GOAD-LITE

Customer:
Orange-CyberDefense
2024-05-21
v1.0

Contact:
Brice Nevitt
213-258-2858
bnevitt@rwpentest.com

Table of Contents

Confidentiality Statement

This document is the exclusive property of Orange-CyberDefense, Real World Pentesting(RWPT), and GOAD-co. This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both Real World Pentesting and Orange-CyberDefense GOAD-co may share this document with auditors under non-disclosure agreements to demonstrate penetration test requirement compliance

Disclaimer

A penetration test is considered a snapshot in time. The findings and recommendations reflect the information gathered during the assessment and not any changes or modifications made outside of that period. Time-limited engagements do not allow for a full evaluation of all security controls. RWPT prioritized the assessment to identify the weakest security controls an attacker would exploit. RWPT recommends conducting similar assessments on an annual basis by internal or third party assessors to ensure the continued success of the controls.

Methodology

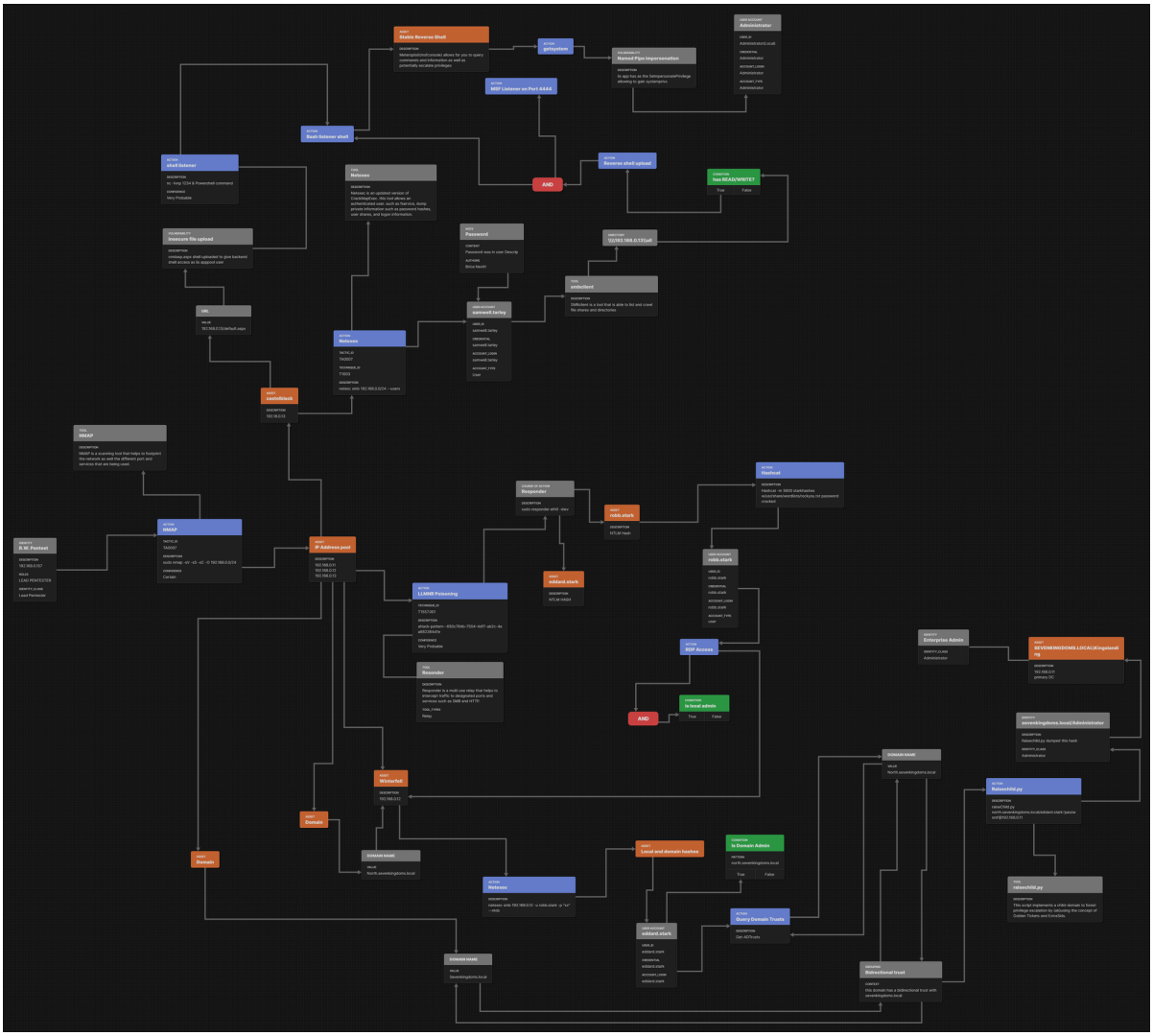
On May 21st, 2024, Real World Pentesting was contacted by Orange-CyberDefense to conduct a Penetration test for GOAD-co to evaluate both the network and system security via an internal penetration test. The MITRE ATT&K Kill chain (https://attack.mitre.org) was used as a baseline methodology to follow for the testing. A blended approach to identifying both network and system vulnerabilities through manual and automated dynamic testing was employed. The primary focus is on manual efforts and automated scanners are also employed to perform other repetitive tasks such as brute force attacks

Scope

In Scope
192.168.0.11-192.168.0.13

Out of Scope
Denial of Service (DoS) attacks against production infrastructure
Phishing / Social Engineering attacks
Attacks against any other IP's on 192.168.0.0 network
Attacks against Gateway Addr.(192.168.0.1) and switch(192.168.0.2)

Attack Flow



Executive Summary

Real World Pentesting evaluated the security posture of Orange-CyberDefense (OCD) on May 21st, 2024. RWPT tested for different vulnerabilities and misconfigurations such as weak passwords, LLMNR Poisoning, and ASREProasting.

