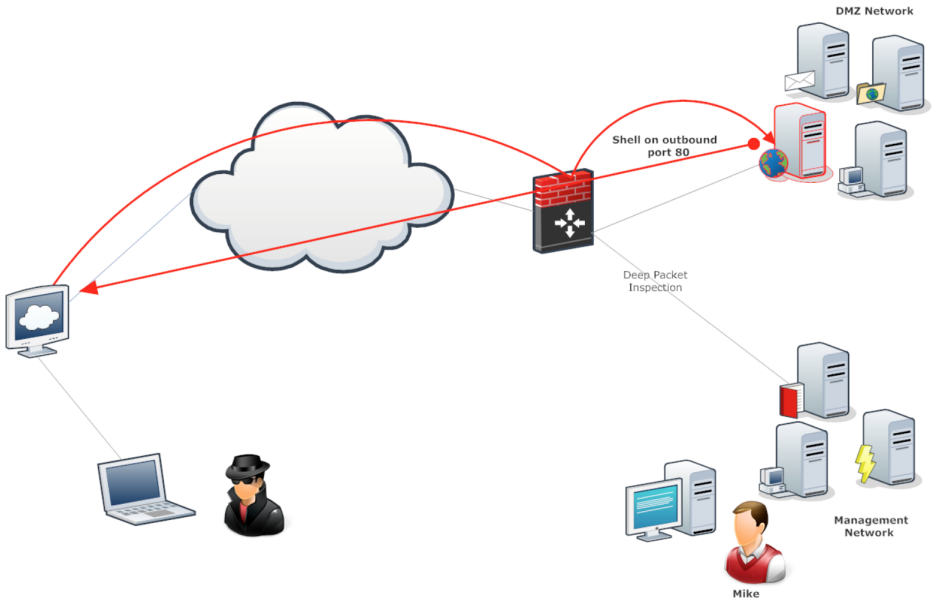

Figure 5: ExtentOfCompromise.png

Location

admin.megacorpone.com

Impact

We were able to extend the original exploit to support HTTP authentication and customize it for the updated version. A copy of this updated exploit will be provided separately from this report.

Recommendation

It is highly recommended to disable all local administrator accounts. In cases where a local administrative account is necessary, it should be assigned a unique name and a complex random password.

References

https://www.exploit-db.com/exploits/24320

https://www.offensive-security.com/reports/sample-penetration-testing-report.pdf

Additional notes

N/A

3.3 Password Reuse

Severity: High
CVSS Score: 7.7 (CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N)

CWE

269 - Improper Privilege Management

Description

MegaCorp One user mike was found to be reusing credentials for the SQLite Manager application and his Windows domain access.

Location

SQLite Manager

Impact

Password reuse in general is a practice which should be highly discouraged and prevented to the extend possible. In this case, the impact of the vulnerability is amplified by the fact that an external attacker indirectly compromised a valid set of internal Windows domain credentials. This compromise potentially allows a substantial increase in the attack surface .

Recommendation

Update the password management policies to enforce the use of strong, unique, passwords for all disparate services. The use of passw ord managers should be encouraged to more easily allow employees to utilize unique passwords across the various systems.

References

https://www.offensive-security.com/reports/sample-penetration-testing-report.pdf

Additional notes

N/A

3.4 Admin Webserver Interface Compromise

Severity: Medium
CVSS Score: 6.4 (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N)

CWE

521 - Weak Password Requirements

Description

The admin.megacorpone.com webserver was found to be running an Apache webserver on port 81. Accessing the root URL of this site resulted in the display of a blank page. We next conducted a quick enumeration scan of the system looking for common directories and files.

The scan results revealed that along with common Apache default files (Please see Appendix A for more information), we identified an "/admin" directory that was only accessible after authentication.

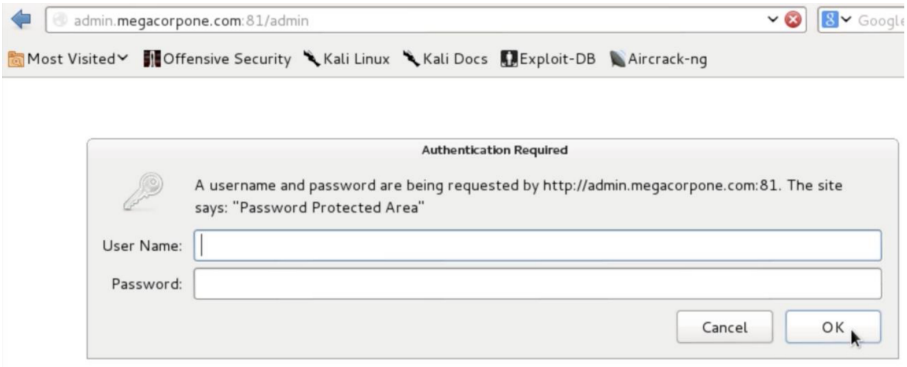

Figure 6: AdminInterface.png

To prepare a targeted brute-force attempt against this system, we compiled a custom dictionary file based on the content of the www.megacorpone.com website. The initial dictionary consisted of 331 custom words, which were then put through several rounds of permutations and substitutions to produce a final dictionary file of 16,201 words. This dictionary file was used along with the username "/admin" against the protected section of the site.

