SEGURIDAD CERO

CURSO GRATIS
ETHICAL HACKING

LUNES 28 SEPTIEMBRE MARTES 29 SEPTIEMBRE
MIÉRCOLES 30 SEPTIEMBRE

CRI	GTM	HND	MEX	PER
6:00 PM	6:00 PM	6:00 PM	7:00 PM	7:00 PM
				

COL	ECU	PAN	PRY	CHL
7:00 PM	7:00 PM	7:00 PM	8:00 PM	8:00 PM
				

BOL	VEN	DOM	ARG	URY
8:00 PM	8:00 PM	8:00 PM	9:00 PM	9:00 PM
				


Curso Online
Ethical Hacking
Professional
Más Información Aquí

SEGURIDAD CERO

Fernando Conislla
Ethical Hacking Expert

- Años de experiencia en servicios de ciberseguridad para entidades gubernamentales, bancarias, medios de pago, etc.
- Instructor en SEGURIDAD CERO e instructor oficial Certiprof
- Expositor en eventos internacionales
- Master en gestión y dirección de la ciberseguridad
- Certificaciones internacionales CEH, CPTE, CSWAE, LCSPC

SEGURIDAD CERO

Santiago Muñoz
Ethical Hacking Expert

- Años de experiencia en ejercicios de Red Team para entidades gubernamentales, financiero, etc.
- Especializado en el hacking de aplicaciones web, Windows y Active Directory.
- Security researcher en Faraday
- Instructor en SEGURIDAD CERO de Ethical Hacking
- Certificaciones internacionales OSCP | CRTP | CTRE


SEGURIDAD
CERO

SEGURIDAD CERO

CLASE 3
HACKING WINDOWS

MIÉRCOLES 30 SEPTIEMBRE

CRI	GTM	HND	MEX	PER
6:00 PM	6:00 PM	6:00 PM	7:00 PM	7:00 PM

COL	ECU	PAN	PRY	CHL
7:00 PM	7:00 PM	7:00 PM	8:00 PM	8:00 PM

BOL	VEN	DOM	ARG	URY
8:00 PM	8:00 PM	8:00 PM	9:00 PM	9:00 PM

EDITORS' PICK | May 16, 2017, 03:31pm EDT

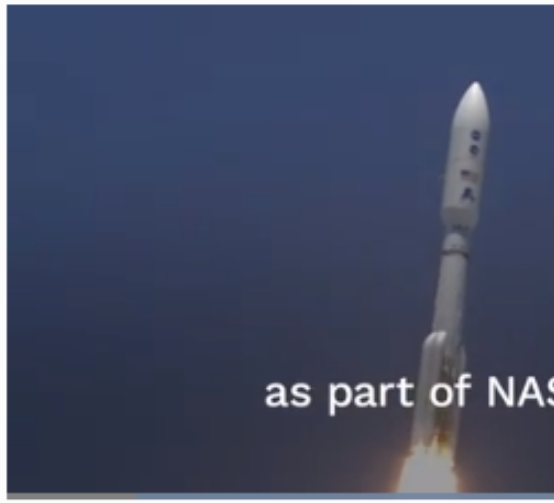
How WannaCry Went From A Windows Bug To An International Incident

Lee Mathews Senior Contributor ⓘ

Cybersecurity

Observing, pondering, and writing about tech. Generally in that order.

This article is more than 3 years old.



Qué es la falla BlueKeep que afecta a computadoras Windows y cómo reducir sus riesgos

Redacción
BBC News Mundo

5 junio 2019

Principales noticias

Qué son los Acuerdos Artemisa con los que EE.UU. planea la minería en la Luna (y por qué causan tensión con Rusia)
Un acuerdo propuesto por la NASA anima la discusión sobre cómo utilizar la Luna con fines comerciales. La forma en la que se interprete el documento, sin embargo, podría generar conflictos.
9 junio 2020

"Esta no es la última pandemia": los científicos que advierten de la "tormenta perfecta" para la aparición de nuevas enfermedades
9 junio 2020