RWPT's lead Penetration Tester, Brice Nevitt was given access to the internal subnet of 192.168.0.0/24 by way of vpn with an ip address of 192.168.0.157. Upon initial enumeration, the following IP addresses were found:

IP	Associated Asset
192.168.0.11	Kingslanding/DC1
192.168.0.12	Winterfell/DC2
192.168.0.13	Castelblack/SRV01

Castelblack

An initial enumeration using nmap of SRV01 led to port 80 being open. This was found to be a hosted web/file server that led to /default.aspx upload page, where file uploads were not properly restricted to certain extensions (GC-005). Using the file 'cmdasp.aspx', this allowed for a brower-based shell to be uploaded in to the file system. After further enumeration on the webserver using gobuster, the uploads directory was found where the .aspx file was stored. Using netcat and a powershell command, the security team was able to get a reverse shell as the appool/default user. The system was then identified as running Windows server 2019.

Further enumeration of the subnet using netexec showed that smb signing was disabled (GC-002), where there they were able to dump the users for the domain north.kingslanding.local. It was then found that the user samwell.tarley had the password of their account in the description of their user account. With this information, the security team found that sam.tarley had access to upload to the share "all" on the system "Castelblack". From here, the security team noticed that proper no AV monitoring in place, as a staged reverse shell was upload without restrictions (GC-001).

Afterwards, a shell was called from metasploit, allowing the ability to query more data within the system. It was then discovered that the user "default apppool" has the privilege "SeImpersonate" (GC-006), Which allowed RWPT to escalate privileges to gain access to the machine as "NT Authority\System". The led to a complete compromise of the system "Castelblack".

Winterfell

After the compromise of the .13 machine, RWPT decided to focus their attention on the machine Winterfell. After seeing smb signing being disabled, the team used the tool Responder to intercept any sort of traffic to the network shares and files. This tool found the hashes of both eddard.stark and robb.stark (GC-004) and using the tool Hashcat on both hashes, the hash for robb.stark was easily cracked (GC-003)

It was then found that robb.stark had access to "Winterfell" and its shared, as well as the ability to RDP in. The team further noticed that robb.stark was set as a local administrator for the "Winterfell" machine (GC-007). The security team was able to dump the ndts contents using netexec. This gave access to a proper hash that belonged to eddard.stark that was used to remote in to the "Winterfell" Machine. The eddard.stark account was found to be a domain admin leading to a full compromise of "Winterfell".

sevenkingdoms.local

After the hashes for eddard.starked were aquired, the ability to use remote desktop protocol with the user hashes was acquired and access to the system as eddard.starked was gained. After enumeration on the machine, the security team found that there was a bi-directional child-parent domain trust between "Winterfell" and "Kingslanding" (192.168.0.11/DC01). A child parent domain trust is where both the parent and the child domain trust each other for its own users to use resources within either domain. For example, domain admins inside of the domain North.sevenkindgoms.local will have domain administrator privilege for the parent domain of sevenkingdoms.local, and vice versa.

With this trust found as well as the hash for eddard.stark obtained earlier, i was able to use the tool raisechild.py to escalate privileges from the child domain to the parent domain, as well as dump the hashes for the sevenkingdoms.local\Administrator Account (GC-008)

Additional Security Vulnerabilities and Misconfigurations

There were four additional misconfigurations found that did not contribute to the initial compromise of the domain, but still were serious to report. During the initial enumeration of the network and its machines, it was found that the account "brandon.stark" was able be kerberoasted by As-rep. This means that the account had disabled kerberos Pre-Authentication (GC-009). Using the tool GetNPUsers.py, the asrep hash for brandon stark was captured and cracked.

Furthermore, using the captured hashes from brandon.stark, the attempt to kerberoast more users was successful with netexec, as the kerberos hashes were captured from both jon.snow and sql_svc (GC-010). The hash for jon.snow was promptly cracking pointing back to the weak password policy.

It was also found that the user "sql_svc" was found to have their kerberos credentials saved in clear text, resulting in the password being stolen (GC-011).

Due to the weak password policy and easily crack passwords, it came to the attention of RWPT that the encryption that GOAD-Co uses for their passwords was NTLM, the depreciated encryption that is prone to password cracking (GC-012).

The following users were either identified as having a weak password or their password was discorvered during the duration of this penetration test and the passwords for these accounts should be changed immediately:

1. arya.stark
2. robb.stark
3. brandon.stark
4. hodor
5. jon.snow
6. samwell.tarly
7. tywin.lannister
8. jaime.lannister
9. tyron.lannister
10. robert.baratheon
11. joffrey.baratheon
12. renly.baratheon
13. petyer.baelish
14. castelblack\Administrator (Local)
15. winterfell\Administrator (Local)
16. sevenkings\Administrator
17. sql_svc

Vulnerability Overview

In the course of this penetration test **6 Critical**, **5 High**, **1 Medium** and **1 Info** vulnerabilities were identified:

