

May the Security be with
you!

Milan Gabor

`#/viris[@ # Q *]`

Whoami





DISCLAIMER

Milan Gabor
@MilanGabor

GaberHYCU
@GaberHycu

Follow



Day 2... Architecting Azure with security
[#ntk19](#)



10:36 AM - 22 May 2019

3 Retweets 10 Likes



jeff ginsberg @Cr0w_Sec · 19h

Replying to [@GaberHycu](#)

What does the H between the S and the I stand for?



[#/viris\[!@#%&*\]](#)

CVE-2019-0708

Patch now! Why the BlueKeep vulnerability is a big deal

What you need to know about the critical security hole that could enable the next WannaCryptor

`#/viris[🔒🔑🔍🔗]`

🔄 You Retweeted



McAfee Labs  @McAfee_Labs · May 21

Our ATR team is sharing their analysis of the wormable RDP Vulnerability CVE-2019-0708, where RDP stands for "Really DO Patch!"



RDP Stands for "Really DO Patch!" – Understanding the Wormable R...

During Microsoft's May Patch Tuesday cycle, a security advisory was released for a vulnerability in the Remote Desktop Protocol (RDP). What w...
securingtomorrow.mcafee.com

Gremo nazaj



#/viris[@ # Q *]



Iz istega leta



Microsoft Work Area

xbox.kuhinja@outlook.com

Password



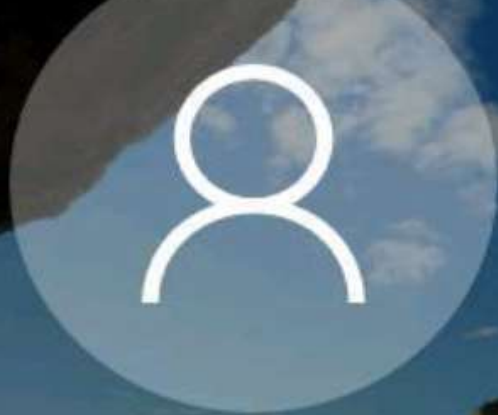
Microsoft...
xbox.kuhi...



