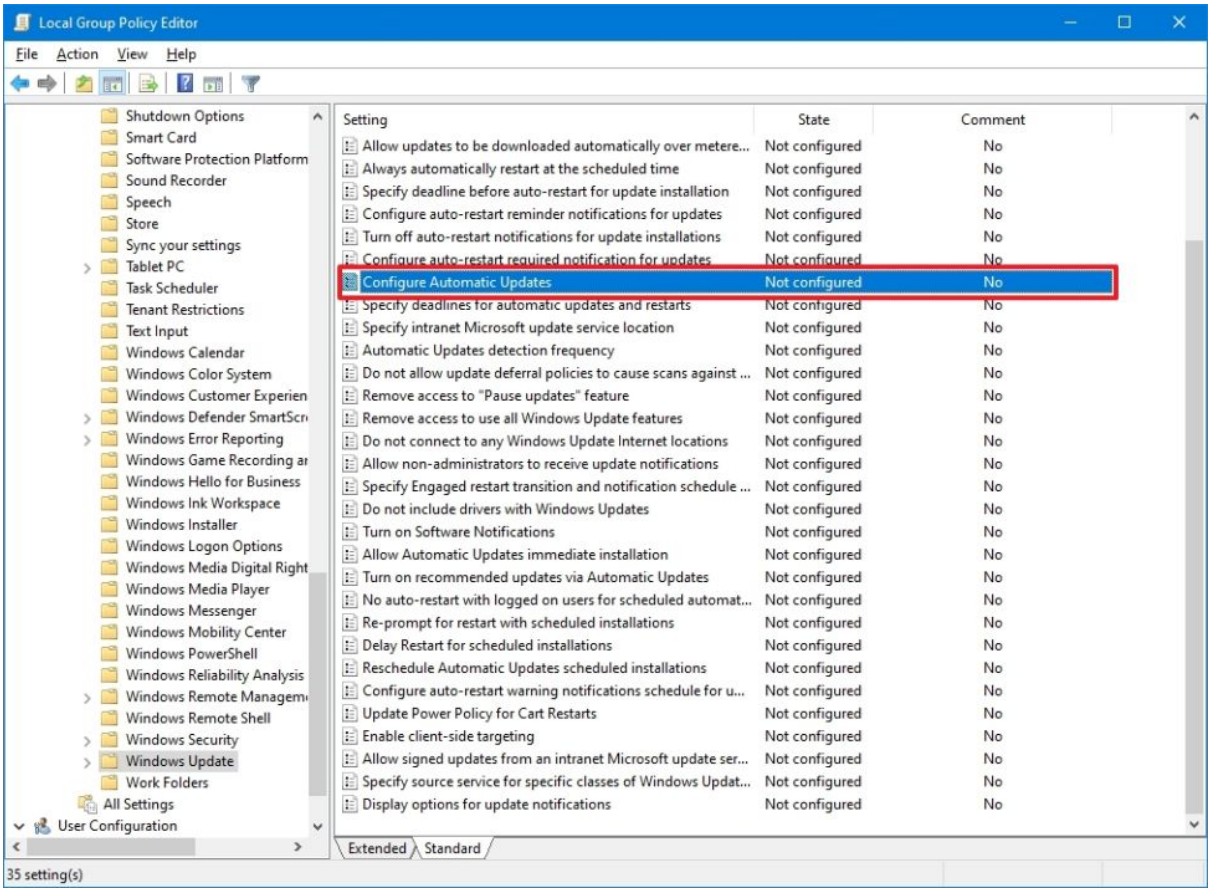
Windows 10 Vulnerable machine

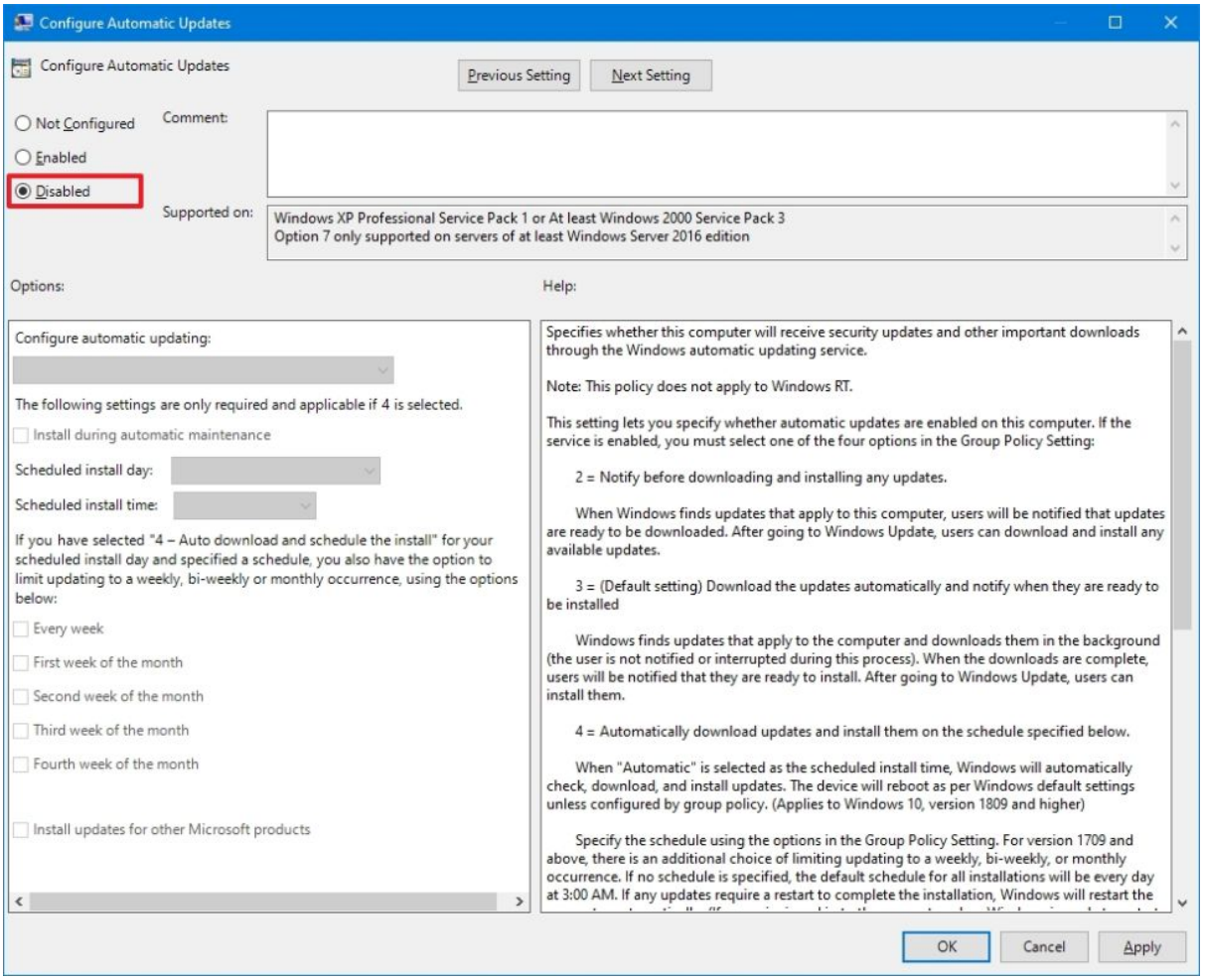
Disable Windows Firewall Permanently

To disable automatic updates on Windows 10 permanently, use these steps:

1. Open **Start.menu**
2. Search for **gpedit.msc** and click the top result to launch the Local Group Policy Editor.