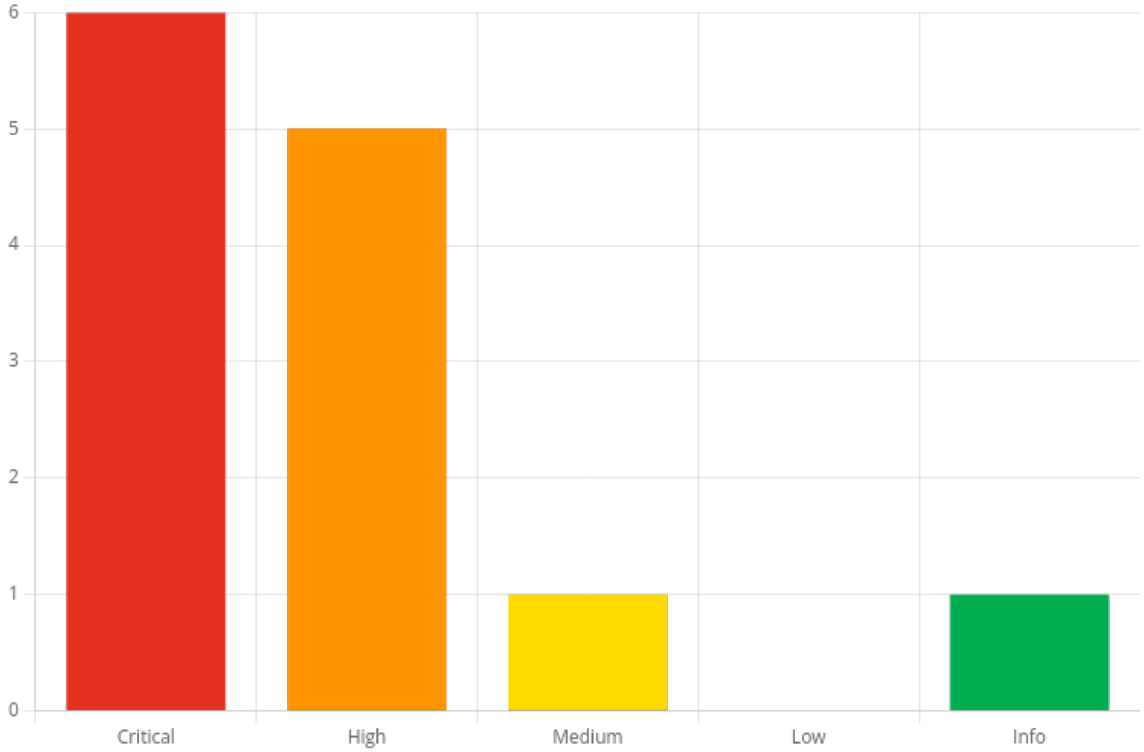


Figure 1 - Distribution of identified vulnerabilities

Vulnerability	Criticality
GC-001:Insufficient Antivirus Monitoring	Critical
Gc-002:SMB Signing Disabled	Critical
GC-003:Weak Password Policy	Critical
GC-004:LLMNR Poisoning	Critical
GC-005:Unrestricted File Upload	High
GC-006:Insufficient Privileges given for local user	High
GC-007 Insufficent Privileges for Domain user	High
GC-008:Domain Trust Abuse	High
GC-009:Kerberoasting via AS-REP	Critical
GC-010:Kerberoasting	High

Vulnerability	Criticality
GC-011:Clear Text Credentials	Medium
GC-012:Weak Password Encryption	Critical
GC-013:Proof of Domain Compromise	Info

1. GC-001:Insufficient Antivirus Monitoring

Criticality: Critical
CVSS-Score: 10.0
Affects: 192.168.0.13

Overview

On IP 192.168.0.13, it was found that insufficient AV monitoring was in place, allowing the security team to remotely upload and execute a reverse shell with out the antivirus detecting it. This was in question from GC-004 when a powershell command was utilized to gain command line access through the web-browser shell.

Impact

This misconfiguration allowed for the team to grab a stable reverse shell on "Castelblack". This stable shell, via metasploit allowed the team to escalate privileges, as seen in GC-002.

Description

This misconfiguration can lead to many different issues, and will always result in a breach of the system and its data.

Proof of Concept

Recommendation

1. Activate Windows Defender.
2. Instill AV monitoring on the system(bitdefender, webroot, sentinelone).

Additional Information

- https://www.security.org/antivirus/do-you-need-antivirus/
- https://www.ncsc.gov.uk/guidance/what-is-an-antivirus-product#:~:text=Once%20it%27s%20on%20your%20computer,protect%20your%20data%20and%20devices.

2. Gc-002:SMB Signing Disabled

Criticality: Critical
CVSS-Score: 10.0
Affects:

- 192.168.0.12
- 192.168.0.13
- samwell.tarley

Overview

During enumeration it was found that SMB signing was disabled. This lead to finding the password of samwell.tarley in the user description as well as access to read and upload files to the "all" shares on Castelblack.

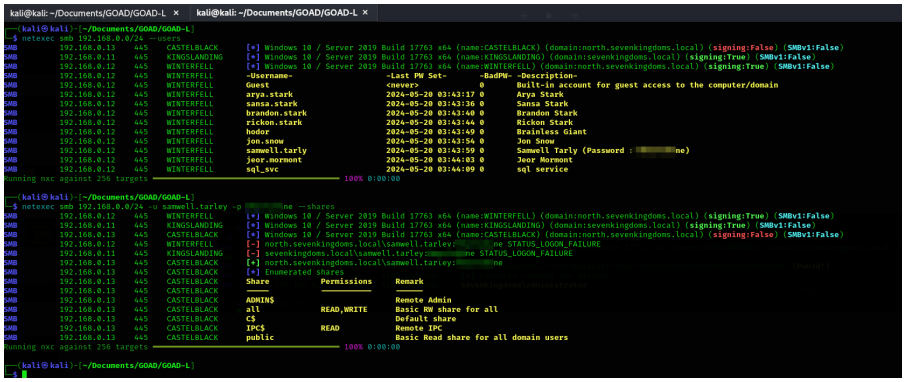
Impact

This initial discorvery led to the password of samwell.tarley as well as the ability to connect to the share "all" and upload files to said share.

Description

With SMB signing disabled, this can lead to many different threats such as LLMNR poisoning, Yielding shells, and authenticating to shares anonymously.

Proof of Concept



Recommendation

1. Enable SMB signing on all domain computers, or alternatively disable NTLM authentication to help mitigate these attacks.

