9144965

Abstract

**This is a report on penetration testing Querier. It will show the steps taken to gain access to the highest credential on the system and some of the tools used.  
  
978 Words**

Information SECURITY

Penetration Testing of Querier



# Intro

This report will look at Queriers network, the vulnerabilities found and the recommended fixes to limit future attacks. You will see how anonymous access to SMB was used to gain access to your MySQL server which would then be used to gain full control of your system. At the end of the report is a list of immediate fixes and recommendations for the future to further increase your security.

# Reconnaissance

The beginning of most attacks will start with a scan of the network. Nmap, a tool designed to scan all 65,535 network ports, discovered that Queriers network had multiple ports open. While this is not unusual, because for connections to be made to your network, their needs to be ports open. The issue arises with what ports are open. In this case it is NetBIOS and Microsoft-ds. NetBIOS on port 139 and Microsoft-ds on port 445 usually indicates Server Message Block (SMB) is open.

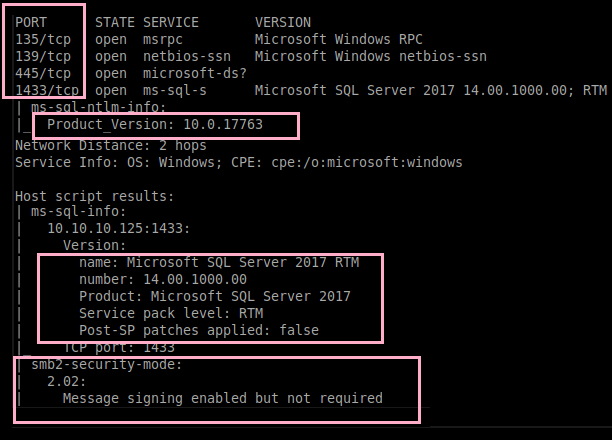


Figure : Netmap showing the ports open, the windows version and the MySQL server version.

SMB is the same vulnerability that caused the ‘WannaCry’ ransomware attack in 2017 and is notoriously vulnerable (Microsoft 2017). A quick look on Mitre shows over 400 entries going all the way back to 1999 (Mitre 2019). This vulnerable service will be the main attack vector used to gain a foothold on the system.

The Nmap scan also showed that it is a Windows 10 system, version 17763. The Microsoft website shows that this version was released on the 12th of November 2018 (Microsoft 2019a). Nmap also shows the system is running a MySQL server, version 2017 RTM and has not been updated since it was installed. This leaves the system open to any vulnerability created after November 2018 and leaves MySQL vulnerable to any exploit created after 2017.