"Bolsonaro sigue una estrategia y un método, que es generar caos"
9 junio 2020

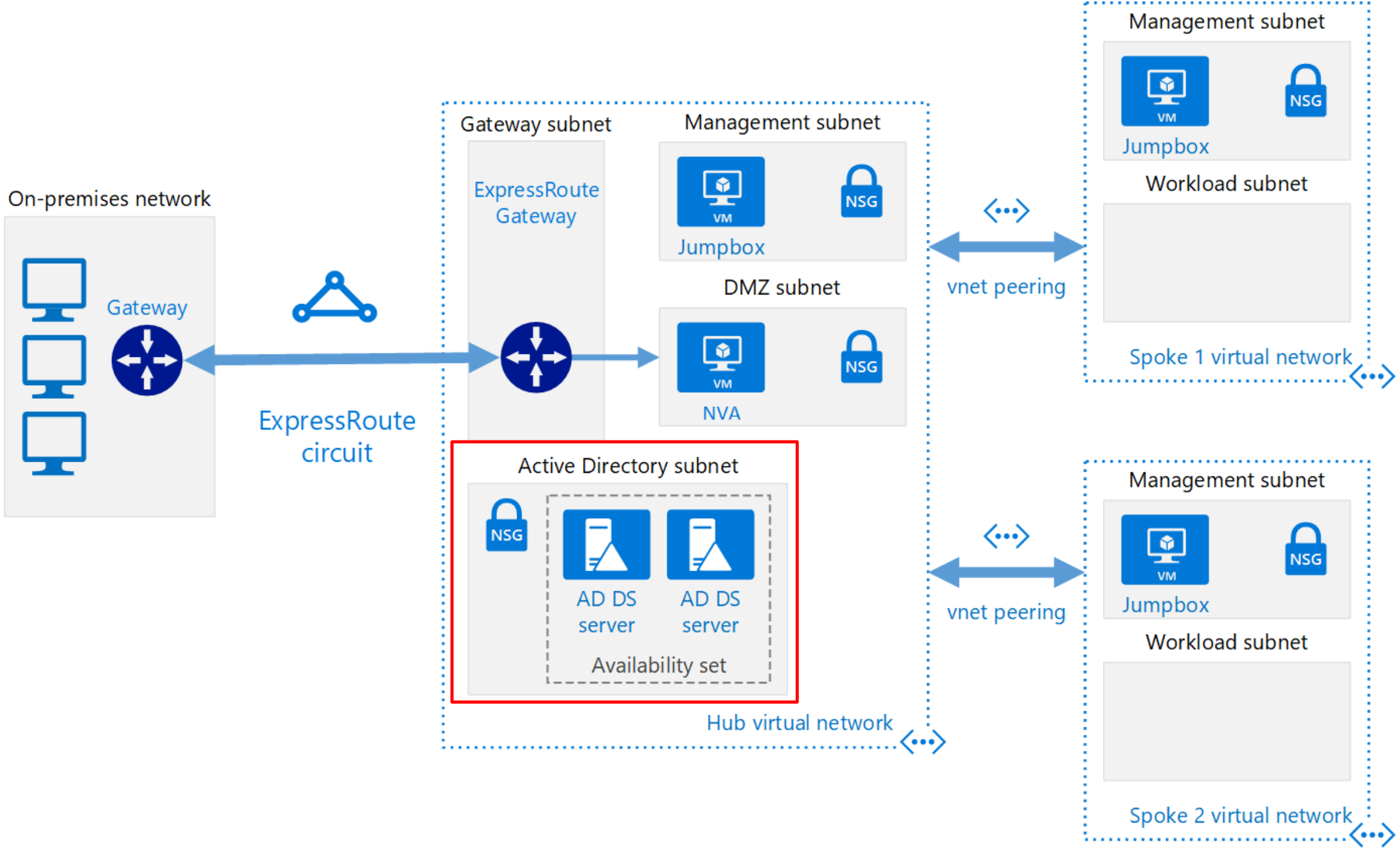
Trustwave®

SMBGhost (CVE-2020-0796): a Critical SMBv3 RCE Vulnerability

March 16, 2020 Karl Sigler

Overview

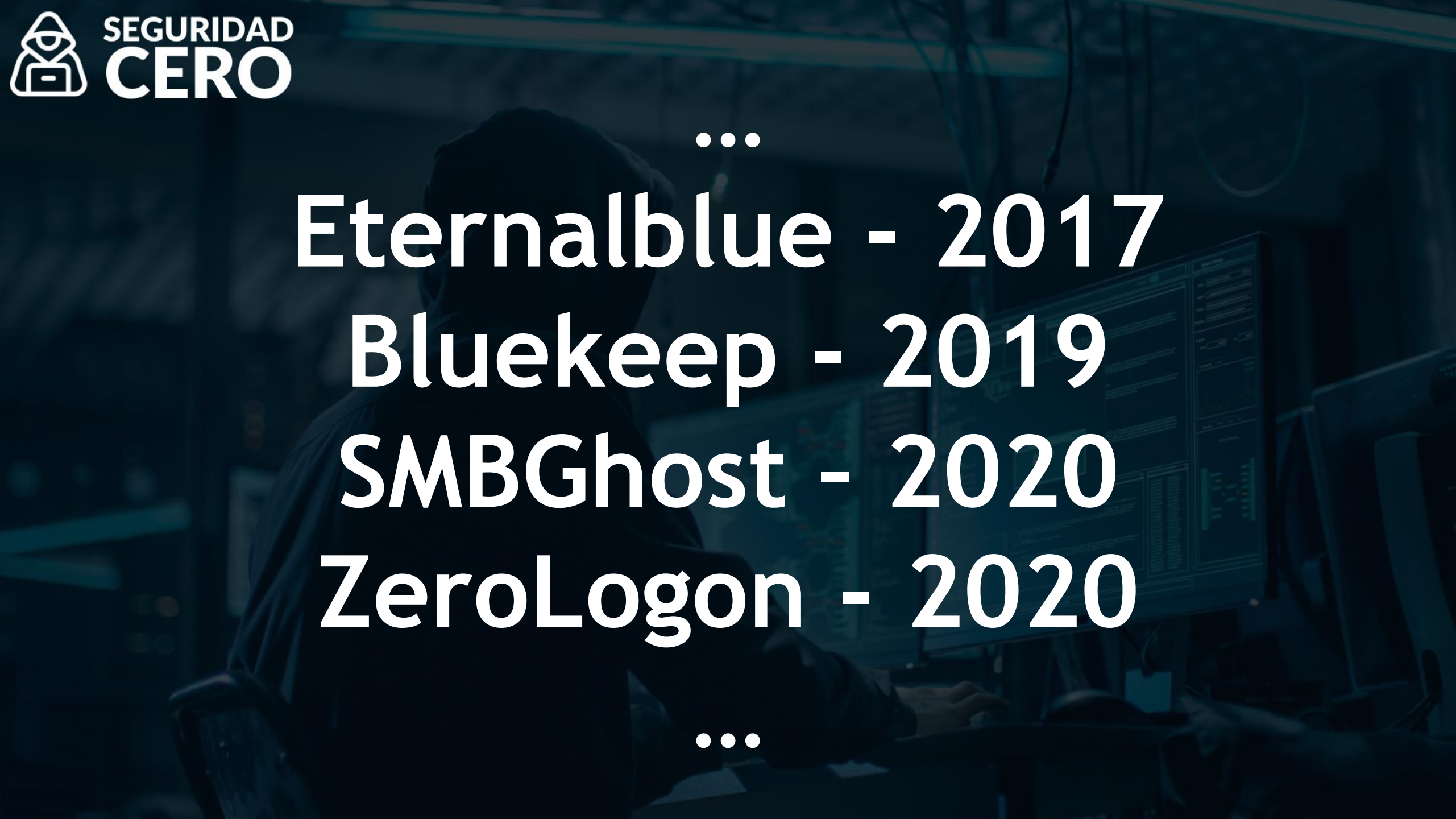
Last week Microsoft announced that there was a buffer overflow vulnerability in SMBv3 (CVE-2020-0796) as implemented in Windows 10 and Windows Server (versions 1903 and 1909). The CVE wasn't initially included in last week's Patch Tuesday, but after news of the vulnerability leaked, Microsoft was forced to release details and an "out of band" patch on Thursday, March 12th. All Windows administrators should check to see if they are vulnerable to this issue and patch as soon as possible where they are.


On-premises network
Gateway
ExpressRoute circuit
Gateway subnet
ExpressRoute Gateway
Management subnet
VM
Jumpbox
NSG
DMZ subnet
VM
NVA
NSG
Active Directory subnet
NSG
AD DS server
AD DS server
Availability set
Hub virtual network
vnet peering
vnet peering
Management subnet
VM
Jumpbox
NSG
Workload subnet
Spoke 1 virtual network
Management subnet
VM
Jumpbox
NSG
Workload subnet
Spoke 2 virtual network

Zerologon – hacking Windows servers with a bunch of zeros

17 SEP 2020 2

Cryptography, Vulnerability


SEGURIDAD
CERO
...
Eternalblue - 2017
Bluekeep - 2019
SMBGhost - 2020
ZeroLogon - 2020
...