3. Navigate to the following path: Computer Configuration > Administrative Templates > Windows Components > Windows Update
4. Double-click the "Configure Automatic Updates" policy on the right side.



5. Check the Disabled option to turn off automatic Windows 10 updates permanently.



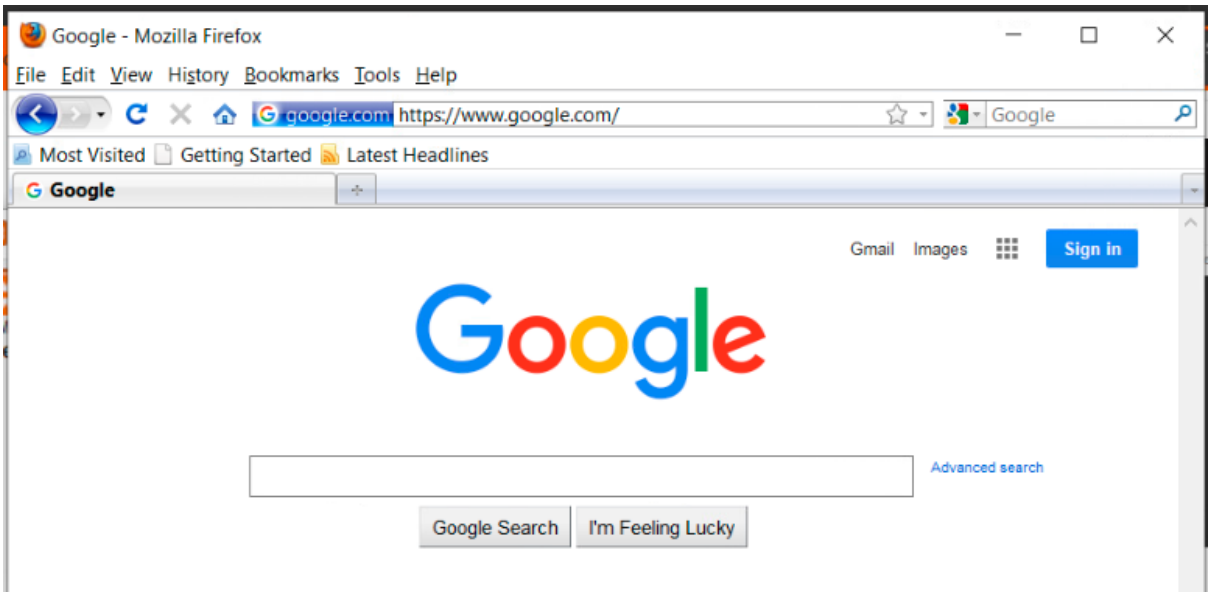
6. Click the Apply button.
7. Click the OK button.

