Harsh V. Kushwaha

17BCN7017

Theory Assignment 01

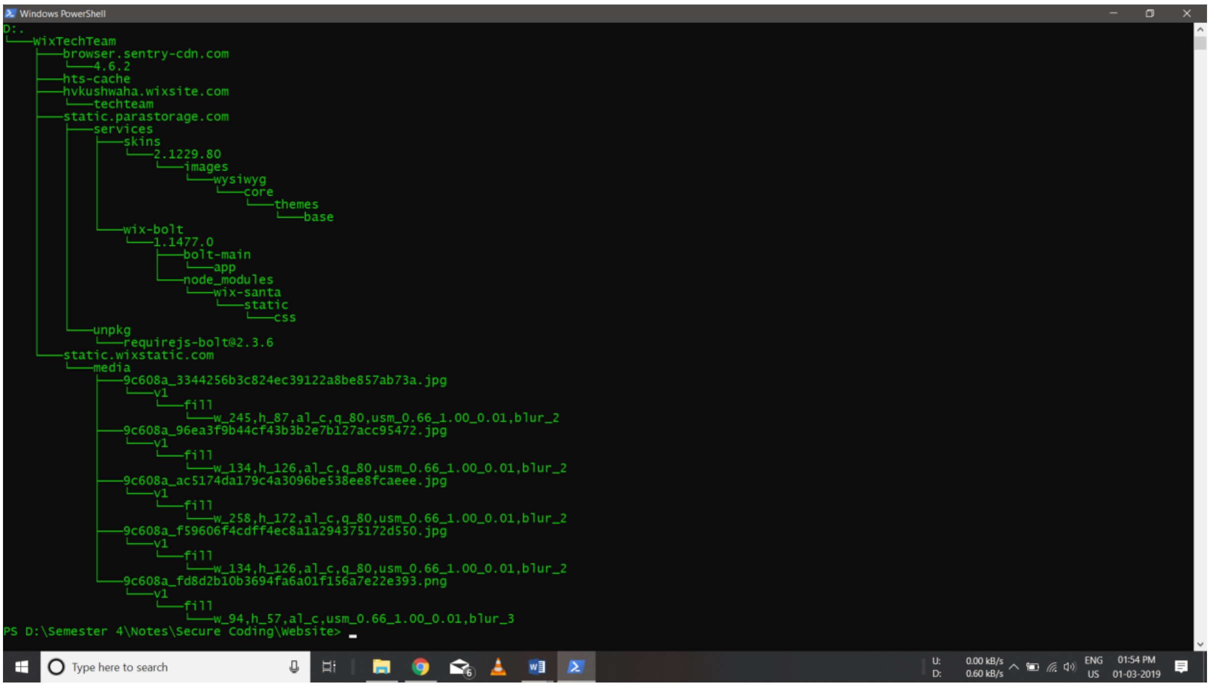
1. **Hosting a simple static webpage on a free server and use httrack to download the static webpage and try httrack on a server side.**