Other user

ENG
SL





DejanG

Password



DejanG



Vojko Divjak



Elvis Guštin



Luka Manojlovič



Nadzornik

ENG



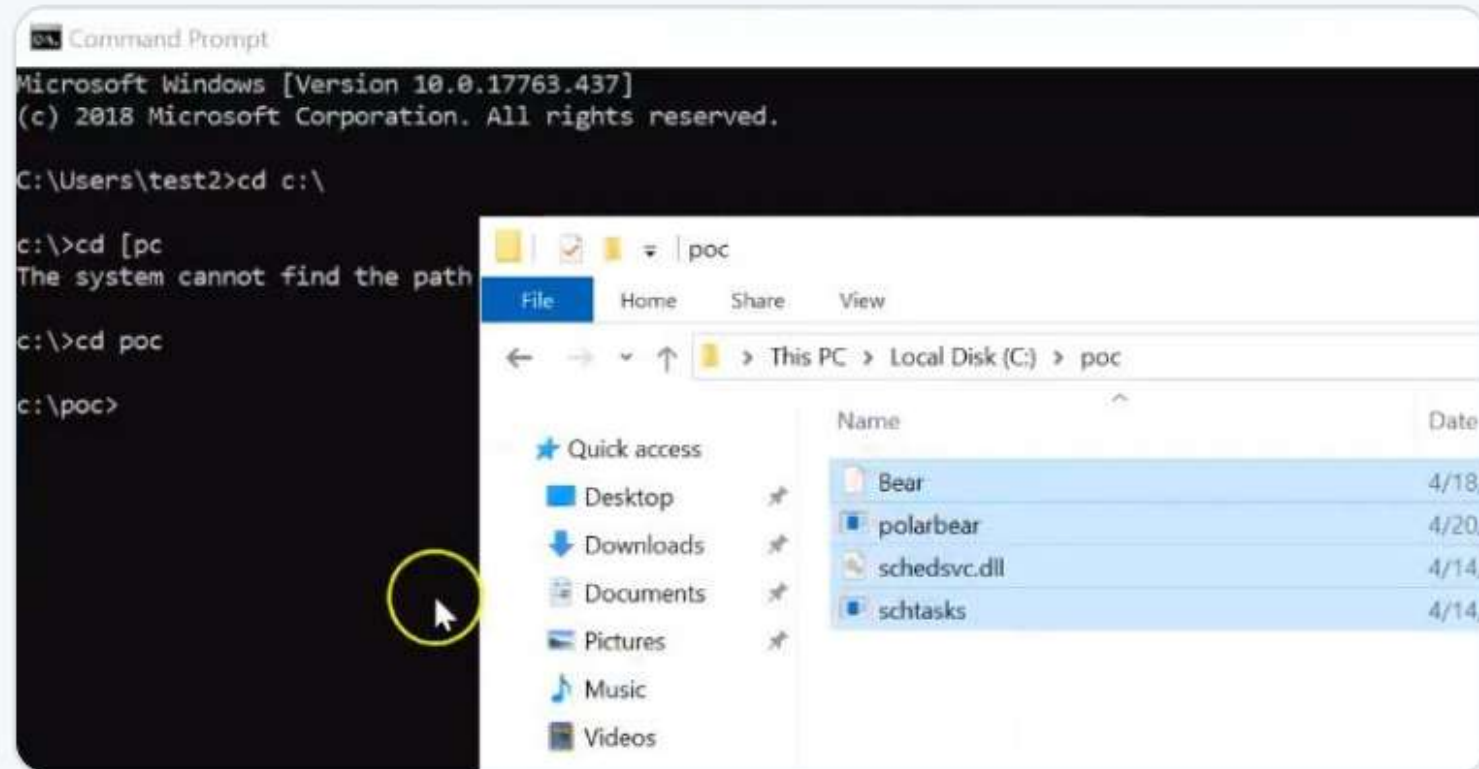
🔄 You Retweeted



Eric Vanderburg @evanderburg · May 22

PoC Exploit For Unpatched Windows 10 Zero-Day Flaw Published Online

i.securitythinkingcap.com/R59r4K



bleepingcomputer.com



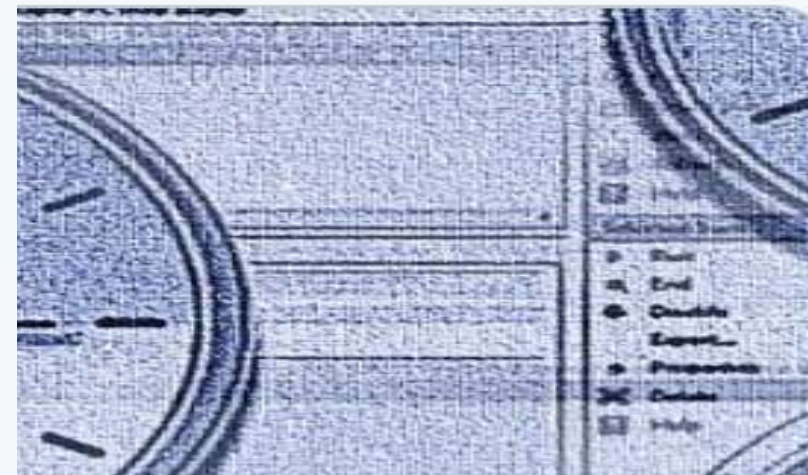
47



78



Task Scheduler - by



s 10 Tas

ped a ne

soft's m



Milan Gabor @MilanGabor · 23h

A ma kdo kaksen lekadol ali kaj drugega paracetamol like? #ntk19 Varnost da glava boli! Kmalu startamo! @NTkonferenca