After you complete the steps, Windows 10 will stop downloading updates automatically

Install Outdated Software/Applications

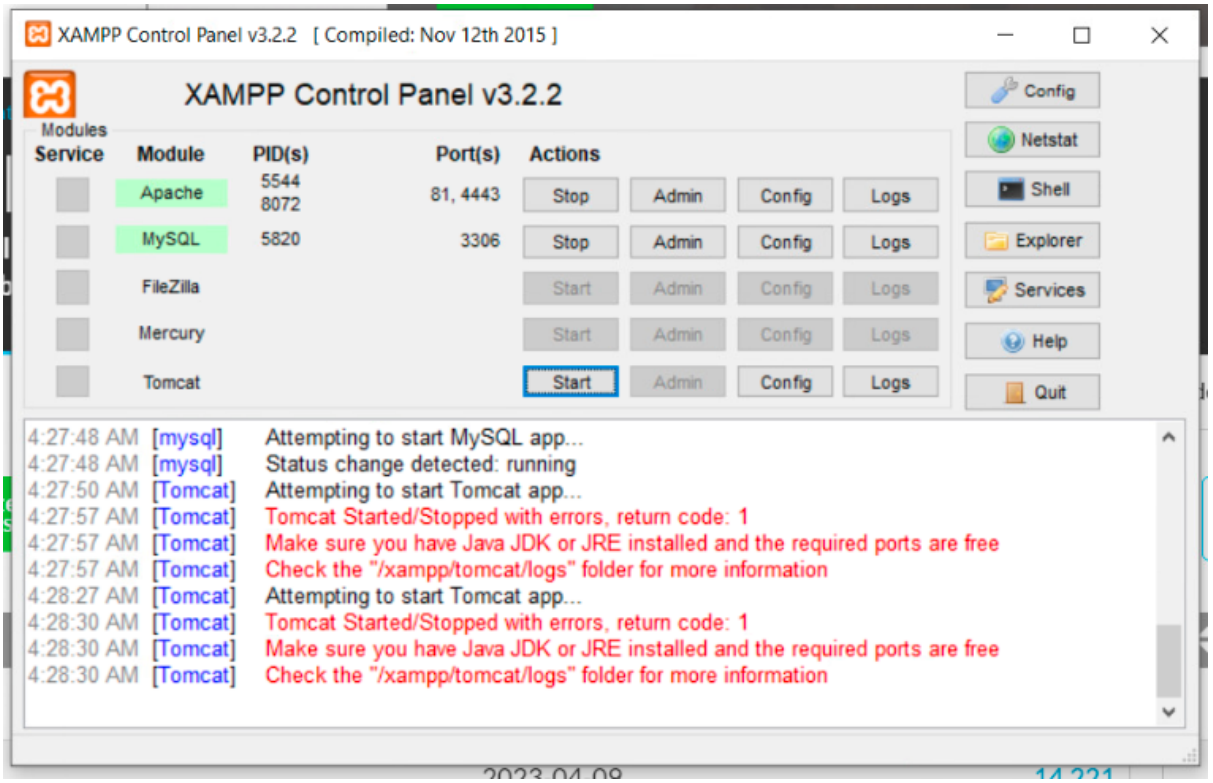
Firefox

- Firefox is a free, open source web browser developed by the Mozilla Foundation and Mozilla Corporation
- Firefox oldest Version link - https://ftp.mozilla.org/pub/mozilla/libraries/win32/



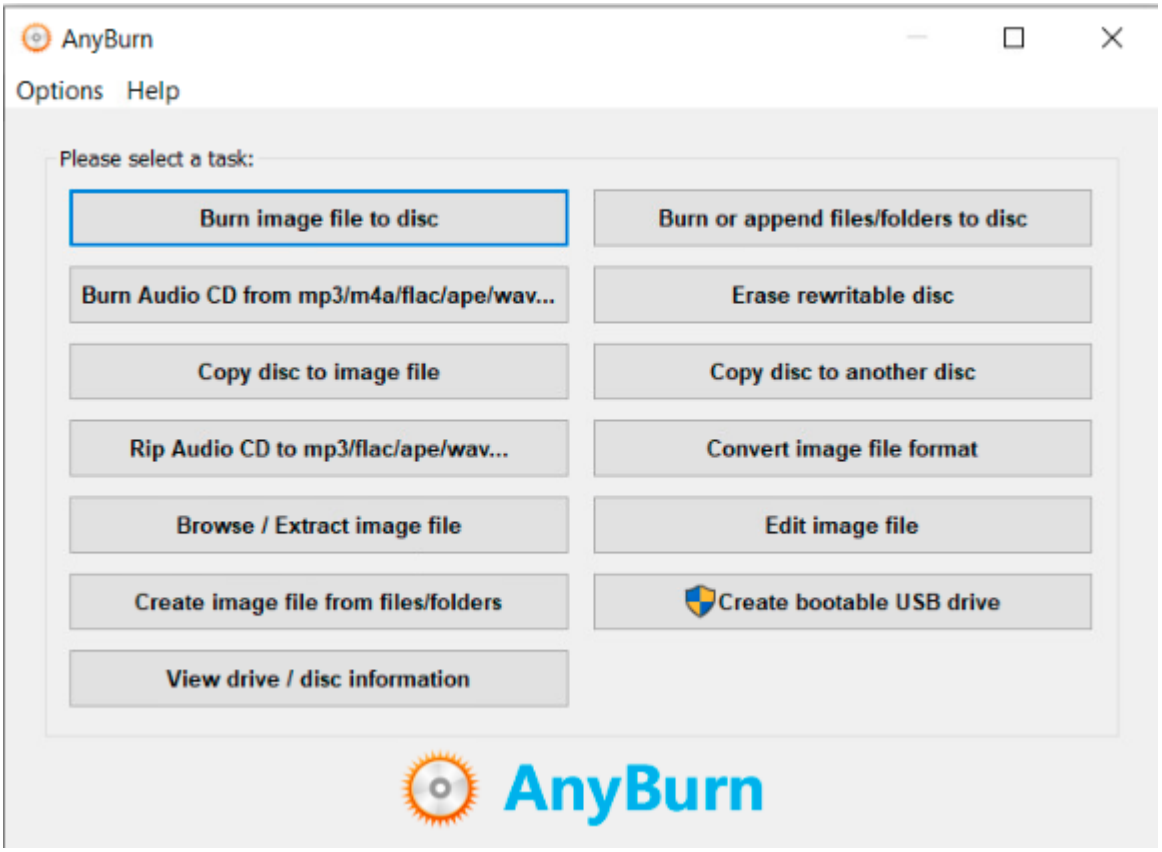
Xampp

- XAMPP is one of the widely used cross-platform web servers, which helps developers to create and test their programs on a local webserver.
- Xampp old version - https://sourceforge.net/projects/xampp/files/XAMPP%20Windows/