Published the website through wix.com

URL - https://hvkushwaha.wixsitecom/techteam

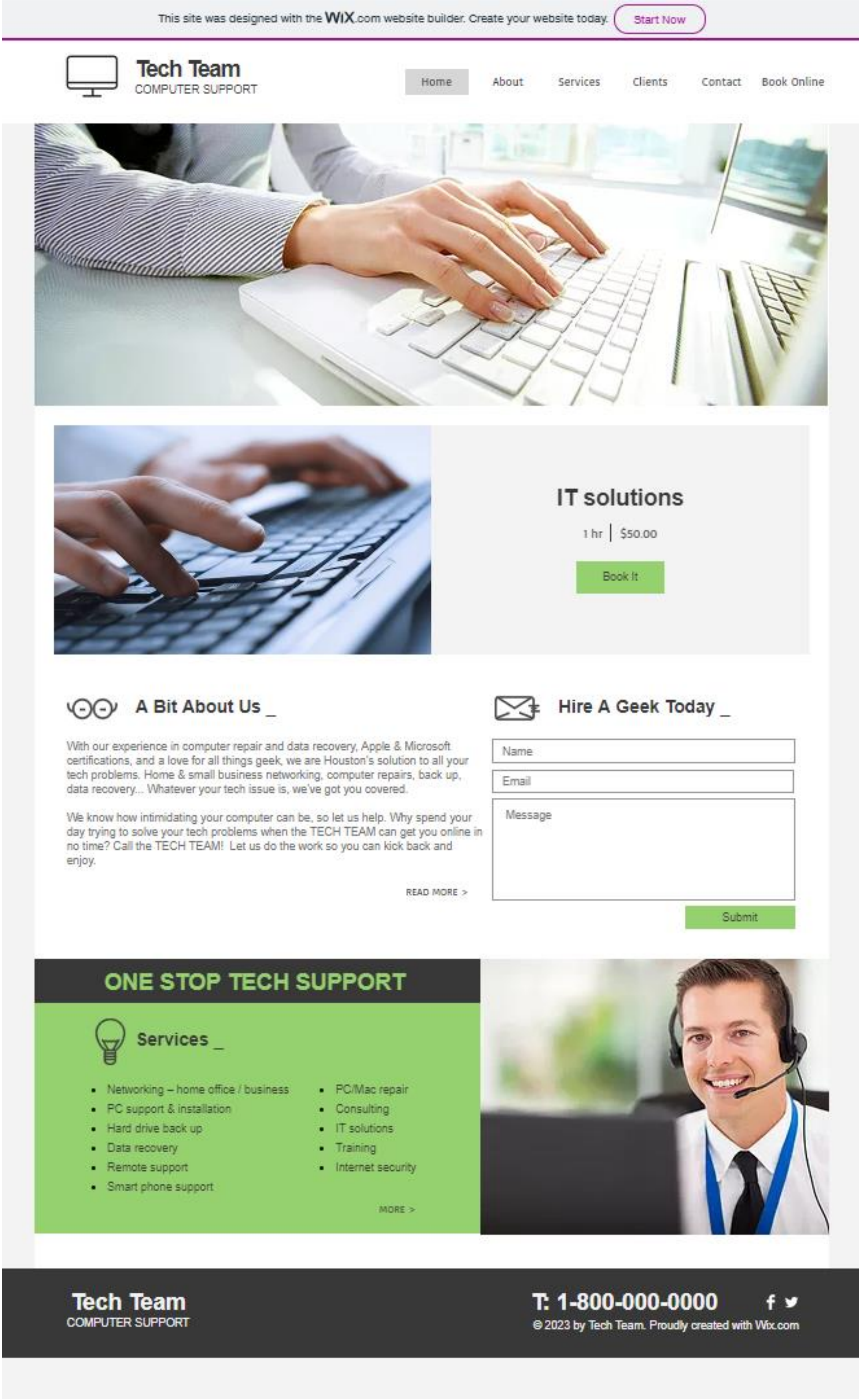
Downloaded it using HTTrack

Tree of the directory



```
D:.
└───WixTechTeam
    ├───browser.sentry-cdn.com
    │   └───4.6.2
    ├───hts-cache
    ├───hvkushwaha.wixsite.com
    │   └───techteam
    ├───static.parastorage.com
    │   ├───services
    │   │   ├───skins
    │   │   │   └───2.1229.80
    │   │   │       └───images
    │   │   │           └───wysiwyg
    │   │   │               └───core
    │   │   │                   └───themes
    │   │   │                       └───base
    │   │   └───wix-bolt
    │   │       └───1.1477.0
    │   │           ├───bolt-main
    │   │           │   └───app
    │   │           └───node_modules
    │   │               └───wix-santa
    │   │                   └───static
    │   │                       └───css
    │   └───unpkg
    │       └───requirejs-bolt@2.3.6
    └───static.wixstatic.com
        └───media
            ├───9c608a_3344256b3c824ec39122a8be857ab73a.jpg
            │   └───v1
            │       └───fill
            │           └───w_245,h_87,al_c,q_80,usm_0.66_1.00_0.01,blur_2
            ├───9c608a_96ea3f9b44cf43b3b2e7b127acc95472.jpg
            │   └───v1
            │       └───fill
            │           └───w_134,h_126,al_c,q_80,usm_0.66_1.00_0.01,blur_2
            ├───9c608a_ac5174da179c4a3096be538ee8fcaeee.jpg
            │   └───v1
            │       └───fill
            │           └───w_258,h_172,al_c,q_80,usm_0.66_1.00_0.01,blur_2
            ├───9c608a_f59606f4cdff4ec8a1a294375172d550.jpg
            │   └───v1
            │       └───fill
            │           └───w_134,h_126,al_c,q_80,usm_0.66_1.00_0.01,blur_2
            └───9c608a_fd8d2b10b3694fa6a01f156a7e22e393.png
                └───v1
                    └───fill
                        └───w_94,h_57,al_c,usm_0.66_1.00_0.01,blur_3
PS D:\Semester 4\Notes\Secure Coding\Website> _
```

The live website looks like –



This site was designed with the WIX.com website builder. Create your website today. Start Now

Tech Team
COMPUTER SUPPORT

Home About Services Clients Contact Book Online

IT solutions

1 hr | $50.00

Book It

A Bit About Us _

With our experience in computer repair and data recovery, Apple & Microsoft certifications, and a love for all things geek, we are Houston's solution to all your tech problems. Home & small business networking, computer repairs, back up, data recovery... Whatever your tech issue is, we've got you covered.

We know how intimidating your computer can be, so let us help. Why spend your day trying to solve your tech problems when the TECH TEAM can get you online in no time? Call the TECH TEAM! Let us do the work so you can kick back and enjoy.

READ MORE >

Hire A Geek Today _

Name

Email

Message

Submit

ONE STOP TECH SUPPORT

Services _

- Networking – home office / business
- PC support & installation
- Hard drive back up
- Data recovery
- Remote support
- Smart phone support
- PC/Mac repair
- Consulting
- IT solutions
- Training
- Internet security

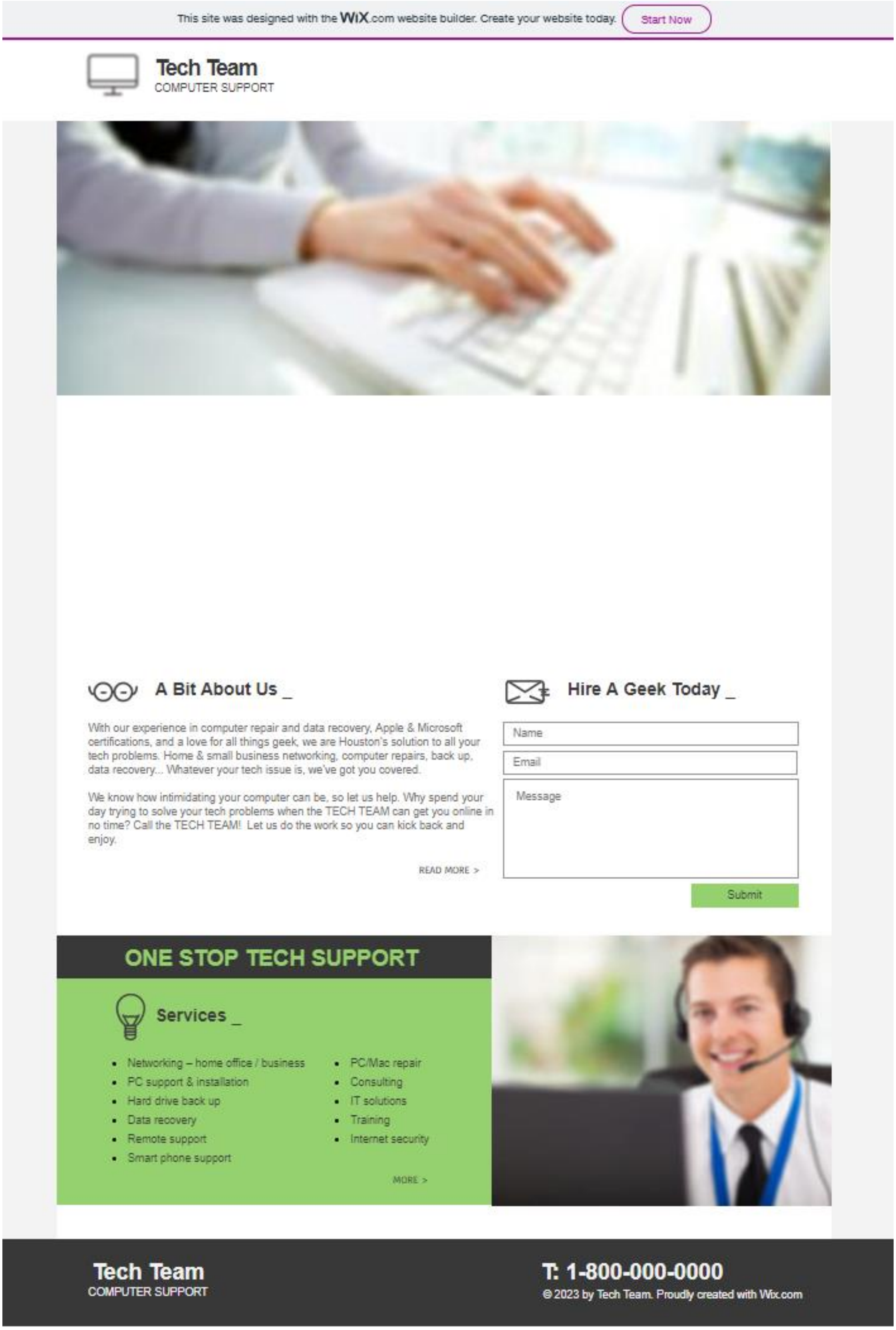
MORE >

Tech Team
COMPUTER SUPPORT

T: 1-800-000-0000

© 2023 by Tech Team. Proudly created with Wix.com

The website downloaded by HTTrack looks like:



This site was designed with the WIX.com website builder. Create your website today. Start Now

Tech Team
COMPUTER SUPPORT

A Bit About Us _

With our experience in computer repair and data recovery, Apple & Microsoft certifications, and a love for all things geek, we are Houston's solution to all your tech problems. Home & small business networking, computer repairs, back up, data recovery... Whatever your tech issue is, we've got you covered.

We know how intimidating your computer can be, so let us help. Why spend your day trying to solve your tech problems when the TECH TEAM can get you online in no time? Call the TECH TEAM! Let us do the work so you can kick back and enjoy.