Microsoft » Windows 10 : Security Vulnerabilities

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Total number of vulnerabilities : **1111** Page : 1 (This Page) 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23

Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	
1	CVE-2016-3236	19			2016-06-15	2018-10-12	10.0	None	Remote	Low	Not required	C

The Web Proxy Auto Discovery (WPAD) protocol implementation in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows S Windows RT 8.1, and Windows 10 Gold and 1511 mishandles proxy discovery, which allows remote attackers to redirect network traffic via unspecified vectors, aka "Windows WPA of Privilege Vulnerability."

2	CVE-2016-3266	264		+Priv	2016-10-13	2018-10-12	10.0	None	Remote	Low	Not required	C

The kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8 1511, and 1607 allow local users to gain privileges via a crafted application, aka "Win32k Elevation of Privilege Vulnerability," a different vulnerability than CVE-2016-3376, CVE-2 7211.

3	CVE-2016-3270	264		+Priv	2016-10-13	2018-10-12	10.0	None	Remote	Low	Not required	C

The Graphics component in the kernel in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows 10 Gold, 1511, and 1607 allows local users to gain privileges via a crafted application, aka "Win32k Elevation of Privilege Vulnerability."

4	CVE-2016-7182	20		Exec Code	2016-10-13	2018-10-12	10.0	None	Remote	Low	Not required	C

The Graphics component in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT and 1607; Office 2007 SP3; Office 2010 SP2; Word Viewer; Skype for Business 2016; Lync 2013 SP1; Lync 2010; Lync 2010 Attendee; and Live Meeting 2007 Console allows atta code via a crafted True Type font, aka "True Type Font Parsing Elevation of Privilege Vulnerability."

5	CVE-2017-8543	281		Exec Code	2017-06-14	2019-10-02	10.0	None	Remote	Low	Not required	C

Microsoft Windows XP SP3, Windows XP x64 XP2, Windows Server 2003 SP2, Windows Vista, Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8, Windows 8.1 an Server 2012 and R2, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allow an attacker to take control of the affected system when Windows Search fails to h "Windows Search Remote Code Execution Vulnerability".

6	CVE-2017-8589	281		Exec Code	2017-07-11	2019-10-02	10.0	None	Remote	Low	Not required	C

Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and Wir

1
Reconocimiento

2
Escaneo

3
Enumeración

4
Analisis de Vulnerabilidades

5
Explotación

6
Reporte

ETHICAL HACKING

METODOLOGIA

TOTAL RESULTS

1,440,807

TOP COUNTRIES

United States	344,708
Russian Federation	248,515
Japan	77,953
Taiwan	72,818
Germany	64,886

TOP SERVICES

SMB	1,420,372
264	7,813
10443	5,761
HTTPS	2,354
HTTP (8080)	1,104

TOP ORGANIZATIONS

Rostelecom	185,087
HiNet	58,997
Cnservers LLC	39,911
Amazon.com	35,097
Peg Tech	29,748

20.184.27.227

Microsoft Azure
Added on 2020-09-27 07:15:47 GMT
Singapore, Singapore

cloud

```
SMB Status
Authentication: enabled
SMB Version: 2
Capabilities: raw-mode
```