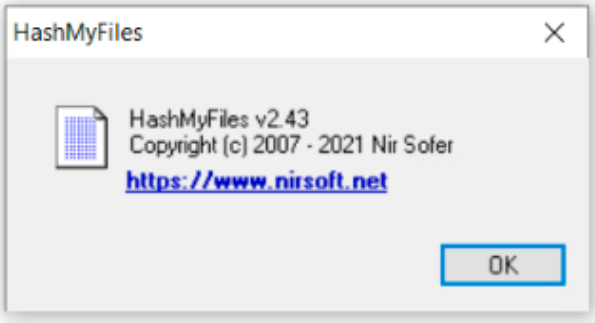
Any burn

- AnyBurn is a lightweight but professional CD / DVD / Blu-ray burning software that everyone must have.
- Any Burn old Version- https://free-any-burn.en.softonic.com/?ex=DINS-635.1



HashMyFile

- HashMyFiles is small utility that allows you to calculate the MD5 and SHA1 hashes of one or more files in your system.
- Hash my File - https://hashmyfiles.soft112.com/



Navicat

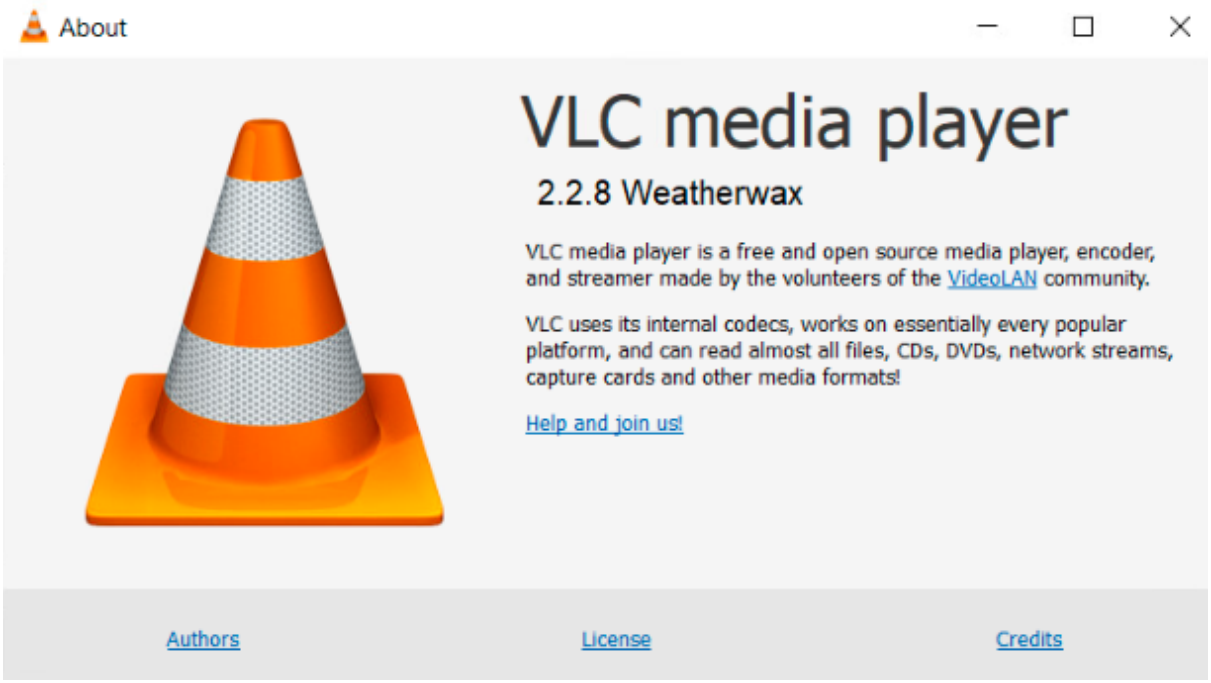
- Navicat is a desktop version of phpmyadmin. Meaning you need to install it on your computer to be able to run it. Phpmyadmin runs on a server.
- Navicat - https://premiumsoft-navicat-premium.software.informer.com/download/

Sqli Hunter

- SQLi-Hunter is a simple #HTTP / #HTTPS proxy server and an #SQLMAP #API wrapper that makes digging SQLi easy.
- Sqli hunter- https://sourceforge.net/projects/sqlihunter/

VLC Media Player

- VLC is a free and open source cross-platform multimedia player and framework that plays most multimedia files, and various streaming
- VIC media player old version- https://download.videolan.org/pub/videolan/vlc/2.2.8/win32/