READ MORE >

Hire A Geek Today _

Name

Email

Message

Submit

ONE STOP TECH SUPPORT

Services _

- Networking – home office / business
- PC support & installation
- Hard drive back up
- Data recovery
- Remote support
- Smart phone support
- PC/Mac repair
- Consulting
- IT solutions
- Training
- Internet security

MORE >

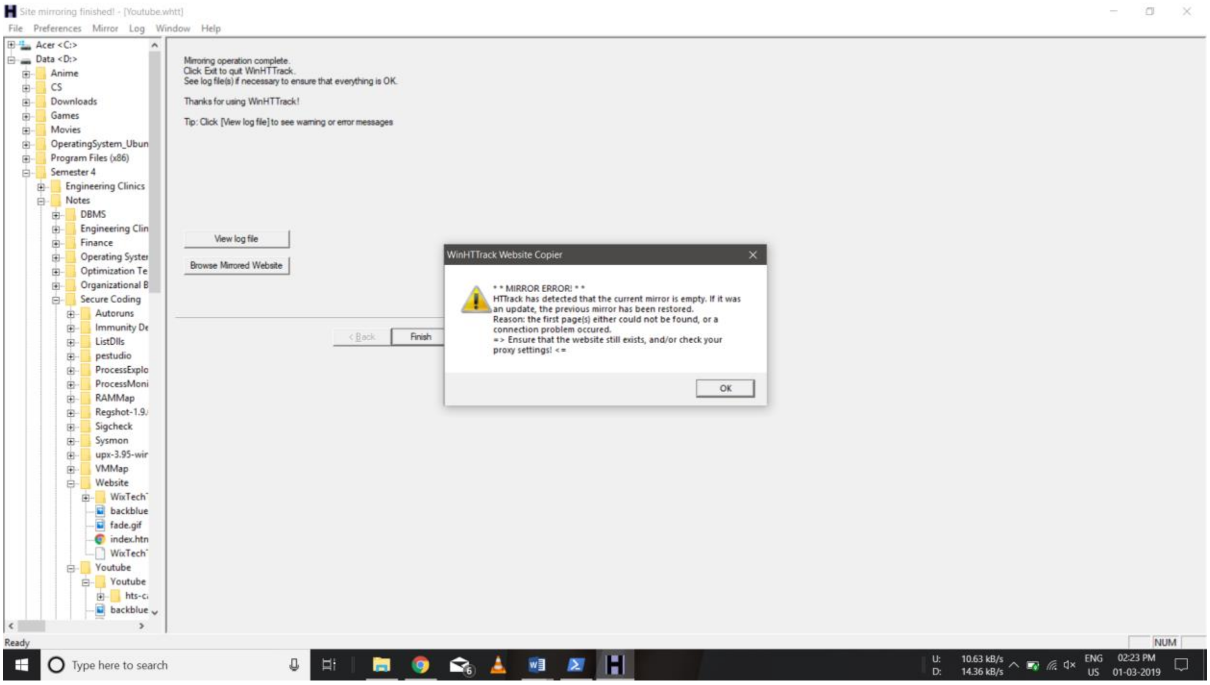
Tech Team
COMPUTER SUPPORT

T: 1-800-000-0000
© 2023 by Tech Team. Proudly created with Wix.com

There was a ‘Let’s Chat’ option available on the website which is not present in the downloaded website. Also, the price the of IT Solution got vanished in the downloaded version.

Now trying to use HTTtack on a server-side. For example – let’s take https://www.youtube.com.

We get an error like this –


Site mirroring finished! - [Youtube.whtt]
File Preferences Mirror Log Window Help
View log file
Browse Mirrored Website
< Back
Finish
WinHTTrack Website Copier
OK

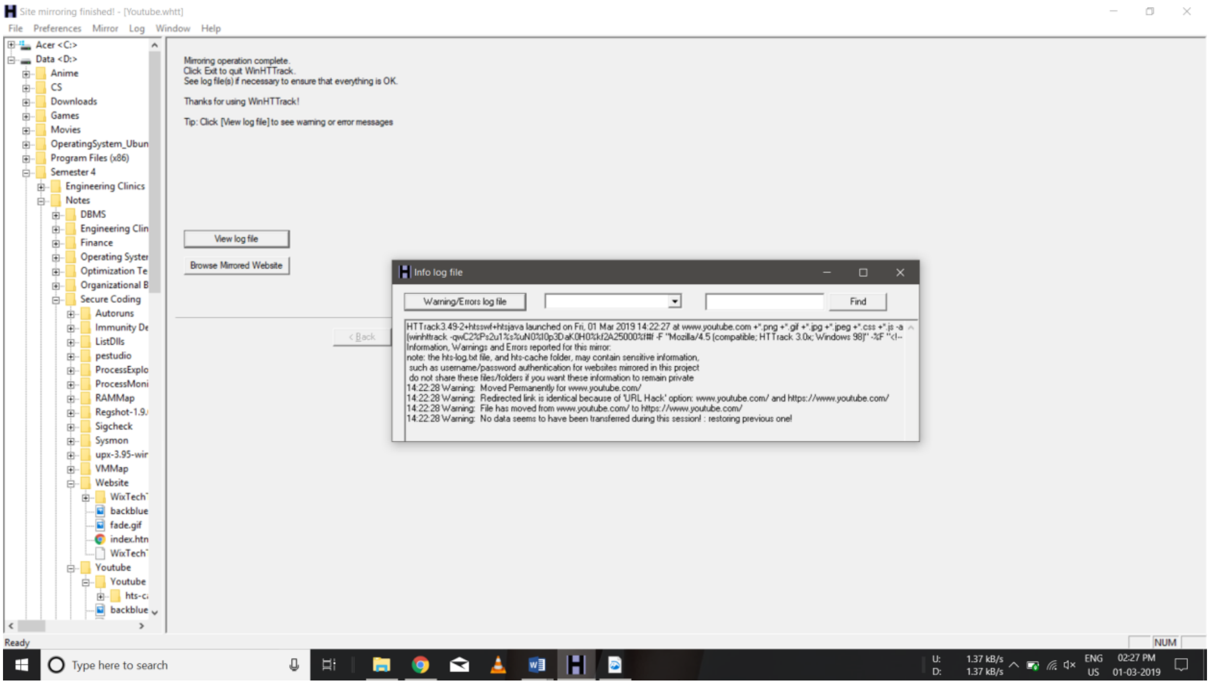
```
Mirroring operation complete.
Click Exit to quit WinHTTrack.
See log file(s) if necessary to ensure that everything is OK.

Thanks for using WinHTTrack!

Tip: Click [View log file] to see warning or error messages
```

```
* * MIRROR ERROR! * *
HTTrack has detected that the current mirror is empty. If it was
an update, the previous mirror has been restored.
Reason: the first page(s) either could not be found, or a
connection problem occured.
=> Ensure that the website still exists, and/or check your
proxy settings! <=
```

The log file –



Mirroring operation complete.
Click Exit to quit WinHTTrack.
See log file(s) if necessary to ensure that everything is OK.

Thanks for using WinHTTrack!

Tip: Click [View log file] to see warning or error messages

```
HTTrack3.49-2+htsswf+htsjava launched on Fri, 01 Mar 2019 14:22:27 at www.youtube.com +*.png +*.gif +*.jpg +*.jpeg +*.css +*.js -a
(winhttrack -qwC2%Ps2u1%s%uN0%I0p3DaK0H0%kf2A25000%f#f -F "Mozilla/4.5 (compatible; HTTrack 3.0x; Windows 98)" -%F "<!--
Information, Warnings and Errors reported for this mirror:
note: the hts-log.txt file, and hts-cache folder, may contain sensitive information,
 such as username/password authentication for websites mirrored in this project
 do not share these files/folders if you want these information to remain private
14:22:28 Warning:  Moved Permanently for www.youtube.com/
14:22:28 Warning:  Redirected link is identical because of 'URL Hack' option: www.youtube.com/ and https://www.youtube.com/
14:22:28 Warning:  File has moved from www.youtube.com/ to https://www.youtube.com/
14:22:28 Warning:  No data seems to have been transferred during this session! : restoring previous one!
```

2. Brief description about SQL Injection.

SQL injection usually occurs when you ask a user for input, like their username / userId, and instead of a name/id, the user gives you an SQL statement that you will **unknowingly** run on your database.

Example

```
txtUserId = getRequestString("UserId");
txtSQL = "SELECT * FROM Users WHERE UserId = " + txtUserId;
```

If there is nothing to prevent a user from entering "wrong" input, the user can enter some "smart" input like this:

```
UserId = 105 OR 1 = 1
```

Then, the SQL statement will look like:

```
SELECT * FROM Users WHERE UserId = 105 OR 1=1;
```

The SQL above is valid and will return ALL rows from the "Users" table, since **OR 1=1** is always TRUE.