# Attack Vectors

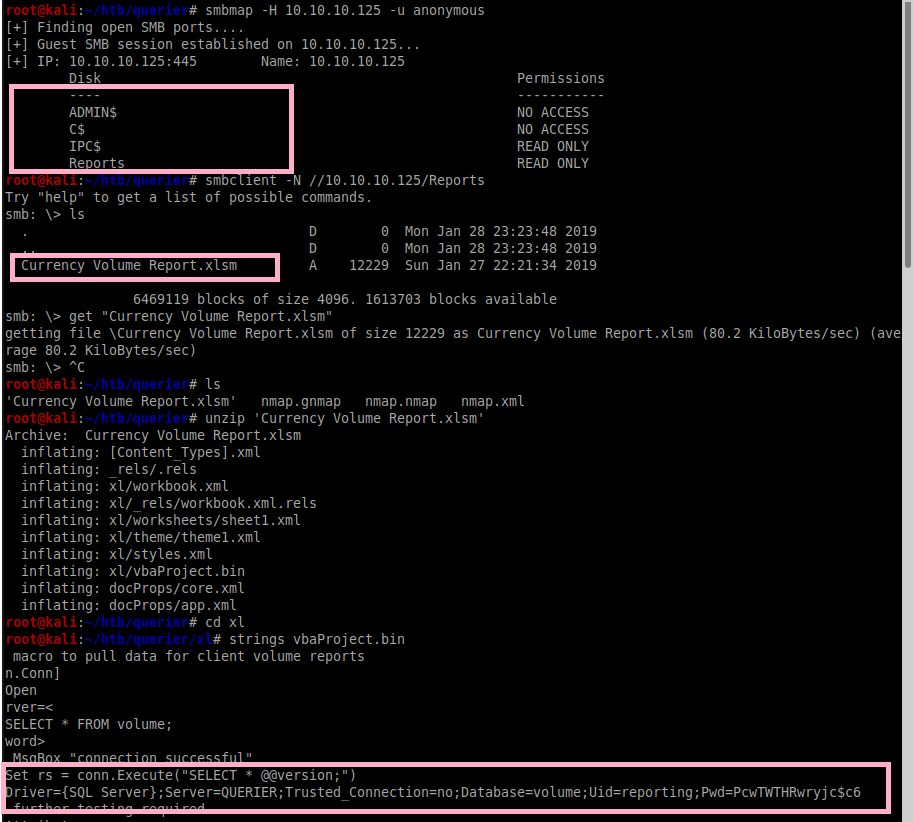
The two main attack vectors used to gain access to the system are SMB and MySQL. After discovering ports 139 and 445 open, the first thing to do, was to try and connect to SMB. The first attempt to connect to SMB failed due to requiring a username and password. On the second attempt, it was discovered that SMB allowed anonymous access. The anonymous account had read only permissions on two folders ‘IPC$’ and ‘Reports’. The ‘IPC$’ folder gave an error, but the ‘Reports’ folder contained ‘Currency Volume Report.xlsm’, which the anonymous account was able to download. Once the file was downloaded and opened it was discovered that the file contained a macro. The macro contained both the username (reporting) and password (PcwTWTHRwryjc) to access the Querier MySQL server. This would be used to pivot away from SMB and towards the secondary attack vector, MySQL. 

Figure : This shows the anonymous connection through SMB and the downloading, unpacking and extraction of the password from the macro.

Connecting to the MySQL server with the username and password gathered from the macro would create a shell and bypass both the firewall and your network security. A shell gives a hacker the ability to run commands on a system. Shell access would be used to further exploit SMB. When SMB connects to a service it uses NTLM as a method of authentication and encryption. NTLM uses a hash of the user’s password as well as other information (Microsoft 2019b).

By making the MySQL server perform an SMB check, this will capture the users hashed password, which are then cracked. It took ‘hashcat’, a program used to crack hashes, 12 seconds to crack the password (corporate568).

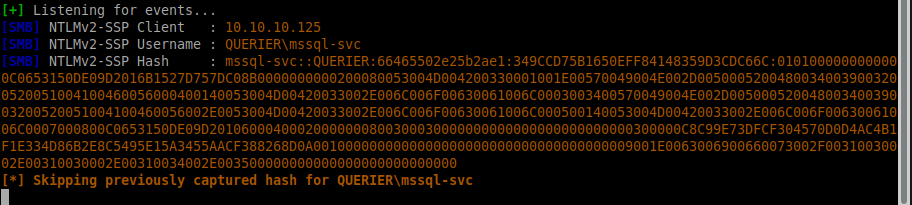


Figure :capturing the NTLM hash



Figure : Shows hashcat cracking the password in 12 seconds and then using it to connect to the MySQL server

This password would be used to further escalate privileges and would finally allow direct access to the Windows system. After further enumeration, the group policy .xml document was found.

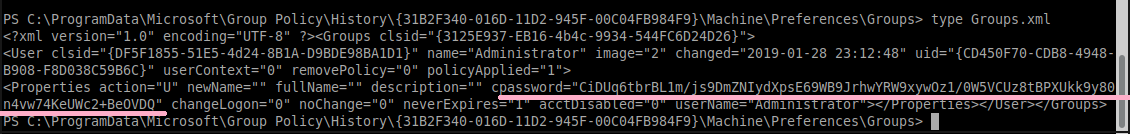


Figure : AES encrypted administrator password in the group policy file

Group policy is used to control what features a user has access to on the system. It can also cache the usernames and hashed passwords of the users who have logged onto the system, including the administrator. Microsoft uses Advanced Encryption Standard (AES) to secure the groups passwords. This means without the private key the password can be difficult to crack. However, Microsoft made the private key public and any password stored in the group policy can now be decoded in seconds (Microsoft 2019c).