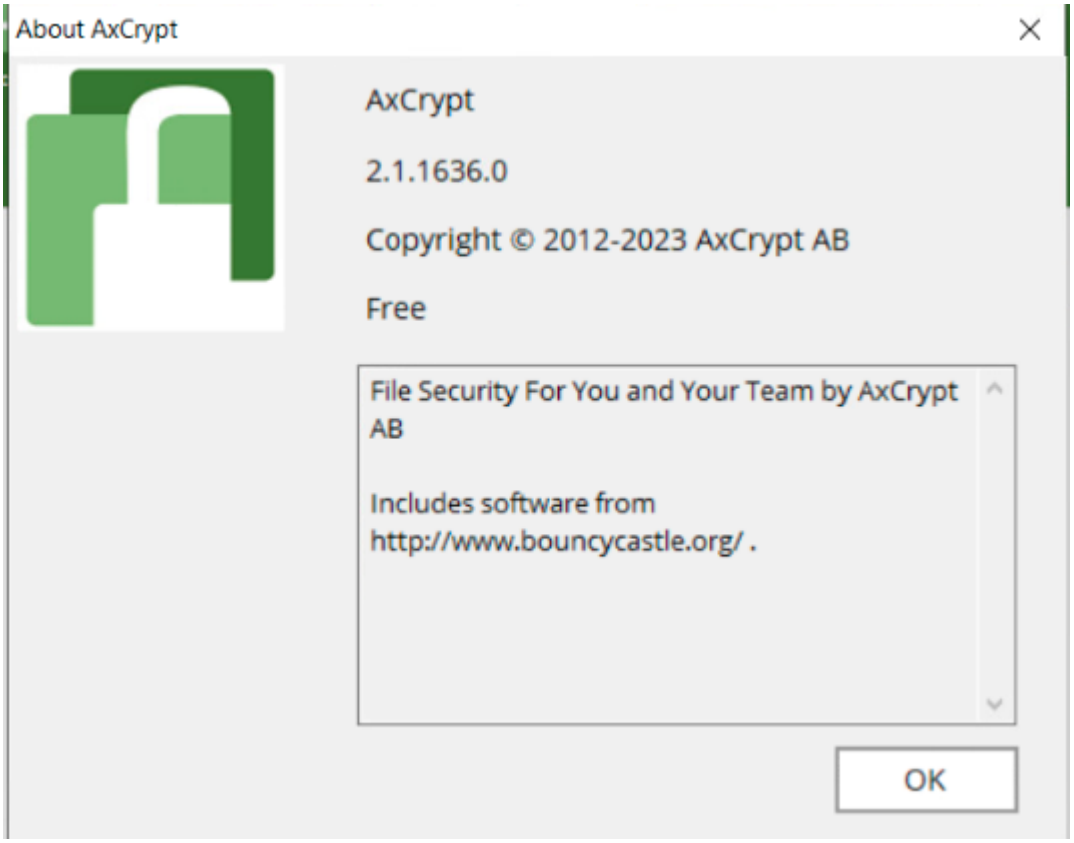


WinRAR

- WinRAR is a trialware file archiver utility for Windows
- It can create and view archives in RAR or ZIP file formats, and unpack numerous archive file formats.
- WinRAR old version - https://www.filehorse.com/download-winrar-32/36813/download/

AxCrypt

- AxCrypt is an affordable open-source file and folder encryption tool that's been around since 2001.
- AxCrypt old version - https://www.techspot.com/downloads/5617-axcrypt.html

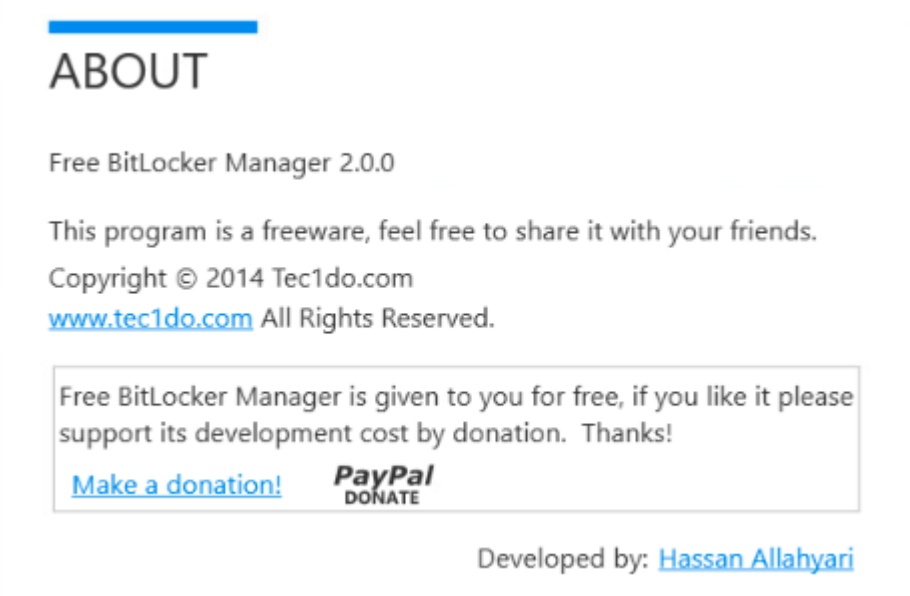


BC Text Encoder

- BCTextEncoder is a line in the BestCrypt family of encryption software products. BCTextEncoder software provides an easy way of encoding and decoding text data.
- BC text encoder old version - https://download.cnet.com/BCTextEncoder/3000-2092_4-75220981.html

FreeBitLockerManager

- Free BitLocker Manager is a strong and yet simple software for managing Microsoft BitLocker drive encryption and is at your service for free
- FreeBitLockerManager old version - https://download.cnet.com/Free-BitLocker-Manager/3000-2092_4-76119984.html