3. What is XSS? How does it cause information leakage?

Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it.

The malicious content sent to the web browser often takes the form of a segment of JavaScript, but may also include HTML, Flash, or any other type of code that the browser may execute. The variety of attacks based on XSS is almost limitless, but they commonly include transmitting private data, like cookies or other session information, to the attacker, redirecting the victim to web content controlled by the attacker, or performing other malicious operations on the user's machine under the guise of the vulnerable site.

4. Explain in detail about GDPR.

The General Data Protection Regulation (EU) 2016/679 ("GDPR") is a regulation in EU law on data protection and privacy for all individuals within the European Union (EU) and the European Economic Area (EEA). It also addresses the export of personal data outside the EU and EEA areas. The GDPR aims primarily to give control to individuals over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU. Superseding the Data Protection Directive 95/46/EC, the regulation contains provisions and requirements pertaining to the processing of personal data of individuals (formally called data subjects in the GDPR) inside the EEA and applies to an enterprise established in the EEA or—

regardless of its location and the data subjects' citizenship—that is processing the personal information of data subjects inside the EEA.

The GDPR consists of 99 articles, grouped into 11 chapters, and an additional 171 recitals with explanatory remarks. The chapters' headings are:

I – General provisions

II – Principles

III – Rights of the data subject

IV – Controller and processor

V – Transfers of personal data to third countries or international organisations

VI – Independent supervisory authorities

VII – Cooperation and consistency

VIII – Remedies, liability and penalties

IX – Provisions relating to specific processing situations

X – Delegated acts and implementing acts

XI – Final provisions

Unless a data subject has provided informed consent to data processing for one or more purposes, personal data may not be processed unless there is at least one legal basis to do so. According to Article 6, the lawful purposes are:

(a) If the data subject has given consent to the processing of his or her personal data;

(b) To fulfil contractual obligations with a data subject, or for tasks at the request of a data subject who is in the process of entering into a contract;

(c) To comply with a data controller's legal obligations;

(d) To protect the vital interests of a data subject or another individual;

(e) To perform a task in the public interest or in official authority;

(f) For the legitimate interests of a data controller or a third party, unless these interests are overridden by interests of the data subject or her or his rights according to the Charter of Fundamental Rights (especially in the case of children).

5. What is Windows exploit guard? Where is it used?

Windows Defender Exploit Guard (Windows Defender EG) is a new set of host intrusion prevention capabilities for Windows 10, allowing you to manage and reduce the attack surface of apps used by your employees.

There are four features in Windows Defender EG:

1. Exploit protection can apply exploit mitigation techniques to apps your organization uses, both individually and to all apps. Works with third-party antivirus solutions and Windows Defender Antivirus (Windows Defender AV).
2. Attack surface reduction rules can reduce the attack surface of your applications with intelligent rules that stop the vectors used by Office-, script- and mail-based malware. Requires Windows Defender AV.
3. Network protection extends the malware and social engineering protection offered by Windows Defender SmartScreen in Microsoft Edge to cover network traffic and connectivity on your organization's devices. Requires Windows Defender AV.
4. Controlled folder access helps protect files in key system folders from changes made by malicious and suspicious apps, including file-encrypting ransomware malware. Requires Windows Defender AV.

Windows 10, version 1803 provides additional protections:

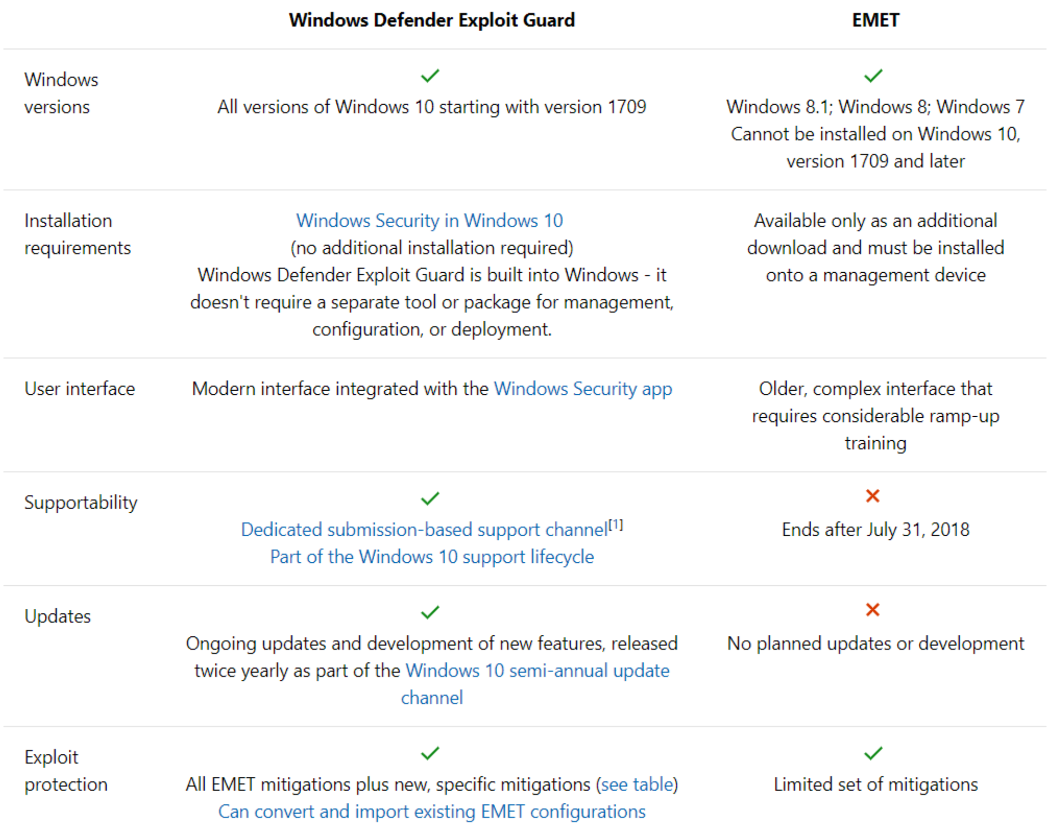
- New Attack surface reduction rules
- Controlled folder access can now block disk sectors