Additional Information

- https://redfoxsec.com/blog/how-to-find-and-fix-smb-signing-disabled-vulnerability/
- https://learn.microsoft.com/en-us/windows-server/storage/file-server/smb-signing?tabs=windows

3. GC-003:Weak Password Policy

Criticality: Critical
CVSS-Score: 10.0
Affects:

- sevenkingdoms.local
- north.sevenkingdoms.local
- robb.stark
- hodor

Overview

Throughout the entirety of the penetration test it was found that a weak password policy was in place. This can and will result in user account breaches, which in turn can result in access to the internal network and its data.

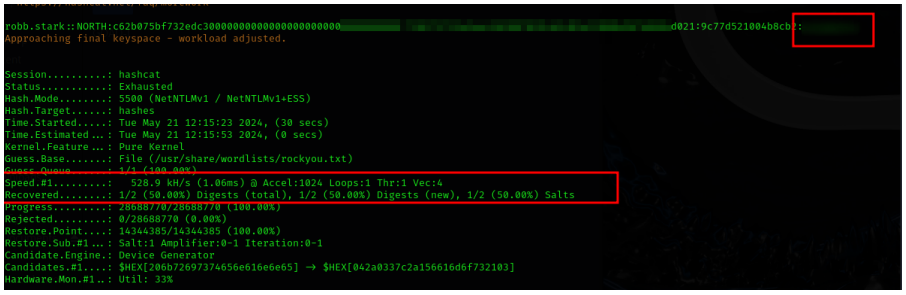
Impact

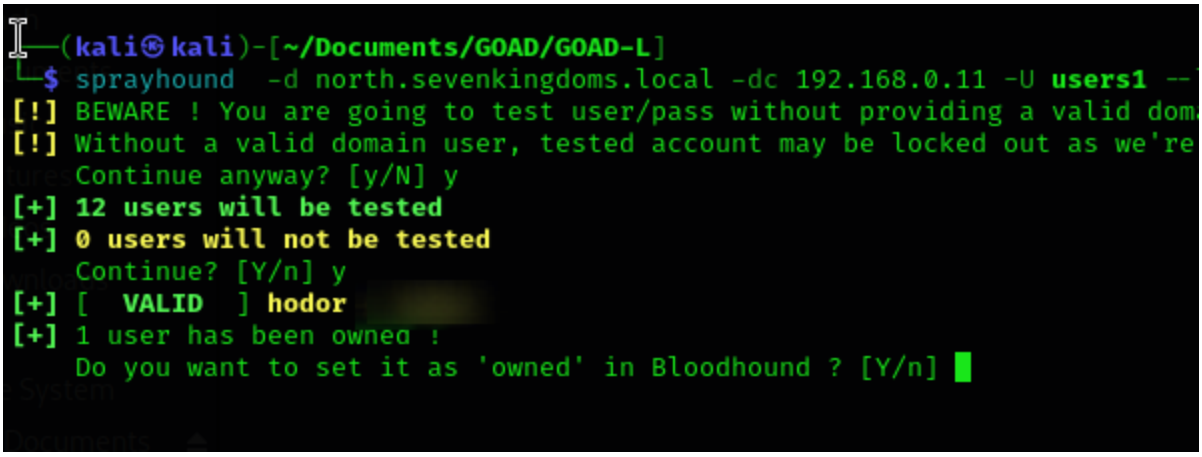
Depending on the account that is breached, this misconfiguration can lead to the compromisation of a workstation/server or the internal network as a whole.

Description

A weak password policy is the first thing many attackers will look for as well as attempt to attack and exploit. If this enforced network wide, then this can lead to a breach of high privileged users as well as the data those accounts have access to.

Proof of Concept





Recommendation

1. Atleast 14 Characters.
2. Enable Password complexity (characters such as !@#).
3. Enforce Password changes every 60 to 90 days.
4. Enfore atleast ONE uppercase letter.

Additional Information

- https://www.microsoft.com/en-us/security/business/security-101/what-ispassword-protection?ef_id=_k_CjwKCAjwoa2xBhACEiwA1sb1BBLLhAfsxmjcEgd1ZmSHsRhrYfFutAdnd_12taA8rFEfjl1UQfd0hoCs8kQAvD_BwE_k_&OCID=AIDcmmdamuj0pc_SEM__k_CjwKCAjwoa2xBhACEiwA1sb1BBLLhAfsxmjcEgd1ZmSHsRhrYfFutAdnd_12taA8rFEfjl1UQfd0hoCs8kQAvD_BwE_k_&gad_source=1&gclid=CjwKCAjwoa2xBhACEiwA1sb1BBLLhAfsxmjcEgd1ZmSHsRhrYfFutAdnd_12taA8rFEfjl1UQfd0hoCs8kQAvD_BwE
- https://www.cisecurity.org/insights/white-papers/cis-password-policy-guide

4. GC-004:LLMNR Poisoning

Criticality: Critical
CVSS-Score: 9.4
Affects:

- 192.168.0.12
- eddard.stark
- robb.stark

Overview

It was found that LLMNR was enabled on "Winterfell". This allows for a remote attacker to intercept information from the victim going to the target such as hashes, clear text passwords, and other sensitive information.

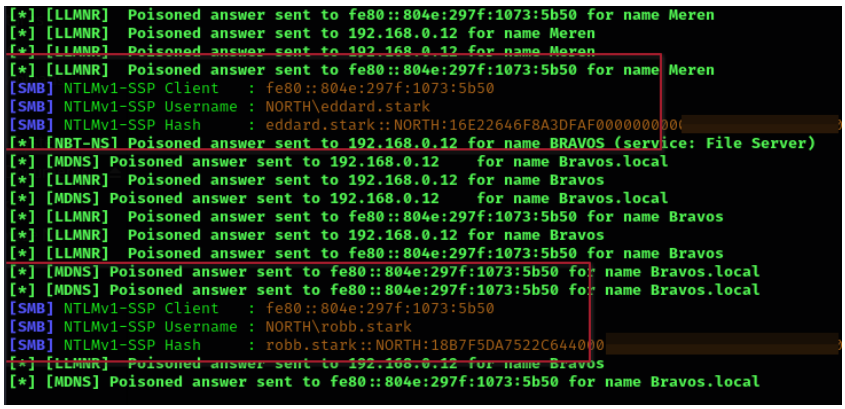
Impact

This finding,ultimately leading to the compromise of "Winterfell" as well as the Domain itself, intercepted the hashes of robb.stark. This allowed for the ability to remote in to "Winterfell" and compromise the domain admin "eddard.stark".