HashCalc

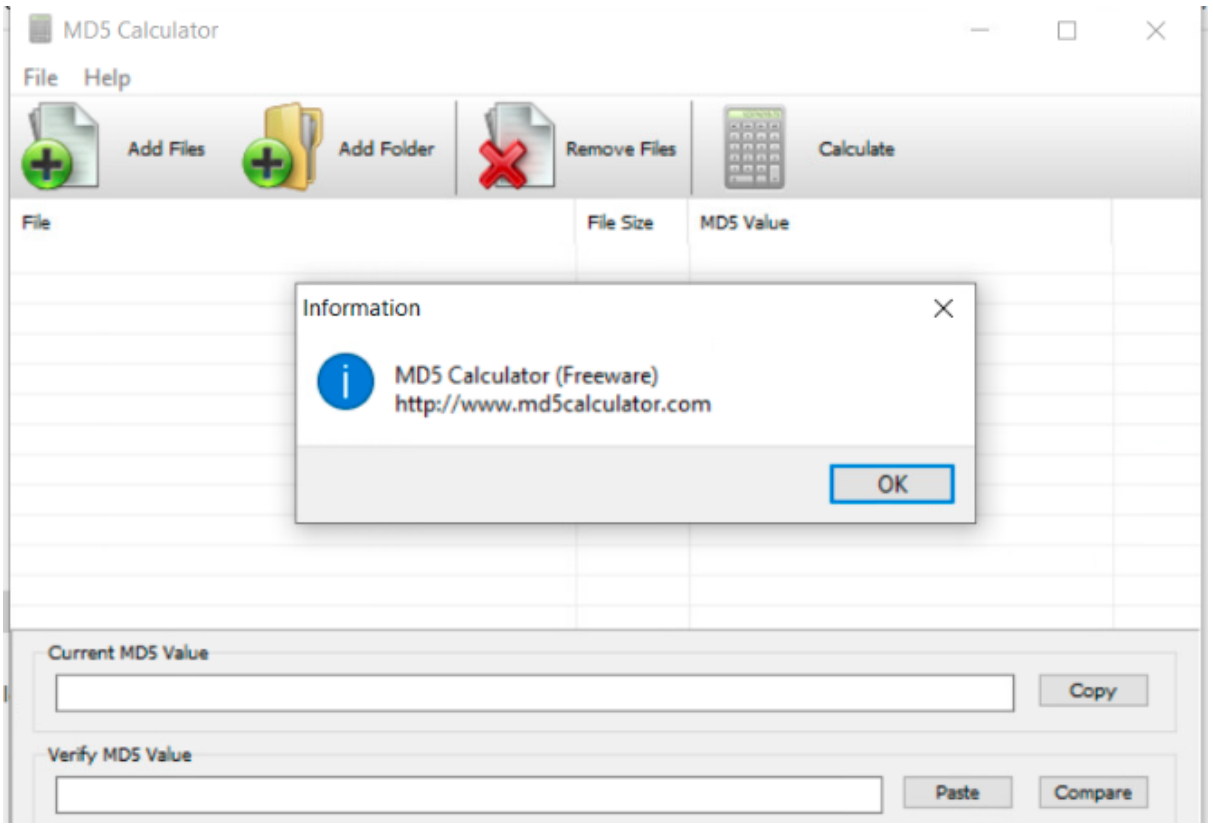
- A fast and easy-to-use calculator that allows to compute message digests, checksums and HMACs for files, as well as for text and hex strings
- HashCalc - https://hashcalc.en.softonic.com/

LophtCrack

- L0phtCrack is a password auditing and recovery application originally produced by Mudge from L0pht Heavy Industries. It is used to test password strength
- LophtCrack 7 - https://l0phtcrack.gitlab.io/releases/7.2.0/lc7setup_v7.2.0_Win64.exe

MD5 Calculator

- MD5 Calculator is a free, simple and easy-to-use MD5 hash value calculation tool, it can quickly calculate, export, import, copy and check MD5 checksum.
- MD5 Calculator - http://www.md5calculator.com/