6. Why EMET removed in Windows 10?

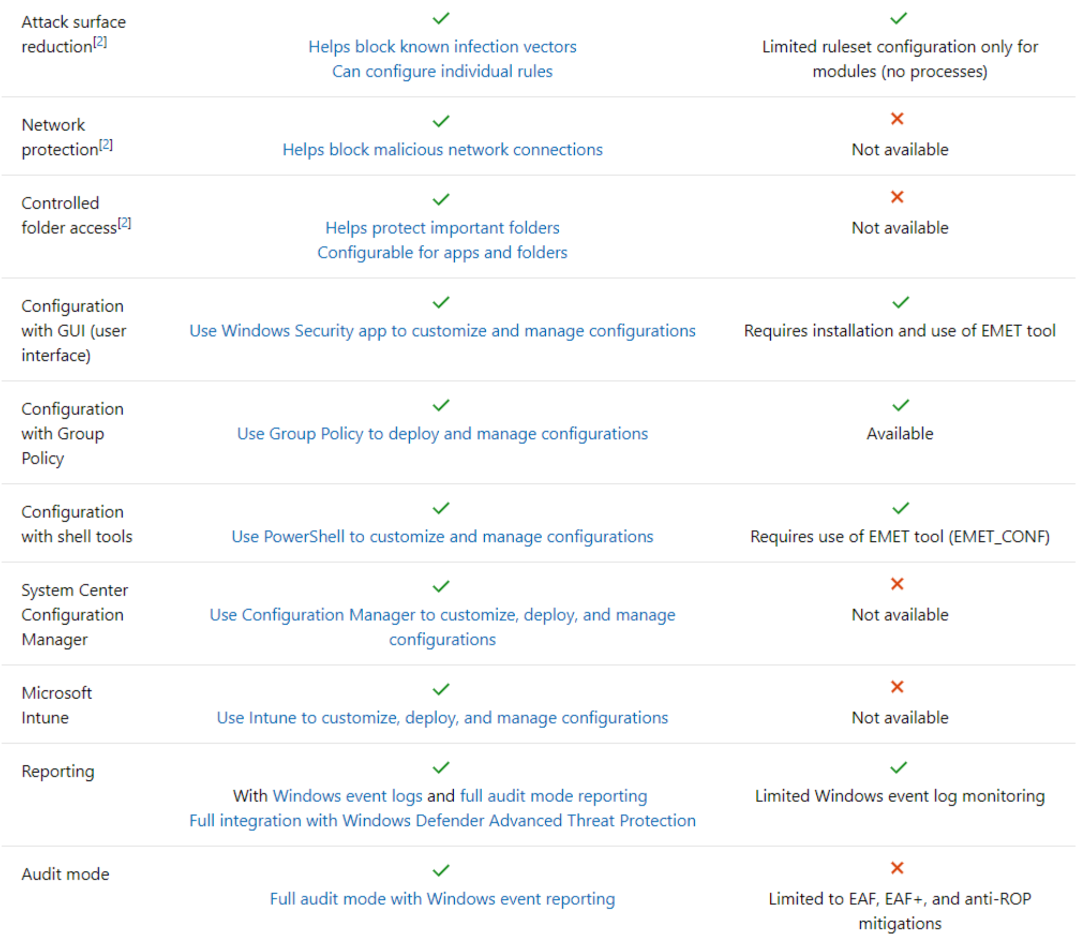
The Enhanced Mitigation Experience Toolkit (EMET) is a utility that helps prevent vulnerabilities in software from being successfully exploited. EMET achieves this goal by using security mitigation technologies. These technologies function as special protections and obstacles that an exploit author must defeat to exploit software vulnerabilities. These security mitigation technologies do not guarantee that vulnerabilities cannot be exploited. However, they work to make exploitation as difficult as possible to perform.

EMET also provides a configurable SSL/TLS certificate pinning feature that is called Certificate Trust. This feature is intended to detect (and stop, with EMET 5.0) man-in-the-middle attacks that are leveraging the public key infrastructure (PKI).

Microsoft removed EMET in the fall creator’s update and integrated it in the Windows Defender Advanced Threat Protection (ATP) service. The following is the comparison between Windows Defender Exploit Guard and EMET.

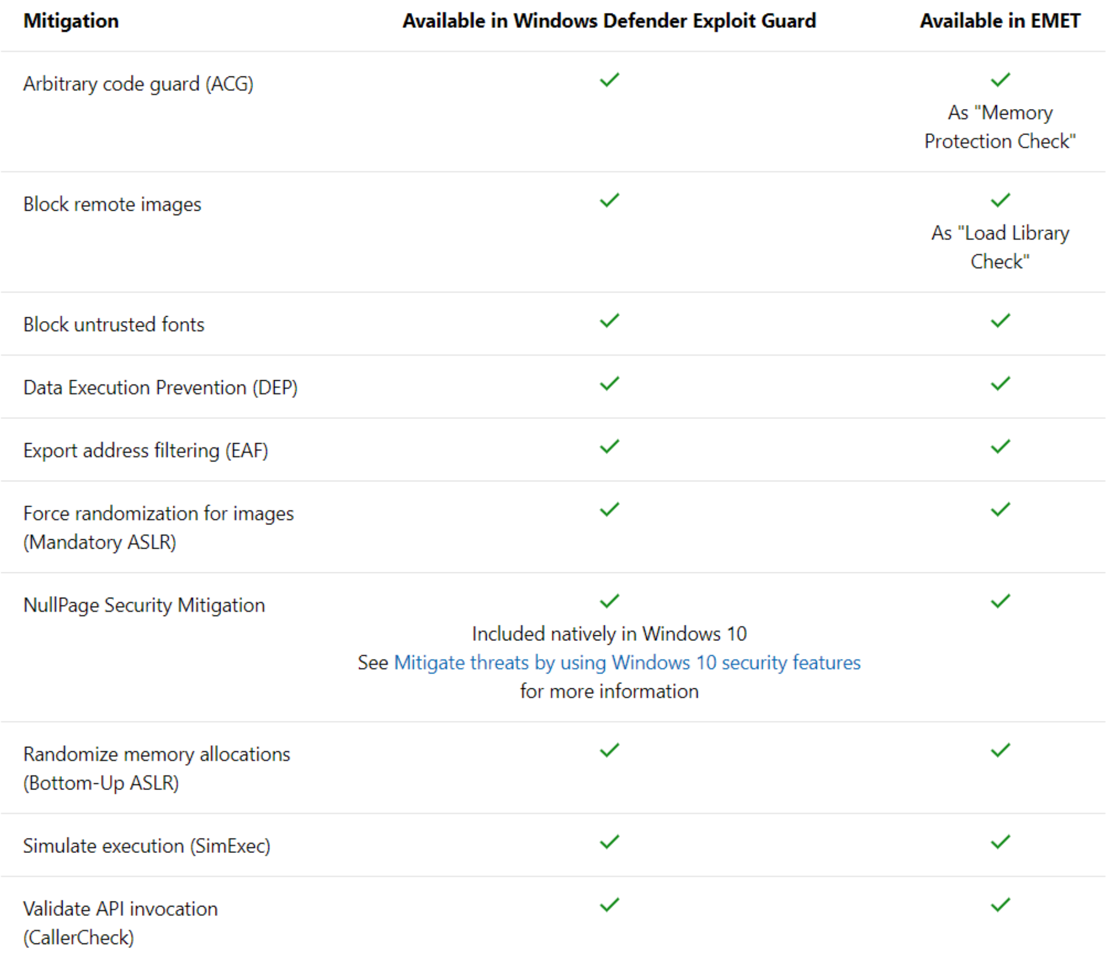


	Windows Defender Exploit Guard	EMET
Windows versions	✓ All versions of Windows 10 starting with version 1709	✓ Windows 8.1; Windows 8; Windows 7 Cannot be installed on Windows 10, version 1709 and later
Installation requirements	Windows Security in Windows 10 (no additional installation required) Windows Defender Exploit Guard is built into Windows - it doesn't require a separate tool or package for management, configuration, or deployment.	Available only as an additional download and must be installed onto a management device
User interface	Modern interface integrated with the Windows Security app	Older, complex interface that requires considerable ramp-up training
Supportability	✓ Dedicated submission-based support channel[1] Part of the Windows 10 support lifecycle	✗ Ends after July 31, 2018
Updates	✓ Ongoing updates and development of new features, released twice yearly as part of the Windows 10 semi-annual update channel	✗ No planned updates or development
Exploit protection	✓ All EMET mitigations plus new, specific mitigations (see table) Can convert and import existing EMET configurations	✓ Limited set of mitigations