Description

Using this method, attackers and intercept smb requests to dump hashes for domain users, administrators and machine passwords. This can lead to an initial compromise as a user or administrator depending on the hash that was stolen at the time. This is done through tools such as responder or ntlmrelay. These tools act as sort of a middle man for many different services.

Proof of Concept



Recommendation

1. Disable Multicast Name Resolution via Group Policy or via NetBios over TCP.
2. If LLMNR is needed then require stronger passwords as well as Network Access control.

Additional Information

- https://attack.mitre.org/techniques/T1557/001/
- https://redfoxsec.com/blog/what-is-llmnr-poisoning-and-how-to-avoid-it/#:~:text=LLMNR%20poisoning%20can%20be%20an,poisoning%20attacks%20is%20reduced%20significantly.

5. GC-005:Unrestricted File Upload

Criticality: High
CVSS-Score: 8.5
Affects: http://192.168.0.13/default.aspx

Overview

Unrestricted file upload is a security vulnerability in web applications that allow users to upload files without proper restrictions. This can be dangerous because attackers can upload malicious files that can take over the server, steal data, or deface the website.

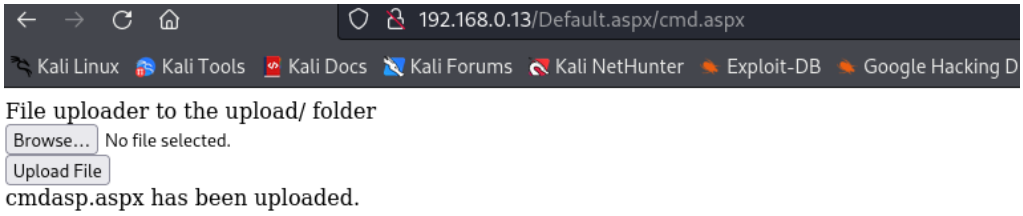
Impact

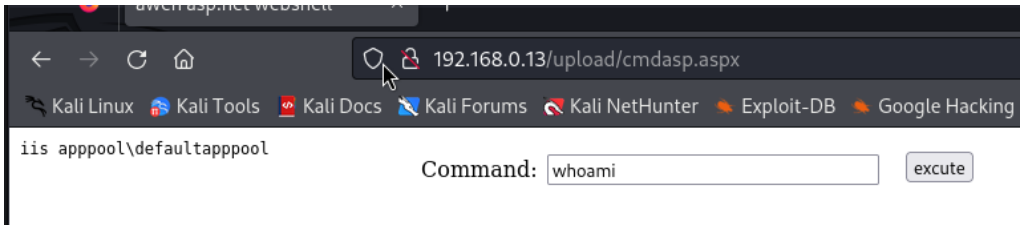
This misconfiguration allowed the use powershell to call back to a netcat listener, giving me shell access to the system as the IIS apppool user.

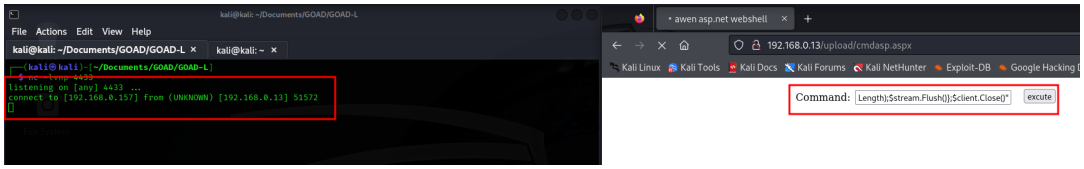
Description

Unrestricted File upload allows for any files to be uploaded to the targeted directory without any repercussions. This means that malicious file extensions such as .exe, .aspx, or .php that call back to reverse shells or query system information are able to be uploaded and accessed with out any need for privileges.

Proof of Concept







Recommendation

1. Restrict file uploads to common extensions used in your environment(.doc, .pdf, .ppt). This will help mitigate the attack vector by disallowing out of scope extensions to be uploaded.
2. Lock the upload directory behind credential access. This will allow only those that have/need access to upload the files to the targeted directory. .

Additional Information

- https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload
- https://learn.snyk.io/lesson/unrestricted-file-upload/

6. GC-006:Insufficient Privileges given for local user

Criticality: High
CVSS-Score: 8.8
Affects:

- 192.168.0.13
- IIS Apppool/Default apppool

Overview

It was found that the user "default apppool" had the privileges "SeImpersonate" applied to the user account. This led to a local compromise of the system "SRV02/Castelblack".

Impact

Complete compromise of local administrator of "SRV02/Castelblack".

Description

The privilege SeImpersonate allows for the user to be impoersonated as well as impersonate other processes. This was executed as follows:

1. Gained a shell as the iis user and changed to the directory c:\shares\all.
2. Used the tool smbclient to upload a file called reverse.exe, as seen in GC-002.
3. Set up a listener inside of metasploit to listen for the call that 'reverse.exe' makes
4. Executed the file as the iis user.
5. The listener then receives the call from reverse.exe, giving a stable shell
6. Inside of the msfconsole, type 'getsystem'. This impersonated the printspooler service, running as NT Authority\System to gain the highest privileges on the workstation.

Proof of Concept

Recommendation

Remove the SeImpersonation attribute from any user/account that does not need it.

