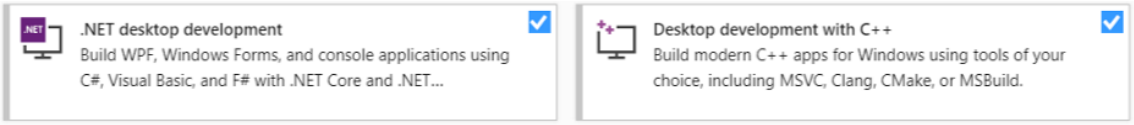
Herramientas descargables y gratis para el curso

1. Upx, https://upx.github.io/
2. Explorer Suite (Cff Explorer) https://ntcore.com/?page_id=388
3. Pe Studio https://www.winitor.com
4. Bintext http://b2b-download.mcafee.com/products/tools/foundstone/bintext303.zip
5. Floss https://github.com/fireeye/flare-floss/releases
6. Ssdeep https://github.com/ssdeep-project/ssdeep/releases
7. Sysinternals suite (Autorun, Procmon), https://docs.microsoft.com/en-us/sysinternals/downloads/sysinternals-suite
8. Process hacker https://processhacker.sourceforge.io/
9. Microsoft Visual Studio https://visualstudio.microsoft.com/es/thank-you-downloading-visual-studio/?sku=Community&rel=16 ← Visual Studio es plug and play, pero asegúrate de instalar esto:



   Si olvidaste instalar estos componentes solo usa el "Visual studio installer" para añadirlos.
10. Python https://www.python.org/downloads/
11. Noriben https://github.com/Rurik/Noriben
12. IDA Pro free version https://www.hex-rays.com/products/ida/support/download_freeware/
13. x32dbg https://x64dbg.com/#start
14. Windows 10, 90 días de prueba -> https://www.microsoft.com/en-us/evalcenter/evaluate-windows-10-enterprise
15. Ubuntu o Kali Linux (recomendamos Kali), Ubuntu -> http://old-releases.ubuntu.com/releases/18.04.2/

    Kali Linux -> https://www.kali.org/downloads/

16. Virtual Box -> https://www.virtualbox.org/wiki/Downloads
17. Inetsim software -> https://www.inetsim.org/downloads.html.
18. Inetsim instrucciones oficiales de instalación -> https://www.inetsim.org/packages.html.
19. Wireshark: https://www.wireshark.org/#download
20. .Net reactor https://www.eziriz.com/dotnet_reactor.htm

PRÁCTICAS

Práctica 1			
Título: Tipo de archivo/File Type	**Recursos**		
	Malware	**Herramientas gratis**	**Sitios web**
	Rams1.exe	pe studio	trID
		cff explorer	Hexadecimal converter
			Portable Executable (PE) format

Práctica 2			
Título: Huella de identificación/Fingerprinting	**Recursos**		
	Malware	**Herramientas gratis**	**Sitios web**
	Rams1.exe	pe studio	Online hash generator
		cff explorer	
		ssdeep	

Práctica 3			
Título: Cadenas/Strings	**Recursos**		
	Malware	**Herramientas gratis**	
	Rams1.exe	floss64	
		bintext	

Práctica 4			
Título: Capturando Keyloggers	**Recursos**		
	Malware	**Herramientas gratis**	
	TotalAware2.exe	Autorun	
		pe studio	

Práctica 5			
Título: Capturando el tráfico de un Keylogger 1/2	**Recursos**		
	Malware	**Herramientas gratis**	
	TotalAware2.exe	cff explorer	
		pe studio	
		bintext	
		wireshark	
		inetsim (Instalación en “Configurando el Laboratorio”)	

Práctica 6			
Título: Revisión de código del Keylogger TotalAware3	**Recursos**		
	Malware	**Herramientas gratis**	**Sitios web**
	Código fuente de “TotalAware3”	Microsoft Visual Studio	Virtual key codes
			Ascii table