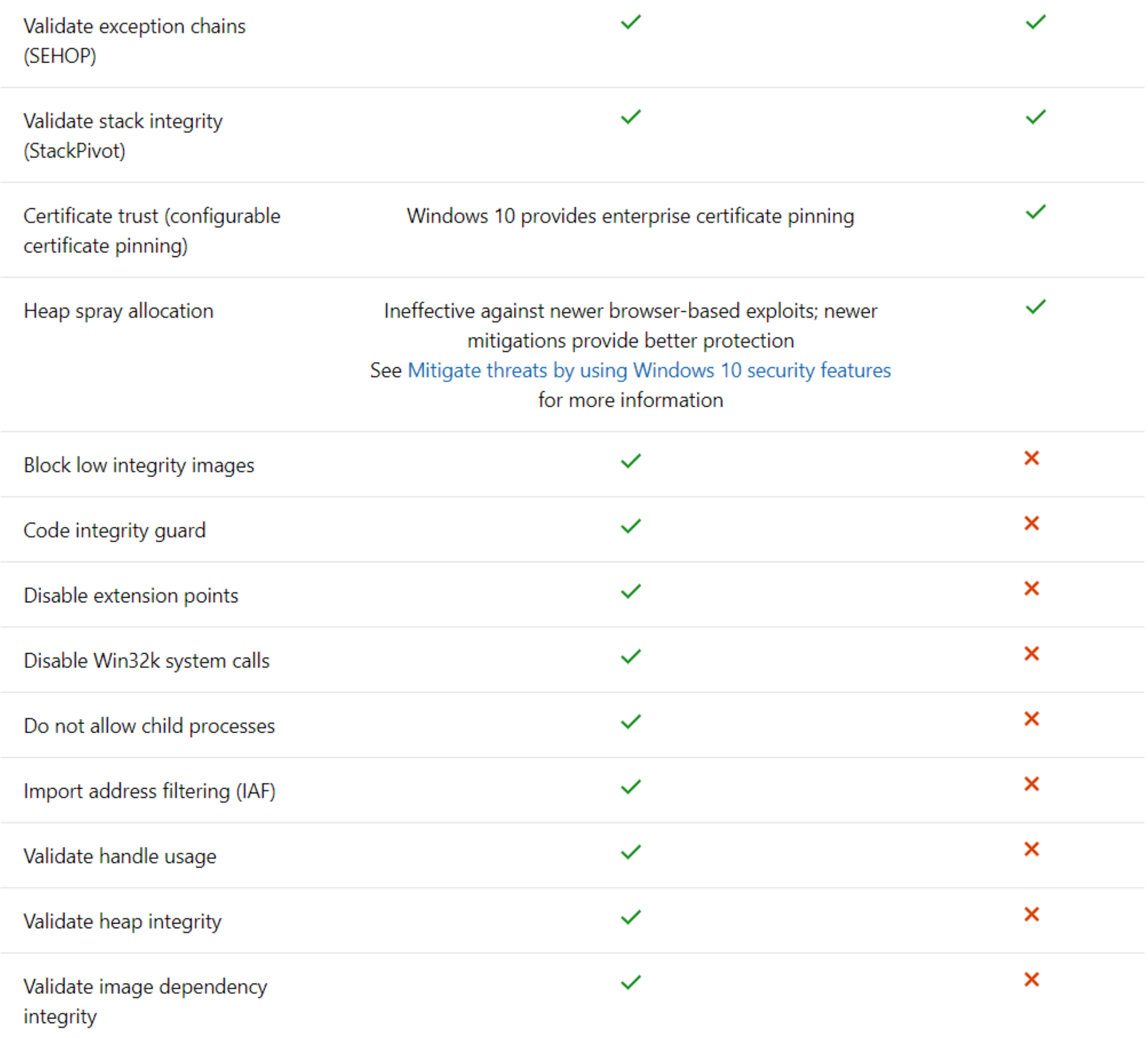


Attack surface reduction[2]	✓ Helps block known infection vectors Can configure individual rules	✓ Limited ruleset configuration only for modules (no processes)
Network protection[2]	✓ Helps block malicious network connections	✗ Not available
Controlled folder access[2]	✓ Helps protect important folders Configurable for apps and folders	✗ Not available
Configuration with GUI (user interface)	✓ Use Windows Security app to customize and manage configurations	✓ Requires installation and use of EMET tool
Configuration with Group Policy	✓ Use Group Policy to deploy and manage configurations	✓ Available
Configuration with shell tools	✓ Use PowerShell to customize and manage configurations	✓ Requires use of EMET tool (EMET_CONF)
System Center Configuration Manager	✓ Use Configuration Manager to customize, deploy, and manage configurations	✗ Not available
Microsoft Intune	✓ Use Intune to customize, deploy, and manage configurations	✗ Not available
Reporting	✓ With Windows event logs and full audit mode reporting Full integration with Windows Defender Advanced Threat Protection	✓ Limited Windows event log monitoring
Audit mode	✓ Full audit mode with Windows event reporting	✗ Limited to EAF, EAF+, and anti-ROP mitigations

Mitigation Comparison –



Mitigation	Available in Windows Defender Exploit Guard	Available in EMET
Arbitrary code guard (ACG)	✓	✓ As "Memory Protection Check"
Block remote images	✓	✓ As "Load Library Check"
Block untrusted fonts	✓	✓
Data Execution Prevention (DEP)	✓	✓
Export address filtering (EAF)	✓	✓
Force randomization for images (Mandatory ASLR)	✓	✓
NullPage Security Mitigation	✓ Included natively in Windows 10 See Mitigate threats by using Windows 10 security features for more information	✓
Randomize memory allocations (Bottom-Up ASLR)	✓	✓
Simulate execution (SimExec)	✓	✓
Validate API invocation (CallerCheck)	✓	✓



Validate exception chains (SEHOP)	✓	✓
Validate stack integrity (StackPivot)	✓	✓
Certificate trust (configurable certificate pinning)	Windows 10 provides enterprise certificate pinning	✓
Heap spray allocation	Ineffective against newer browser-based exploits; newer mitigations provide better protection See Mitigate threats by using Windows 10 security features for more information	✓
Block low integrity images	✓	✗
Code integrity guard	✓	✗
Disable extension points	✓	✗
Disable Win32k system calls	✓	✗
Do not allow child processes	✓	✗
Import address filtering (IAF)	✓	✗
Validate handle usage	✓	✗
Validate heap integrity	✓	✗
Validate image dependency integrity	✓	✗

7. Write briefly how recovery software works.

Let's take the example of a book which is now old, and you want to throw it in the dustbin. If you want to recover the book you can pretty much go and take the book back from the dustbin. But what if the recycling company comes and collects the garbage. You would pretty much have to go to their facility and search the for the book yourself. Suppose they remove the cover of all the books and collects all the pages and keep it separately. It would be very difficult to search for the book now. Maybe it's a family photo album or a novel you were writing from a very long time. So, you would be happy even if you get the pages back.

Similarly, whenever you delete a file from your system, it first goes in the recycle bin and it is pretty much still accessible but when you delete it from recycle bin then the system removes the address of that file, but it is still present there. The space where it was located is now available for new files to move in. If there was no allocation, your file is still present in the bits 0 and 1. You just need a professional tool which can access the memory location and collect your file.

File recovery programs can be used to resurrect files of any type or size, from pictures, music and videos to documents and spreadsheets. Data recovery software can locate and restore emails, executables and compressed files. The best file recovery software can even maintain the folder organization of your files, and it may be able to recover a complete partition or drive.

8. What is Thunking and why Thunking is necessary for Windows?

A thunk is a subroutine used to inject an additional calculation into another subroutine. Thunks are primarily used to delay a calculation until its result is needed, or to insert operations at the beginning or end of the other subroutine. It can simply be thought of as a function that takes no arguments, waiting to be called upon to do its work. They have a variety of other applications in compiler code generation and modular programming.

Kernel-mode drivers must validate the size of any I/O buffer passed in from a user-mode application. If a 32-bit application passes a buffer containing pointer-precision data types to a 64-bit driver, and no thunking takes place, the driver will expect the buffer to be larger than it actually is. This is because pointer precision is 32 bits on 32-bit Microsoft Windows and 64 bits on 64-bit Windows. For example, consider the following structure definition:

```
typedef struct _DRIVER_DATA
{
    HANDLE          Event;
    UNICODE_STRING  ObjectName;
} DRIVER_DATA;
```

On 32-bit Windows, the size of the DRIVER_DATA structure is 12 bytes.