Additional Information

- https://www.ired.team/offensive-security/privilege-escalation/windows-namedpipes-privilege-escalation
- https://juggernaut-sec.com/seimpersonateprivilege/

7. GC-007 Insufficent Privileges for Domain user

Criticality: High
CVSS-Score: 8.2
Affects:

- 192.168.0.12
- robb.stark

Overview

Upon enumeration of robb.stark, it was found that the user account had local admin privileges on the"Winterfell" workstation. This allowed me to dump the local and domain hashes, which intunr gave me access to the eddard.stark account.

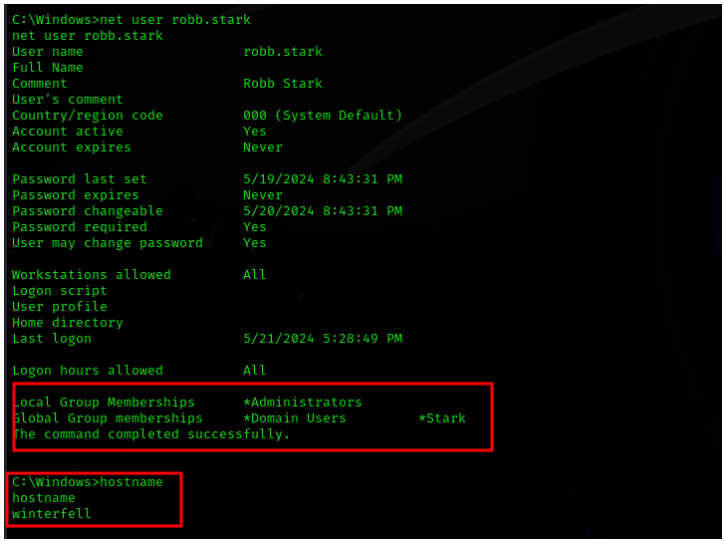
Impact

This misconfiguration ultimately led to the compromise of the north.sevenkingdoms.local domain.

Description

Having a user account as a local admin can lead to privilege abuse, such as dumping hashes, intercepting domain traffic or changing user and admin passwords. This risk can allow attackers to navigate deeper into the network by leveraging permissions.

Proof of Concept



Recommendation

Segement the privileges so that users and/or services do not have complete local or domain admin privileges on a single computer.

8. GC-008:Domain Trust Abuse

Criticality: High
CVSS-Score: 7.3
Affects:

- north.sevenkingdoms.local
- sevenkingdoms.local
- 192.168.0.11
- 192.168.0.12
- eddard.stark

Overview

It was found that the domains 'sevenkingdoms.local' and 'north.sevenkingdoms.local' had a child/parent relationship in place. This can be abused if the domain admin account is able to elevate the child domain using the tool ''raisechild.py'.

Impact

This finding led to complete compromise of the domain 'sevenkingdoms.local' as an enterprise administrator.

Description

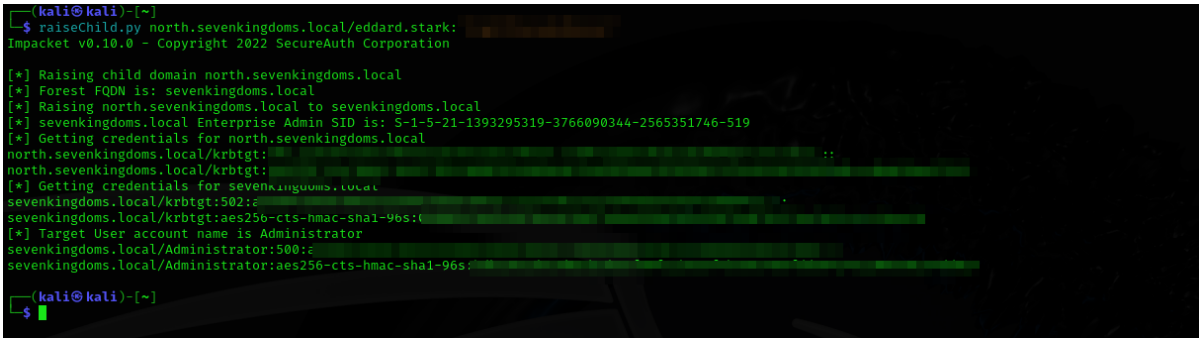
The Trust Relationship:

A child domain inherently trusts the parent domain, allowing users and services from the parent domain to access resources in the child domain. This trust is bidirectional by default, meaning the parent domain also trusts the child domain to some extent. The specific permissions granted by the trust can be configured, but often include access to user accounts, groups, and resources.

Technical Techniques:

1. Kerberos Ticket Manipulation: Attackers can exploit vulnerabilities in Kerberos ticket granting to forge tickets that grant them access to resources in the parent domain. This can be achieved through techniques like Golden Ticket attacks if the attacker gains access to a powerful account in the child domain.
2. Forced Authentication: The attacker can trick a legitimate user in the child domain to authenticate to a malicious server controlled by them. This can be done through phishing attacks or exploiting vulnerabilities in legitimate services. Once the user authenticates, the attacker can potentially leverage the trust relationship to gain access to the user's resources in the parent domain.

Proof of Concept



Recommendation

1. Principle of Least Privilege: Grant users and services in the child domain only the minimum access required to perform their tasks. This reduces the potential damage if an attacker gains access.
2. Strict Trust Permissions: Configure trust permissions to only allow the necessary access to resources. Don't grant full domain access through trusts unless absolutely necessary.
3. Secure Child Domain: Maintain strong security practices in the child domain, including enforcing strong passwords, implementing multi-factor authentication (MFA), and keeping systems patched.