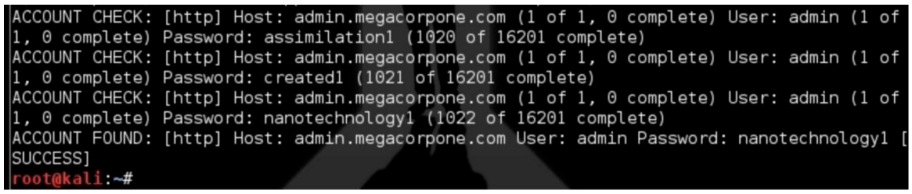

Figure 7: Bruteforce.png

Location

admin.megacorpone.com

Impact

Using common enumeration and brute -forcing techniques, it is possible to retrieve the administrative password for the SQLite Manager web interface. Due to the lack of any additional authentication mechanisms, it is also possible to retrieve all user password hashes in the underlying database. Successful retrieval of plaintext passwords could allow further compromise of the target environment if password reuse is found to exist.

Recommendation

Ensure that all administrative interfaces are protected with comp lex passwords or passphrases. Avoid use of common or business related words, which could be found or easily constructed with the help of a dictionary.

References

https://owasp.org/www-project-top-ten/2017/A2_2017-Broken_Authentication

https://www.offensive-security.com/reports/sample-penetration-testing-report.pdf

Additional notes

N/A

3.5 Citrix Environment Compromise

Severity: Medium
CVSS Score: 6.3 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L)

CWE

16 - Configuration

Description

Using remote desktop access to the internal network, we proceeded to explore the network in search of high value targets. One such target appeared to be a Citrix server, which was set as the homepage on the compromised host. Using the same credentials that were utilized to establish the remote desktop connection, we were able to successfully login to this Citrix environment.

This Citrix environment exposed “Internet Explorer” as the only available application. This is a commonly utilized method by many organizations to limit access to the underlying operating syste m of the Citrix server. It is important to note that many methods exist to bypass this configuration. In this case, we utilized the “Save” dialog window to create a batch file that would provide us with a Powershell interface. This is possible as the “Save” dialog operates in much the same manner as a standard “Windows Explorer” file management window.

Location

Citrix environment

Impact

This allowed us to gain full administrative control of the Citrix system

Recommendation

All corporate assets should be kept current with latest vendor-supplied security patches. This can be achieved with vendor-native tools or third-party applications, which can provide an overview of all missing patches. In many instances, third-party tools can also be used for patch deployment throughout a heterogeneous environment.

References

https://www.offensive-security.com/reports/sample-penetration-testing-report.pdf

Additional notes

N/A

4 Additional Notes

4.1 Appendix A: About Offensive Security

Offensive Security advocates penetration testing for impact as opposed to penetration testing for coverage. Penetration testing for coverage has risen in popularity in recent years as a simplified method of assessments used in situations where the goal is to meet regulatory needs. As a form of vulnerability scanning, penetration testing for coverage includes selective verification of d iscovered issues through exploitation. This allows service providers the ability to conduct the work largely through the use of automated toolsets and maintain consistency of product across multiple engagements. Penetration testing for impact is a form of attack simulation under controlled conditions, which closely mimics the real world, targeted attacks that organizations face on a day-to-day basis. Penetration testing for impact is a goal-based assessment, which creates more than a simple vulnerability inventory, instead providing the true business impact of a breach. An impact-based penetration test identifies areas for improvement that will result in the highest rate of return for the business. Penetration testing for impact poses the challenge of requiring a high skillset to successfully complete.

As demonstrated in this sample report, Offensive Security believes that it is uniquely qualified to deliver world-class results when conducting penetration tests for impact, due to the level of expertise found within our team of security professionals. Offensive Security does not maintain a separate team for penetration testing and other activities that the company is engaged in. This means that the same individuals that are involved in Offensive Security's industry leading performance-based training, the production of industry standard tools such as Kali Linux, authors of best selling books, creators of 0-day exploits, and maintainers of industry references such as Exploit-DB are the same individuals that are involved in the delivery of services. Offensive Security offers a product that cannot be matched in the market. However, we may not be the right fit for every job. Offensive Security typically conducts consulting services with a low volume, high skill ratio to allow Offensive Security staff to more closely mimic real world situations. This also allows customers to have increased access to industry-recognized expertise all while keeping costs re asonable.

As such, high volume/fast turn-around engagements are often not a good fit for our services. Offensive Security is focused on conducting high quality, high impact assessments and is actively sought out by customers in need of services that cannot be delivered by other vendors.