HANDLE Event UNICODE_STRING ObjectName USHORT Length USHORT Maximum Length PWSTR Buffer 32 bits (4 bytes) 16 bits (2 bytes) 16 bits (2 bytes) 32 bits (4 bytes)

On 64-bit Windows, the size of the DRIVER_DATA structure is 24 bytes. (The 4 bytes of structure padding are required so that the Buffer member can be aligned on an 8-byte boundary.)

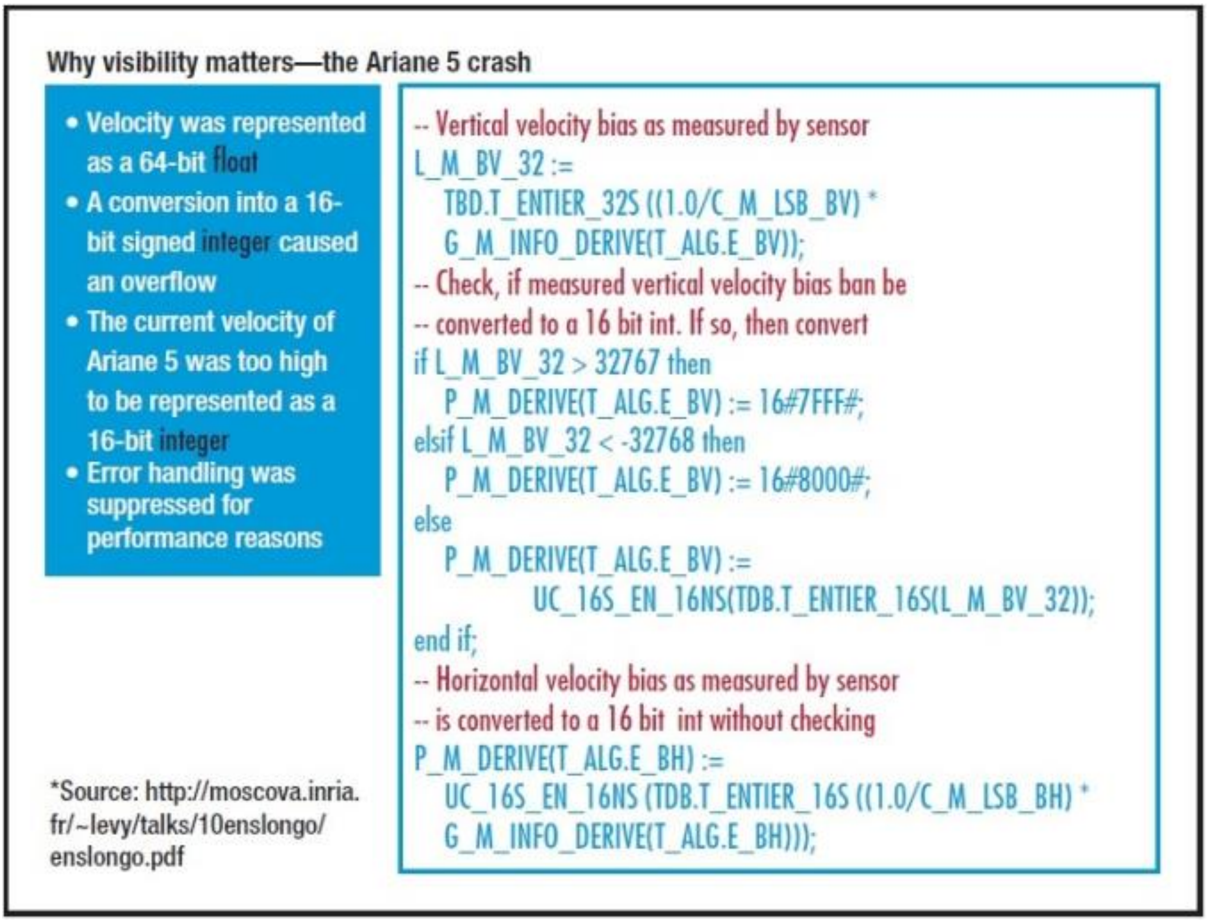
HANDLE Event UNICODE_STRING ObjectName USHORT Length USHORT Maximum Length Empty (Structure Padding) PWSTR Buffer 64 bits (8 bytes) 16 bits (2 bytes) 16 bits (2 bytes) 32 bits (4 bytes) 64 bits (8 bytes)

If a 64-bit driver receives 12 bytes of DRIVER_DATA when it expected 24 bytes, the size validation will fail. To prevent this, the driver must detect whether a DRIVER_DATA structure was sent by a 32-bit application, and if so, thunk it appropriately before performing the validation.

9. Case study: signed overflow, Ariane 5.

Ariane 5 is a European expendable heavy lift launch vehicle that is part of the Ariane rocket family. It is used to deliver payloads into geostationary transfer orbit (GTO) or low Earth orbit (LEO), can launch two-three satellites, and up to eight micro satellites at a time.

Ariane 5 is a two-stage heavy class booster rocket. Length — 52-53 m, maximum diameter — 5.4 m, starting weight: 775-780 tonnes (depending on the configuration)



Why visibility matters—the Ariane 5 crash

- Velocity was represented as a 64-bit float
- A conversion into a 16-bit signed integer caused an overflow
- The current velocity of Ariane 5 was too high to be represented as a 16-bit integer
- Error handling was suppressed for performance reasons

```
-- Vertical velocity bias as measured by sensor
L_M_BV_32 :=
   TBD.T_ENTIER_32S ((1.0/C_M_LSB_BV) *
   G_M_INFO_DERIVE(T_ALG.E_BV));
-- Check, if measured vertical velocity bias ban be
-- converted to a 16 bit int. If so, then convert
if L_M_BV_32 > 32767 then
   P_M_DERIVE(T_ALG.E_BV) := 16#7FFF#;
elsif L_M_BV_32 < -32768 then
   P_M_DERIVE(T_ALG.E_BV) := 16#8000#;
else
   P_M_DERIVE(T_ALG.E_BV) :=
            UC_16S_EN_16NS(TDB.T_ENTIER_16S(L_M_BV_32));
end if;
-- Horizontal velocity bias as measured by sensor
-- is converted to a 16 bit  int without checking
P_M_DERIVE(T_ALG.E_BH) :=
   UC_16S_EN_16NS (TDB.T_ENTIER_16S ((1.0/C_M_LSB_BH) *
   G_M_INFO_DERIVE(T_ALG.E_BH)));
```

*Source: http://moscova.inria.fr/~levy/talks/10enslongo/enslongo.pdf

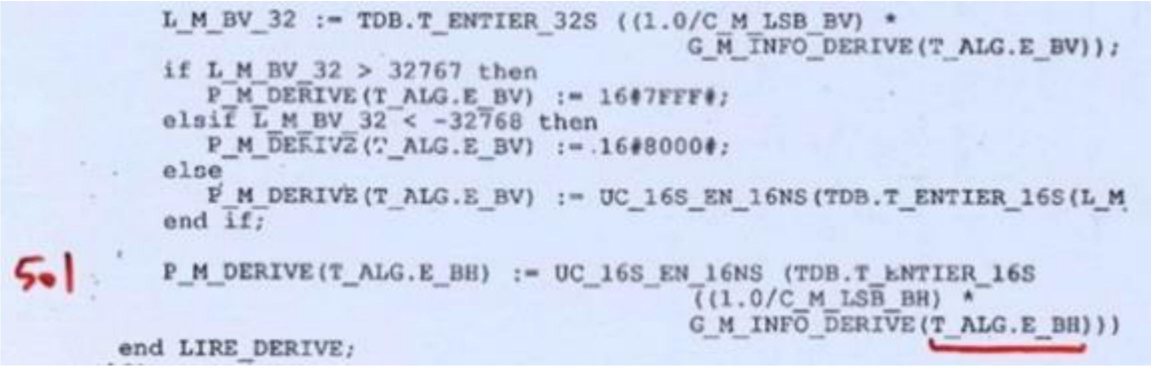
The investigation revealed that this software module contained seven variables involved in type conversion operations. It turned out that the developers performed the analysis for the vulnerability of all operations, capable of throwing an exception.