The administrator password (MyUnclesAreMarioAndLuigi!!1!) would be used to gain NT Authority\System credentials, the highest authority you can gain on a Windows machine.

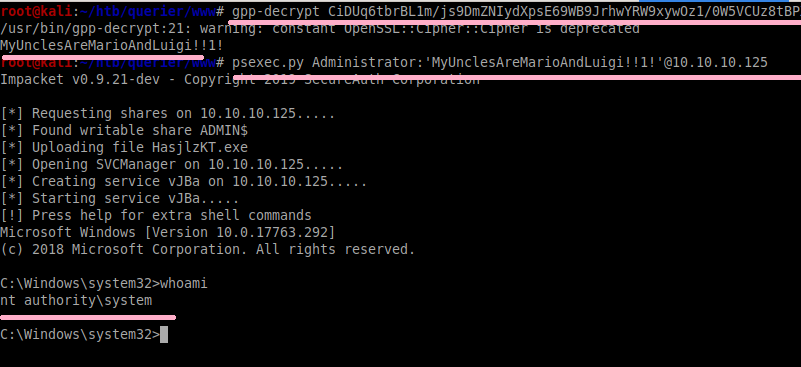


Figure : Shows the administrator password being decrypted and used to gain NT Authority on system

# Gathered credentials

User: Reporting Password: PcwTWTHRwryjc

User: mssql-svc Password: corporate568

User: NT Authority Password: MyUnclesAreMarioAndLuigi!!1!

# Conclusion

The three main ways systems get hacked are;

* Outdated software
* Default and weak passwords
* Phishing attacks

This report is about testing Querier’s systems. This means phishing attacks were out of scope. Of the three passwords discovered, there were no default passwords and one weak password for the mssql-svc user. There was also anonymous access to SMB and passwords saved in the group policy.

For outdated software, both SMB and MySQL were outdated and unpatched. This unpatched software allowed a foothold on to the system and helped gain access to the highest credentials available. Both SMB and MySQL are easily exploitable and can allow even a beginner hacker to gain access to your system.

When creating a network, it is recommended to have multiple layers of defence. This can limit the blast radius of being hacked. These layers can include; active management of operating systems such as patches and updates, stronger encryption of passwords and sensitive files, firewalls and a network intrusion detection system such as SNORT. These should all be top priority for securing your system and would have stopped this attack.

# Recommendations

These are the recommendations for your system right now. For passwords it is recommended that you enforce stronger password limits and require 2 factor authentication (2fa) and disable group policy from storing passwords. If you intend to continue using SMB then it is recommended you update to SMBv3, make it inaccessible from the internet and disable anonymous access. This can be accomplished by blocking it in your firewall and SMBv3 automatically disables anonymous access. For MySQL it is recommended that you update it and only allow access from your internal network. It is also considered bad practise to store sensitive username and passwords in macros.

# References

Microsoft (2017) *Microsoft Security Bulletin MS17-010 - Critical* [online] available from <https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010> [28 November 2019]

Microsoft (2019a) *Windows 10 release information* [online] available from <https://docs.microsoft.com/en-us/windows/release-information> [28 November 2019]

Microsoft (2019b*) 2.2.1.1.4 Password Encryption* [online] available from <https://docs.microsoft.com/en-us/openspecs/windows\_protocols/ms-nlmp/c083583f-1a8f-4afe-a742-6ee08ffeb8cf> [28 November 2019]

Microsoft (2019c) *4.1 NTLM Over Server Message Block (SMB)* [online] available from <https://docs.microsoft.com/en-us/openspecs/windows\_protocols/ms-gppref/2c15cbf0-f086-4c74-8b70-1f2fa45dd4be> [28 November 2019]

Mitre (2019) *Search Results* [online] available from <https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=smb> [28 November 2019]