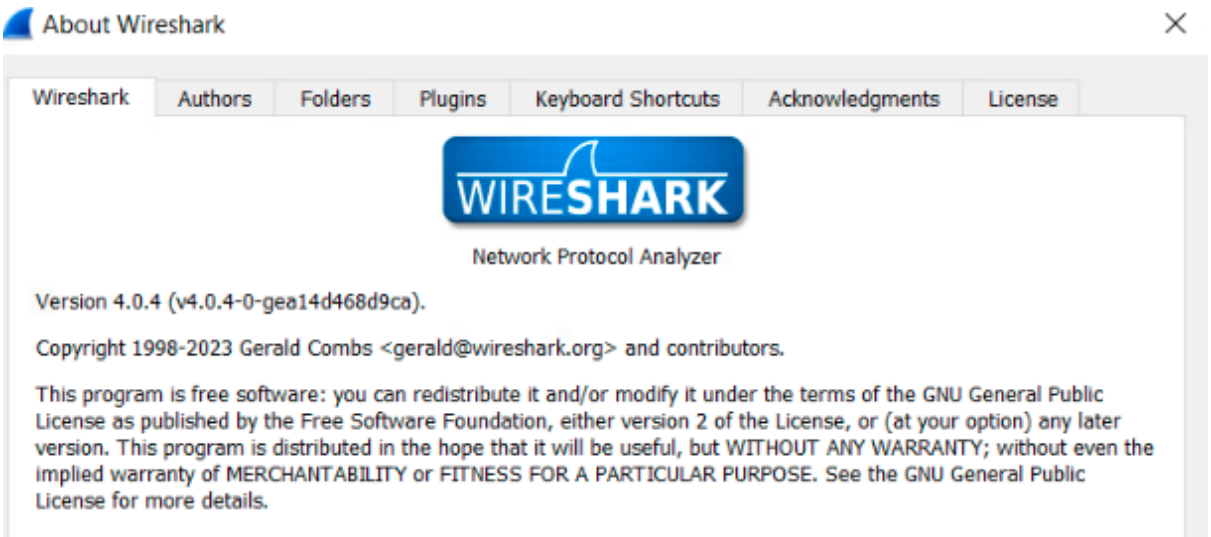


CrypTool

- CrypTool is an open-source project that is a free e-learning software for illustrating cryptographic and cryptanalytic concepts.
- CrypTool old version - https://www.cryptool.org/ct1download/SetupCrypTool_1_4_42_en.exe

Wireshark

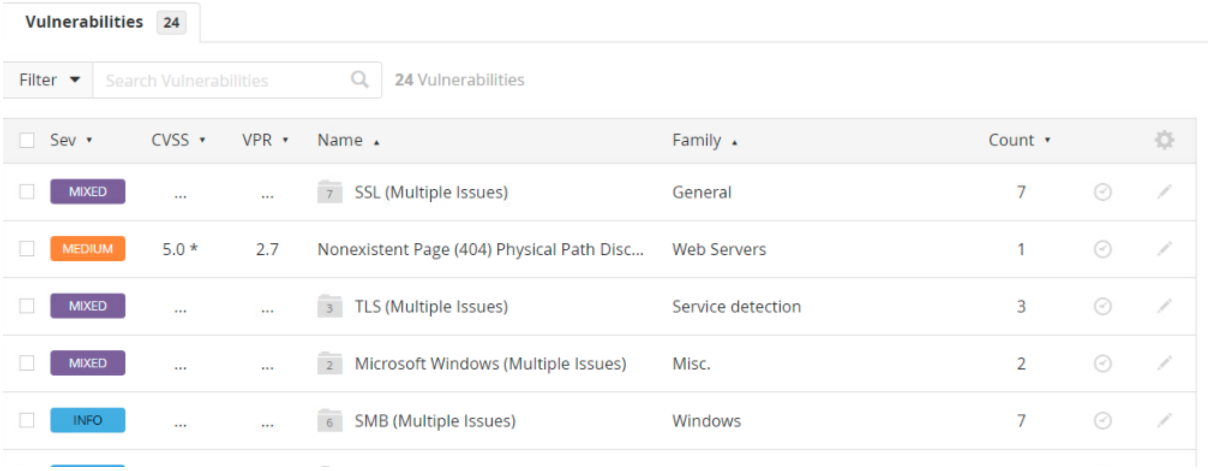
- Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education.
- Wireshark old version - https://wireshark.en.uptodown.com/windows/download



- After installation of vulnerable Application & by enabling the services of Xampp
- Windows will become vulnerable.

Run a Nessus and nmap scan to see the vulnerability and open ports in windows

Nessus Scan



Vulnerabilities 24

Filter | Search Vulnerabilities | 24 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count
MIXED	...	...	SSL (Multiple Issues)	General	7
MEDIUM	5.0 *	2.7	Nonexistent Page (404) Physical Path Disc...	Web Servers	1
MIXED	...	...	TLS (Multiple Issues)	Service detection	3
MIXED	...	...	Microsoft Windows (Multiple Issues)	Misc.	2
INFO	...	...	SMB (Multiple Issues)	Windows	7