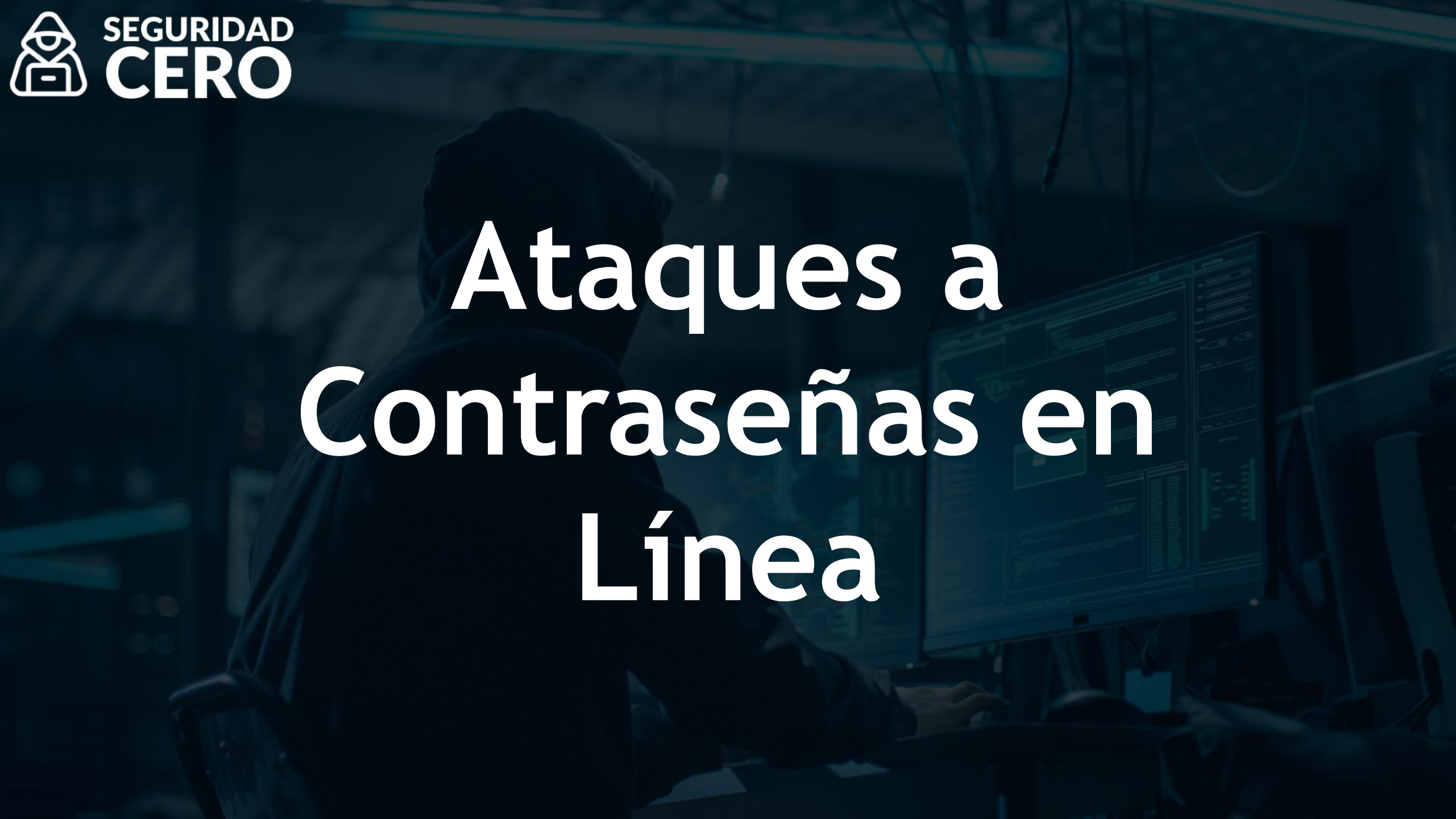
94.50.41.97

Unix
Rostelecom
Added on 2020-09-27 07:15:33 GMT
Russia, Surgut

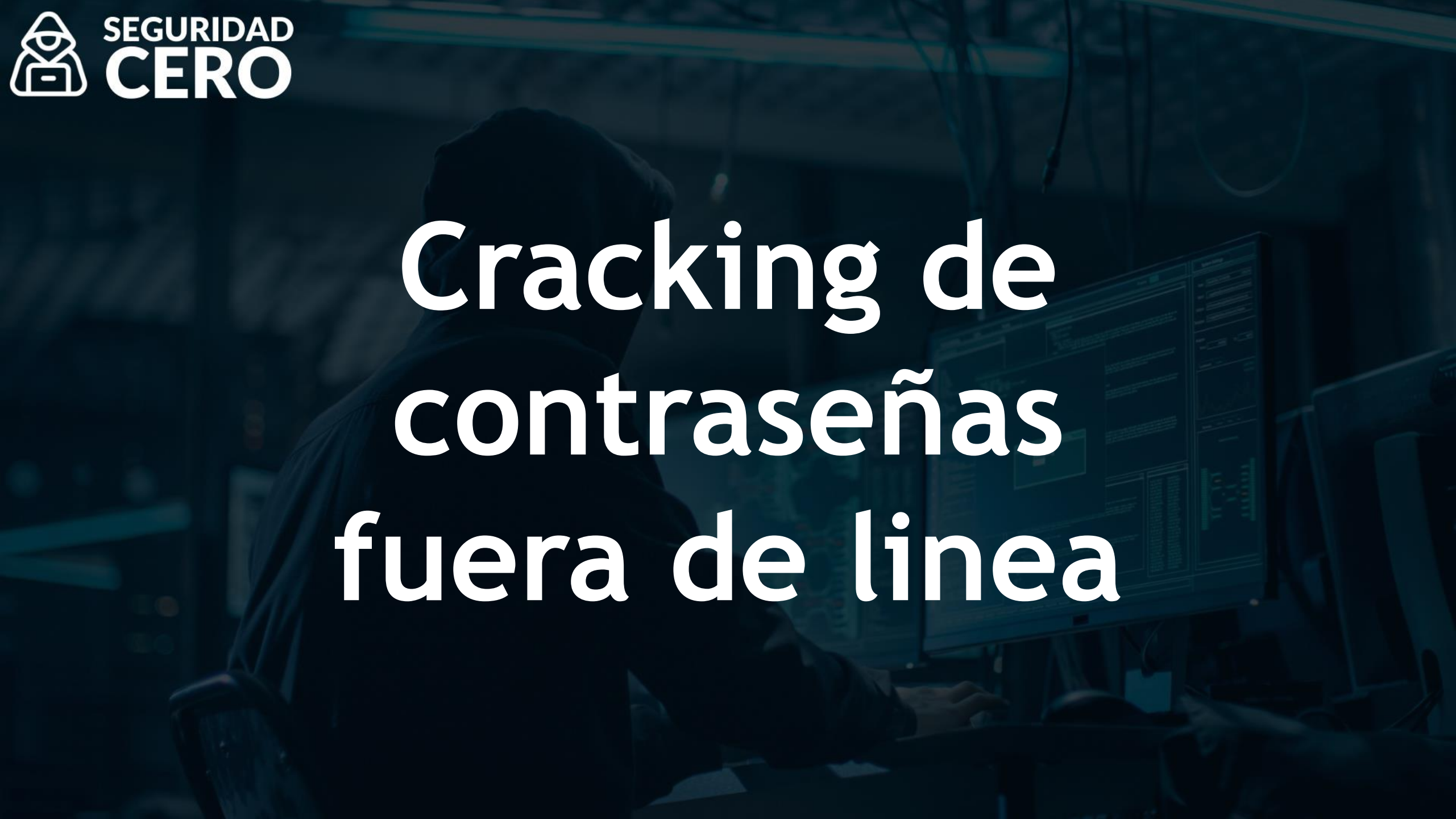
```
SMB Status
Authentication: disabled
SMB Version: 1
Capabilities: raw-mode,unicode,large-files,nt-smb,rpc-remote-api,nt-status,level2-oplocks,lock-and-read,nt-find,dfs,infolevel-passthru,larg
curity

Shares
Name                    Type       Comments
-------------------------------------------------------------------------
public                  Disk       shared folders on each volume
IPC$                    IPC        IPC Service (DSL Gateway)
```

88.208.206.48

server88-208-206-48.live-servers.net
Windows Web Server 2008 R2 7601 Service Pack 1
1&1 Internet AG
Added on 2020-09-27 07:15:44 GMT



Ataques a Contraseñas en Línea



Cracking de contraseñas fuera de linea