My NEW favorite way to run powershell.exe

```
CA: Select Administrator: Windows Command Processor - forfiles /p C:\WINDOWS\sy...  
C:\>forfiles /p %COMSPEC:~0,19% /s /c "@file -noe" /m po*l.*e  
ERROR: Access is denied for "C:\WINDOWS\system32\com\dmp\".  
ERROR: Access is denied for "C:\WINDOWS\system32\LogFiles\WMI\RtBackup\".  
ERROR: Access is denied for "C:\WINDOWS\system32\spool\PRINTERS\".  
ERROR: Access is denied for "C:\WINDOWS\system32\spool\SERVERS\".  
  
Windows PowerShell  
Copyright (C) Microsoft Corporation. All rights reserved.  
  
PS C:\WINDOWS\system32\WindowsPowerShell\v1.0> _
```



- Inspired by ITW obfuscation
- Forfiles.exe RECURSIVE usage → **/s**
- Wildcarding powershell.exe → **po*l.*e**
- Executing matched binary in command → **@file**
- Some substring DOSfuscation to make it more original ;)

**REAL-WORLD EXPERIENCE
IS USUALLY
THE BEST TEACHER**



Lanski real-case scenario

> Firma A

- » Napredni NextGen FW
- » MS okolje
- » AV
- » Budget \$\$\$\$\$\$
- » Resursi +++++++

> Owned: < 1 dan

> Firma B

- » Napredni NextGen FW
- » MS okolje
- » AV
- » Budget \$
- » Resursi +

> Owned: „samo“ DB





<Let's hack>

`#!/viris[@#Q*]`

Scenarija

> 1

- » Zakaj je dodeliti lokalni admina uporabniku pogubno za Domain admina!

> 2

- » PingCastle – kako enostavno in hitro preverim stanje moje domene (on premise!)

Opis okolja

- > Domena
- > Windows server 2016
- > Admin: Miha (God, Car, whatever you like)
- > Delovna postaja z Windows 10
- > Uporabnik: Simona (ki rada stalka in pravi, da zna hekat), zna pa biti nadležna in da bo mir, dobi lokalnega admina

Cilji

- > Simona želi postati boginja
- > Pridobi LAB\God

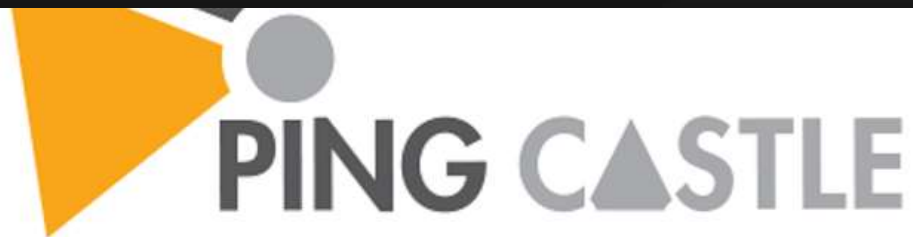
> Težave

- » Ni BitLockerja, ni težav (zamenja 1 exe in zmaga)
- » BitLocker (doda mašino in zmaga)

PingCastle

- > Zastonj orodje za analizo varnosti vaše domene
- > Navaden uporabnik
- > www.pingcastle.com

#/viris[💻🔒🔍🔑]