Additional Information

- https://www.sevenlayers.com/index.php/blog/515-abusing-trusts-sid-hijacking
- https://cryptex.blog/posts/childtoea/

9. GC-009:Kerberoasting via AS-REP

Criticality: Critical
CVSS-Score: 9.4
Affects:

- north.sevenkingdoms.local
- brandon.stark

Overview

The domain 'north.sevenkingdoms.local' was found to be susceptible to asrep-roasting. This allowed the ability to dump the kerberos hashes for the user 'brandon.stark'.

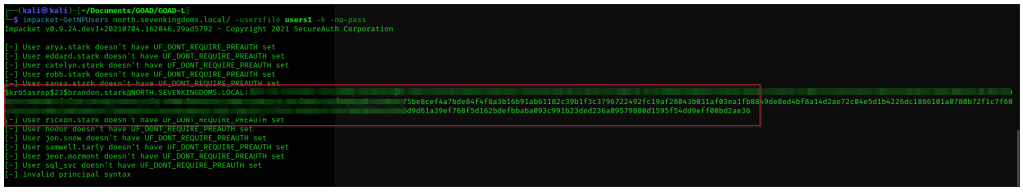
Impact

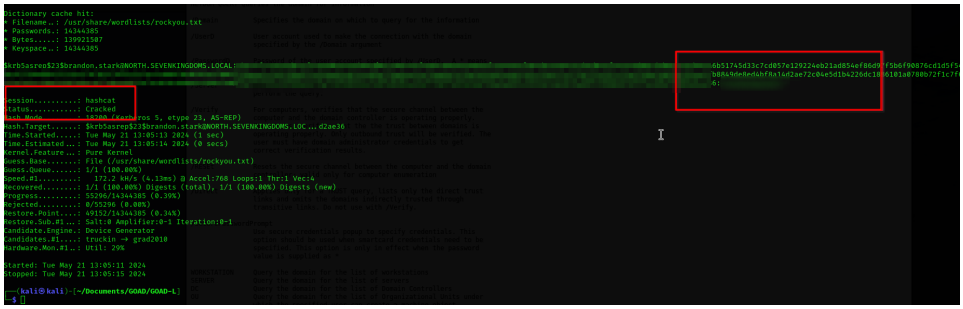
This had no impact of total domain compromisation for 'north.sevenkingdoms.local' or 'sevenkingdoms.local', but the credentials were used in GC-010.

Description

This attack targets users that disabled Kerberos pre-authentication for an authentication ticket(AS-REP). This does not require a password for the domain and will dump any associated hashes with the user accounts.

Proof of Concept





Recommendation

1. Enable Kerberos Pre-Authentication.
2. Use Stronger Passwords.

Additional Information

- https://book.hacktricks.xyz/windows-hardening/active-directory-methodology/asreproast
- https://www.picussecurity.com/resource/blog/as-rep-roasting-attack-explained-mitre-attack-t1558.004

10. GC-010:Kerberoasting

Criticality: High
CVSS-Score: 8.8
Affects:

- north.sevenkingdoms.local
- jon.snow
- 192.168.0.12

Overview

Using the credentials that were found in GC-009, the service account 'jon.snow' was found to be kerberoastable and revealed the kerberoas ticket hashes for its account.

Impact

This had no impact of total domain compromisation for 'north.sevenkingdoms.local' or 'sevenkingdoms.local', but could lead to more serious damage from a threat actor.

Description

Kerberoasting is a post-exploitation attack technique that targets Active Directory and aims to extract password hashes for service accounts. When a service ticket is requested for a service account, the KDC generates a Ticket Granting Ticket (TGT) specifically for that service. This TGT is encrypted with the password hash of the service account associated with the requested SPN. However, a historical weakness of the Kerberos protocol lies in its use of RC4 encryption for this TGT, which is susceptible to offline brute-forcing attacks.

Proof of Concept

Recommendation

1. Enforce Strong Passwords.

2. Limit SPNs: Grant SPNs only to service accounts that genuinely require them. Reduce the attack surface by minimizing the number of vulnerable service accounts..

Additional Information

- https://www.strongdm.com/what-is/kerberoasting#:~:text=a%20Kerberoasting%20Attack-,Kerberoasting%20is%20a%20type%20of%20attack%20that%20targets%20the%20Kerberos,gain%20access%20to%20sensitive%20resources.
- https://www.sentinelone.com/cybersecurity-101/what-is-kerberoasting-attack/

11. GC-011:Clear Text Credentials

Criticality: Medium
CVSS-Score: 6.9
Affects:

- 192.168.0.12
- sql_svc

Overview

It was found that the service account 'sql_svc' had its password stored in clear text, which was dumped by the tool 'Mimikatz'. This is usually caused by a misconfguration with the lsass service.

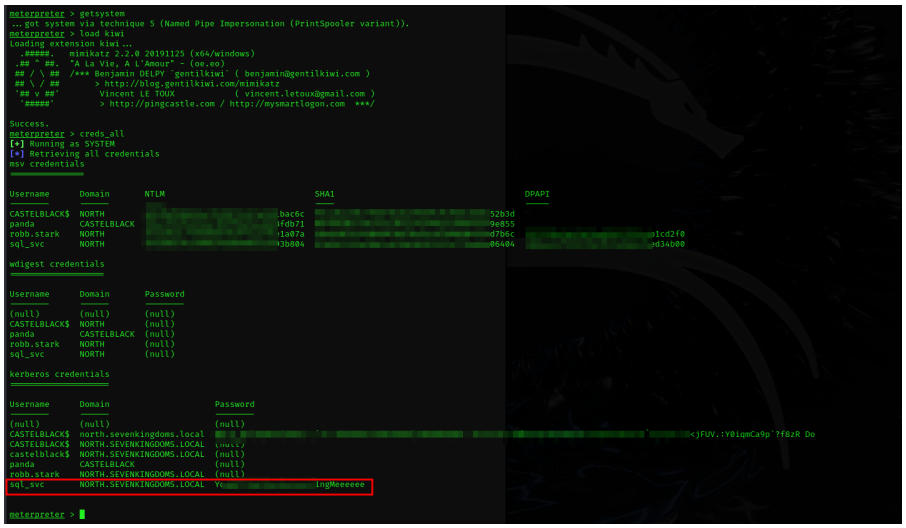
Impact

This had no impact of total domain compromisation for 'north.sevenkingdoms.local' or 'sevenkingdoms.local', but could lead to more serious damage from a threat actor.