It was their conscious action – to add adequate protection to four variables and leave three of them – including BH – unprotected. The ground for this decision was the certainty that overflow is not possible in these variables in general.

This confidence was supported by the evaluations, showing that the expected range of physical parameters that was taken as the basis for the determination of the values of the mentioned variables can never lead to an undesirable situation. And it was true — but for the trajectory evaluated for Ariane 4.

The new generation Ariane 5 rocket launched on an entirely different trajectory, for which no evaluations were carried out. Meanwhile, it turned out that the "horizontal velocity" (together with the initial acceleration) exceeded the estimated (for Ariane 4) more than five times.

The protection of all 7 (including BH) variables wasn't provided because the maximum workload for the IRS computer was declared as 80%. The developers had to look for ways to reduce unnecessary evaluation expenses, and they weakened the protection in that fragment where theoretically the accident could not happen. When it occurred, then the exception handling mechanism was activated, which turned out to be completely inadequate.

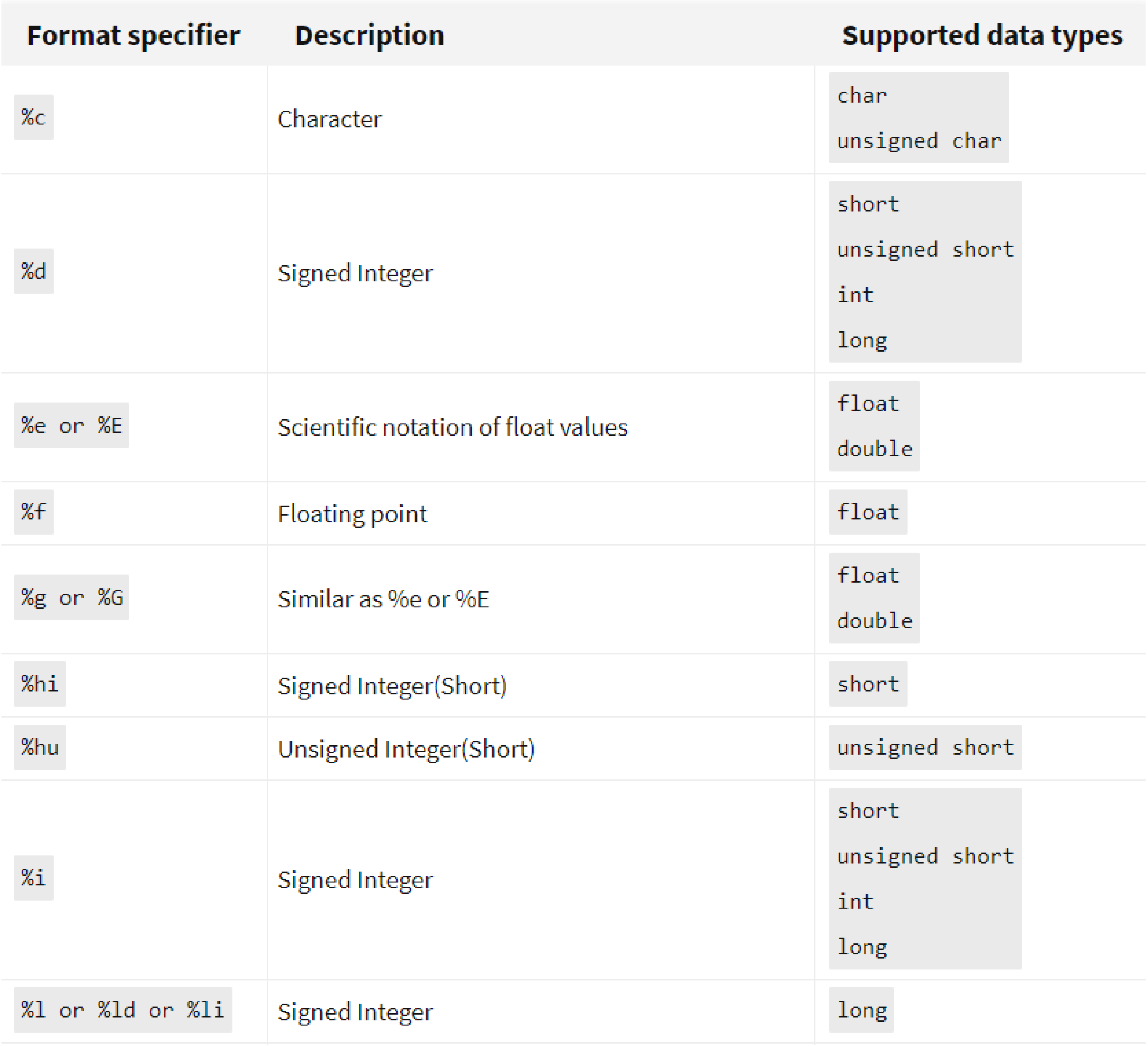


```
        L_M_BV_32 := TDB.T_ENTIER_32S ((1.0/C_M_LSB_BV) *
                                          G_M_INFO_DERIVE(T_ALG.E_BV));
        if L_M_BV_32 > 32767 then
           P_M_DERIVE(T_ALG.E_BV) := 16#7FFF#;
        elsif L_M_BV_32 < -32768 then
           P_M_DERIVE(T_ALG.E_BV) := 16#8000#;
        else
           P_M_DERIVE(T_ALG.E_BV) := UC_16S_EN_16NS(TDB.T_ENTIER_16S(L_M
        end if;

501     P_M_DERIVE(T_ALG.E_BH) := UC_16S_EN_16NS (TDB.T_ENTIER_16S
                                          ((1.0/C_M_LSB_BH) *
                                          G_M_INFO_DERIVE(T_ALG.E_BH)))
     end LIRE_DERIVE;
```

10. Write briefly about Format specifiers and its types.

In C programming we need lots of format specifier to work with various data types. Format specifiers defines the type of data to be printed on standard output. Whether to print formatted output or to take formatted input we need format specifiers. Format specifiers are also called as format string.



Format specifier	Description	Supported data types

`%c`	Character	`char`
		`unsigned char`

`%d`	Signed Integer	`short`
		`unsigned short`
		`int`
		`long`

`%e or %E`	Scientific notation of float values	`float` `double`
`%f`	Floating point	`float`
`%g or %G`	Similar as %e or %E	`float` `double`
`%hi`	Signed Integer(Short)	`short`
`%hu`	Unsigned Integer(Short)	`unsigned short`

`%i`	Signed Integer	`short`
		`unsigned short`
		`int`
		`long`

`%l or %ld or %li`	Signed Integer	`long`

`%lf`	Floating point	`double`
`%Lf`	Floating point	`long double`

`%lu`	Unsigned integer	`unsigned int`
		`unsigned long`

`%lli, %lld`	Signed Integer	`long long`
`%llu`	Unsigned Integer	`unsigned long long`

`%o`	Octal representation of Integer.	`short`
		`unsigned short`
		`int`
		`unsigned int`
		`long`

`%p`	Address of pointer to void void *	`void *`
`%s`	String	`char *`

`%u`	Unsigned Integer	`unsigned int`
		`unsigned long`

`%x or %X`	Hexadecimal representation of Unsigned Integer	`short`
		`unsigned short`
		`int`
		`unsigned int`
		`long`

`%n`	Prints nothing	
`%%`	Prints % character	