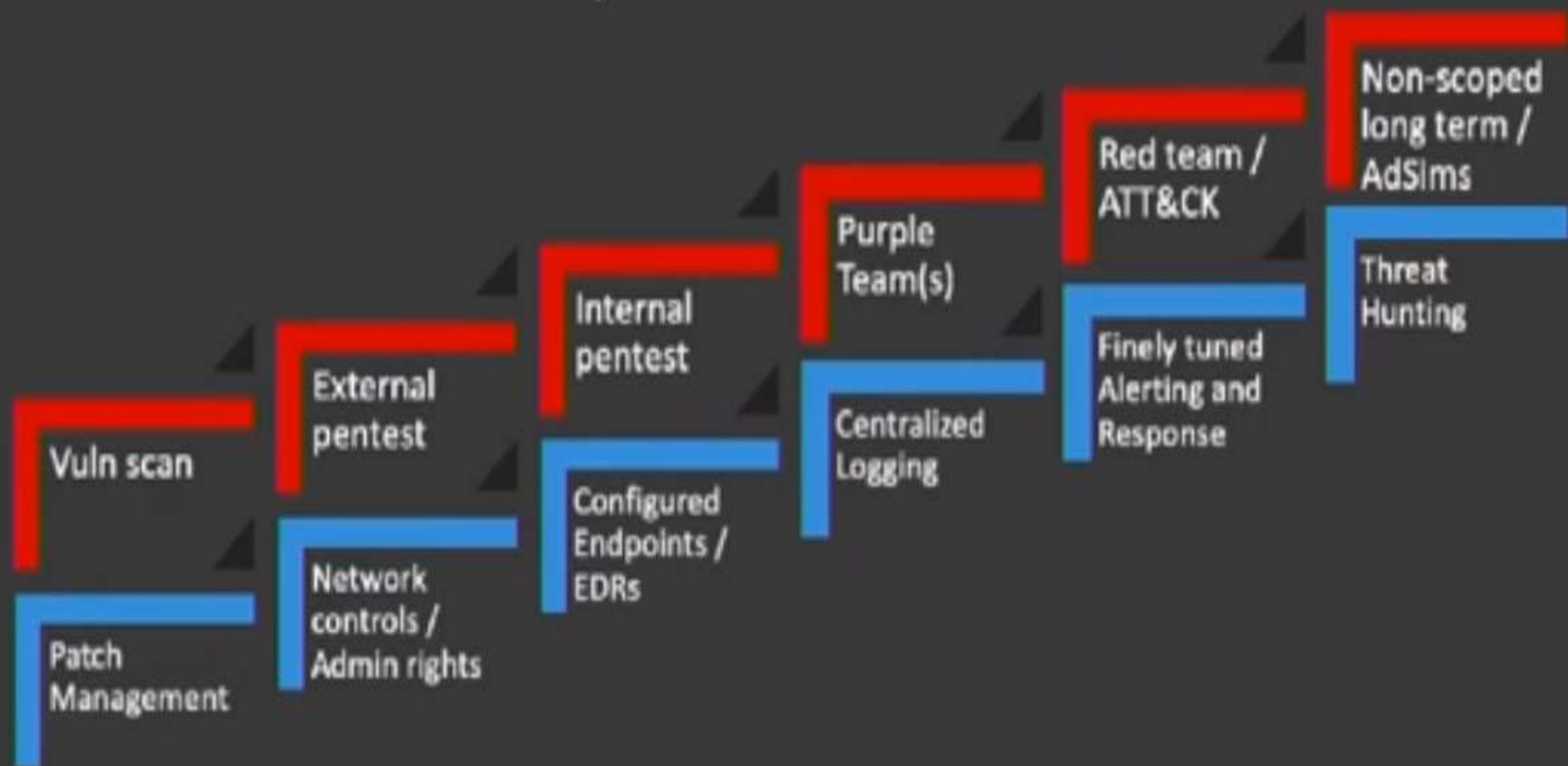


Get Active Directory Security at 80% in 20% of the time
Active directory is quickly becoming a critical failure point in any big sized company, as it is both complex and costly to secure..



TIME TO
FOLLOW UP

Offense Defense Touchpoints



Končni namigi!

- > Assume breach paradigma
- > Miha Pihler: Poskrbite za higijeno
- > Vidljivost znotraj vašega okolja
- > LAPS
- > Ko/če naročite pentest, dajte najti čas, da spremljate, kaj se dogaja v vašem omrežju
- > Vavčerji

Še več končnih namigov

- > Opravite delo, ne samo zapiskov!
- > Sharing is caring. Pogovarjajte se! Utrujajte ljudi! Tudi mene!
- > Igrajte se. Labsi so na voljo!
- > **Izobražujte se!**
- > Igrajte se! Hack the box platforma!

Do it with
PASSION
or not at all





MAY

Security

BE WITH

YOU