SEGURIDAD
CERO
Software
Desactualizado

Ataques de Ingenieria Social

Ataques Basados en Malware

Kernel Exploits


SEGURIDAD
CERO
Servicios
Vulnerables de
Terceros


SEGURIDAD
CERO
Servicios
Nativos
Vulnerables

SEGURIDAD CERO

CLASE 3
HACKING WINDOWS

MIÉRCOLES 30 SEPTIEMBRE

CRI	GTM	HND	MEX	PER
6:00 PM	6:00 PM	6:00 PM	7:00 PM	7:00 PM

COL	ECU	PAN	PRY	CHL
7:00 PM	7:00 PM	7:00 PM	8:00 PM	8:00 PM

BOL	VEN	DOM	ARG	URY
8:00 PM	8:00 PM	8:00 PM	9:00 PM	9:00 PM


Curso Online
Ethical Hacking
Professional
Más Información Aquí

SEGURIDAD CERO

CURSO GRATIS
ETHICAL HACKING

LUNES 28 SEPTIEMBRE MARTES 29 SEPTIEMBRE
MIÉRCOLES 30 SEPTIEMBRE

CRI	GTM	HND	MEX	PER
6:00 PM	6:00 PM	6:00 PM	7:00 PM	7:00 PM
				

COL	ECU	PAN	PRY	CHL
7:00 PM	7:00 PM	7:00 PM	8:00 PM	8:00 PM
				

BOL	VEN	DOM	ARG	URY
8:00 PM	8:00 PM	8:00 PM	9:00 PM	9:00 PM