Description

The lsass service saves the credentials that are used in the system. When configured properly, this will save the passwords in a hash that sometimes will contain extra characters, known as "salting". When misconfigured, the servce can save these passwords in weak formats, such as NTLM or md5, or in clear text revealing the password itself.

Proof of Concept



Recommendation

1. Open “gpedit.msc” on the workstation.
2. Go to: Local Computer Policy>Computer Configuration>Windows Settings>Security Settings>Local Policies>Security Options.
3. Find the policy: Network access: Do not allow storage of passwords and credentials for network authentication.
4. Choose the Local Security Settings to “Enable”

Additional Information

- https://www.adamcouch.co.uk/stopping-mimikatz-from-dumping-clear-text-credentials/
- https://thalpius.com/2024/01/23/microsoft-defender-for-identity-recommended-actions-stop-clear-text-credentials-exposure/

12. GC-012:Weak Password Encryption

Criticality: Critical
CVSS-Score: 9.3
Affects:

- north.sevenkingdoms.local
- sevenkingdoms.local

Overview

During the duration fo the penetration test, it was found that the user password encryption was set to NTLM, a weaker password standard.

Impact

Ths password standard led to the complete compromise of the domain 'north.sevenkingdoms.local' and 'sevenkingdoms.local' as an Enterprise Admin.

Description

The NLTM password standard is prone to offline password attacks as well as brute-force attacks. This standard can ususally be cracked withing 1 to 2 minutes depending on the password length. NTLM is more susceptible to LLMNR poisoning as well as smbrelay attacks.

Proof of Concept

c66d72021a2d4744409969a581a1705e	Unknown	Not found.
af52e9ec3471788111a6308abff2e9b7	Unknown	Not found.
[redacted]e2869616080	NTLM	[redacted]ei
[redacted]dcf8c349954b	NTLM	[redacted]ime
b3b3717f7d51b37fb325f7e7d048e998	Unknown	Not found.
[redacted]:84ea60dbe	NTLM	[redacted]rld
[redacted]b3829866b08f1	NTLM	[redacted]ion
[redacted]d631acfcd49bce	NTLM	[redacted]rell
d75b9fdf23c0d9a6549cff9ed6e489cd	Unknown	Not found.
[redacted]2568b086c8d210	NTLM	[redacted]nger@
52ff2a79823d81d6a3f4f8261d7acc59	Unknown	Not found.
9a2a96fa3ba6564e755e8d455c007952	Unknown	Not found.

dbd13e1c4e338284ac4e9874f7de6ef4	Unknown	Not found.
1790725bb530361382069d57ce5ca61a	Unknown	Not found.
?28940e2ff4e709	NTLM	dle
d977b98c6c9282c5c478be1d97b237b8	Unknown	Not found.
cba36eccfd9d949c73bc73715364aff	Unknown	Unrecognized hash format.
e2f51ac91e1a07a	NTLM	fy
2c643546d00054420505a2bf86d77c47	Unknown	Not found.
560a3f932129	NTLM	iseec
7978dc8a66d8e480d9a86041f8409560	Unknown	Not found.
9c6c95525e	NTLM	or
39aff05e3ccb1755	NTLM	thing
62068ac826843	NTLM	ane
6dccf1c567c56a40e56691a723a49664	Unknown	Not found.
84a5092f53390ea48d660be52b93b804	Unknown	Not found.

Recommendation

Disable NTLMv1 responses in either Group Policy:

1. Use “Start->Run” and type in “gpedit.msc” in the “Run” dialog box. A “Group Policy” window will open.
2. Click down to “Local Computer Policy -> Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> Security Options.
3. Find the policy “Network Security: LAN Manager authentication level”.
4. Right click on this policy and choose “Properties”.
5. Choose “Send NTLMv2 response only/refuse LM & NTLM”.
6. Click OK and confirm the setting change.

Or via the registry system:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Lsa DWORD :
LmCompatibilityLevel : 0.

Additional Information

- https://serverfault.com/questions/1105707/how-to-restrict-ntlm-v1-to-select-servers#:~:text=You%20can%20disable%20NTLMv1%20through,Refuse%20LM%20NTLM%E2%80%9D.
- https://www.csun.edu/it/ntlmv1#:~:text=Disabling%20NTLMV1,disable%20NTLMv1%20through%20the%20registry.
- https://www.silverfort.com/blog/resolve-the-risks-of-ntlmv1/

13. GC-013:Proof of Domain Compromise

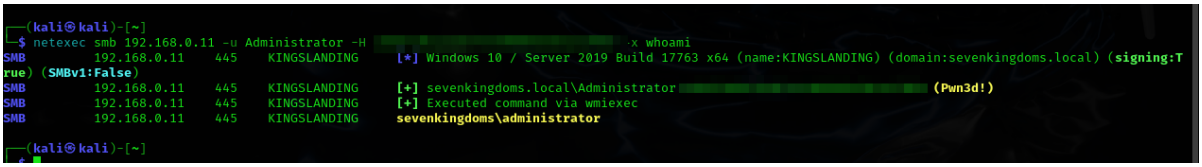
Criticality: Info
CVSS-Score: 0.0
Affects: sevenkingdoms.local

Overview

Below is a Proof of Concept that domain compromised was achieved.

Description

Proof of Concept



Recommendation

List of Changes

Version	Date	Description	Author
1.0	2024-05-24	Internal Penetration Test Report for GOAD-CO	Brice Nevitt