Nmap scan Result

```
nmap -T4 -A -v 172.25.10.29
Not shown: 986 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
21/tcp   open  ftp           Microsoft ftpd
| ftp-syst:
|_  SYST: Windows_NT
|_ms-sql-info: ERROR: Script execution failed (use -d to debug)
|_ms-sql-ntlm-info: ERROR: Script execution failed (use -d to debug)
22/tcp   open  ssh           OpenSSH for_Windows_8.1 (protocol 2.0)
|_ms-sql-ntlm-info: ERROR: Script execution failed (use -d to debug)
|_ms-sql-info: ERROR: Script execution failed (use -d to debug)
| ssh-hostkey:
|   3072 8c37def1399f100dc7fff78b6b2f59c2 (RSA)
|   256 e97073e831dea3e942b6319c3273ab20 (ECDSA)
|_  256 1130f5bd3c17a9c9717df13fa483cdd0 (ED25519)
80/tcp   open  http          Microsoft IIS httpd 10.0
|_http-title: IIS Windows
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_ms-sql-ntlm-info: ERROR: Script execution failed (use -d to debug)
|_ms-sql-info: ERROR: Script execution failed (use -d to debug)
|_http-server-header: Microsoft-IIS/10.0
81/tcp   open  http          Apache httpd 2.4.34 ((Win32) OpenSSL/1.1.0i PHP/7.2.9)
|_ms-sql-info: ERROR: Script execution failed (use -d to debug)
|_http-title: Index of /
| http-methods:
|   Supported Methods: POST OPTIONS HEAD GET TRACE
|_  Potentially risky methods: TRACE
|_http-favicon: Unknown favicon MD5: 6EB4A43CB64C97F76562AF703893C8FD
| http-ls: Volume /
|   maxfiles limit reached (10)
| SIZE  TIME              FILENAME
| -     2022-01-29 15:00  Crypticity/
| -     2022-01-29 14:58  Crypticity/Crypticity/
| -     2022-01-29 15:00  Megarex%20Shopping/
| -     2022-01-29 14:58  Megarex%20Shopping/Megarex%20Shopping/
| -     2022-01-29 15:00  Modern%20Cyber%20Corps/
| -     2022-01-29 14:59  Modern%20Cyber%20Corps/Modern%20Cyber%20Corps/
| -     2022-01-29 15:00  ModernCyberCorpsT/
| -     2022-01-29 14:59  ModernCyberCorpsT/ModernCyberCorpsT/
| -     2021-05-05 23:55  OneDrift/
| -     2022-01-29 15:00  Tevel%20Escapes/
|_
|_ms-sql-ntlm-info: ERROR: Script execution failed (use -d to debug)
|_http-server-header: Apache/2.4.34 (Win32) OpenSSL/1.1.0i PHP/7.2.9
```

```
135/tcp  open  msrpc         Microsoft Windows RPC
|_ms-sql-info: ERROR: Script execution failed (use -d to debug)
|_ms-sql-ntlm-info: ERROR: Script execution failed (use -d to debug)
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
|_ms-sql-ntlm-info: ERROR: Script execution failed (use -d to debug)
|_ms-sql-info: ERROR: Script execution failed (use -d to debug)
445/tcp  open  microsoft-ds  Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
|_ms-sql-info: ERROR: Script execution failed (use -d to debug)
|_ms-sql-ntlm-info: ERROR: Script execution failed (use -d to debug)
2869/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Service Unavailable
|_ms-sql-info: ERROR: Script execution failed (use -d to debug)
|_ms-sql-ntlm-info: ERROR: Script execution failed (use -d to debug)
3306/tcp open  mysql         MariaDB (unauthorized)
|_ms-sql-ntlm-info: ERROR: Script execution failed (use -d to debug)
|_ms-sql-info: ERROR: Script execution failed (use -d to debug)
3389/tcp open  ms-wbt-server Microsoft Terminal Services
|_ms-sql-info: ERROR: Script execution failed (use -d to debug)
|_ms-sql-ntlm-info: ERROR: Script execution failed (use -d to debug)
|_ssl-date: 2023-04-17T12:04:59+00:00; 0s from scanner time.
| ssl-cert: Subject: commonName=DESKTOP-RJ713C4
| Issuer: commonName=DESKTOP-RJ713C4
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2023-02-14T04:46:29
| Not valid after:  2023-08-16T04:46:29
| MD5:   887a49a3f53011663f0a095fac32cb62
|_SHA-1: 66e73c85c4f0ddbf1192658815f6561f9b14e19a
```

```
4443/tcp open  http          Apache httpd 2.4.34 ((Win32) OpenSSL/1.1.0i PHP/7.2.9)
|_http-title: Index of /
| http-methods:
|   Supported Methods: POST OPTIONS HEAD GET TRACE
|_  Potentially risky methods: TRACE
|_http-favicon: Unknown favicon MD5: 6EB4A43CB64C97F76562AF703893C8FD
|_ms-sql-ntlm-info: ERROR: Script execution failed (use -d to debug)
| http-ls: Volume /
|   maxfiles limit reached (10)
| SIZE  TIME              FILENAME
| -     2022-01-29 15:00  Crypticity/
| -     2022-01-29 14:58  Crypticity/Crypticity/
| -     2022-01-29 15:00  Megarex%20Shopping/
| -     2022-01-29 14:58  Megarex%20Shopping/Megarex%20Shopping/
| -     2022-01-29 15:00  Modern%20Cyber%20Corps/
| -     2022-01-29 14:59  Modern%20Cyber%20Corps/Modern%20Cyber%20Corps/
| -     2022-01-29 15:00  ModernCyberCorpsT/
| -     2022-01-29 14:59  ModernCyberCorpsT/ModernCyberCorpsT/
| -     2021-05-05 23:55  OneDrift/
| -     2022-01-29 15:00  Tevel%20Escapes/
|_
|_ms-sql-info: ERROR: Script execution failed (use -d to debug)
|_http-server-header: Apache/2.4.34 (Win32) OpenSSL/1.1.0i PHP/7.2.9
5357/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_ms-sql-ntlm-info: ERROR: Script execution failed (use -d to debug)
|_http-title: Service Unavailable
|_ms-sql-info: ERROR: Script execution failed (use -d to debug)
|_http-server-header: Microsoft-HTTPAPI/2.0
5800/tcp open  vnc-http      TightVNC (user: desktop-rj713c4; VNC TCP port: 5900)
|_http-title: TightVNC desktop [desktop-rj713c4]
|_ms-sql-ntlm-info: ERROR: Script execution failed (use -d to debug)
|_ms-sql-info: ERROR: Script execution failed (use -d to debug)
| http-methods:
|_  Supported Methods: GET
5900/tcp open  vnc           VNC (protocol 3.8)
| vnc-info:
|   Protocol version: 3.8
|   Security types:
|     VNC Authentication (2)
|     Tight (16)
|   Tight auth subtypes:
|_    STDV VNCAUTH_ (2)
|_ms-sql-ntlm-info: ERROR: Script execution failed (use -d to debug)
|_ms-sql-info: ERROR: Script execution failed (use -d to debug)
MAC Address: 00:0C:29:0A:36:9A (VMware)
```

EOD