ICT POWER.IT

Microsoft

#POWERCON2021

Cybersecurity: cultura e consapevolezza nell'azienda moderna

Domenico Caldarelli

Head of Cyber Security

domenico.caldarelli@itisistemi.it

Chi sono

Domenico Caldarelli
Head of Cyber Security, ITI srl

- Ethical Hacker
- Systems Engineer
- ICTPower

domenico.caldarelli@itisistemi.it


SEVCON
EXIDE
ProSeries
BATTERY ISOLATOR


NORMAL
P
POWER
CHARGE
Navigation
Aquarium
Telefon
FM
TA
CANCEL
RES/+
SET/-

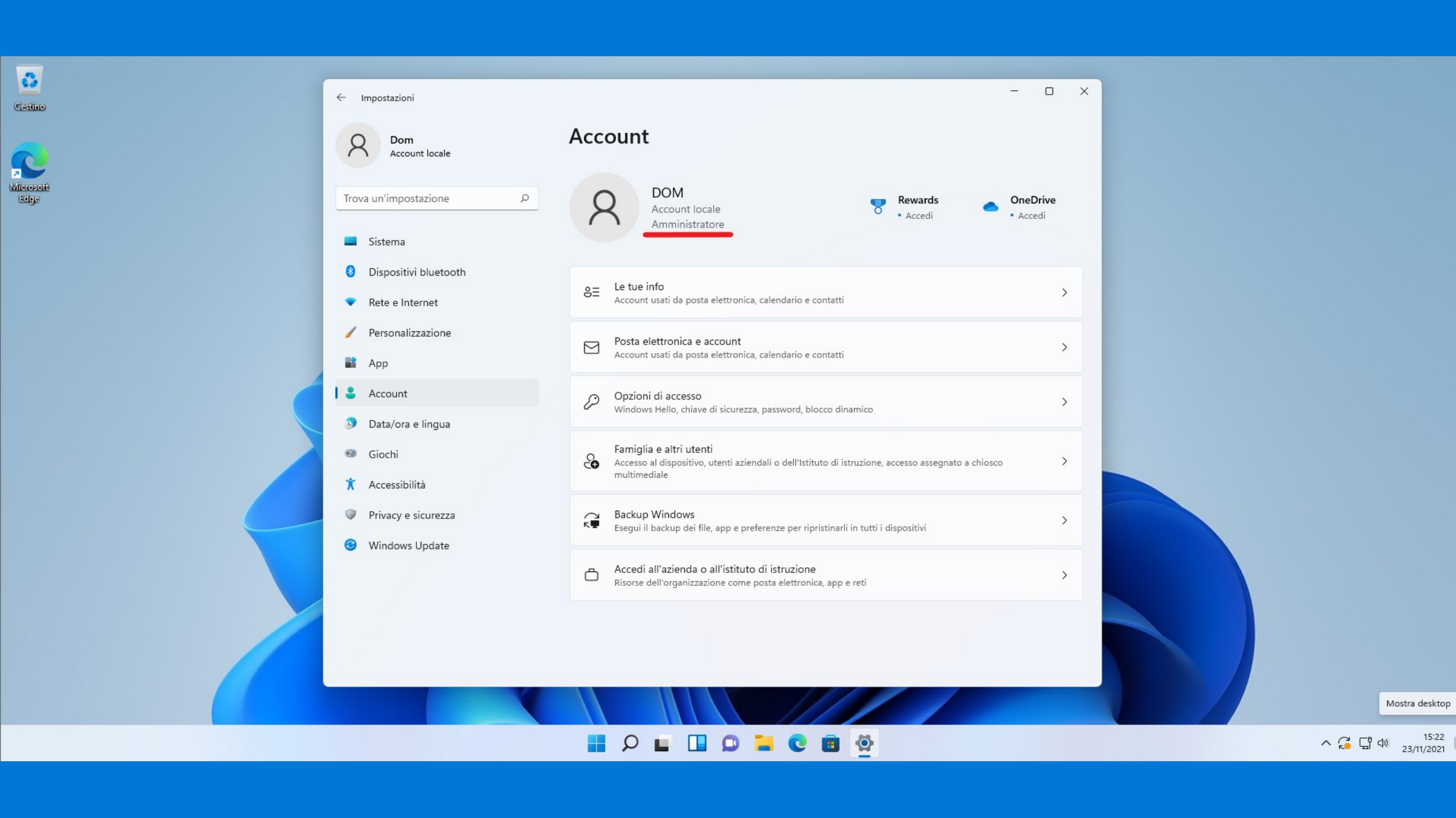

TIME BANDIT
Bill Dunlevy
Harry Lafnear
(VERSION 2.0)
BANDIT 1'S CONTROLLER:
JOYSTICK 2
BANDIT 2'S CONTROLLER:
(FOR TWO PLAYER GAME)
JOYSTICK 1
PRESS F1 & F2 TO CHANGE CONTROLLERS
PRESS "1" OR "2" TO START THE ADVENTURE
ATARI SC1224
520 STation
ATARI 520ST
ATARI 520ST


68
P R N D
KM/H
475 km
15:12
17° C
Profile
Navigate
ROCK FM
Peter Gabriel - Sledgehamm...
20.0
AIRBAG


P
282 km
1-vsh-107
OPEN
OPEN
AUTO
10:43
8° C
Test 1
Navigeren
Oost-Vlaanderen
DEURLE
Golfclub
Royal Latem Golf Club
SINT-MARTENS-LATEM
KROON
HOOGLATEM
Kortrijksesteenweg
Sint-Martens-Latem
20.0
HANDMATIG


12:40 PM
Thu, 15 Nov 2018
16° Amsterdam
Phone
Messages
Internet
Play Store
Camera
LETSGO DIGITAL


Bluetooth
Download the Free App!*
She has MILLIONS of things to say!
Cayla can...
Answer Questions
Understand & Chat
stories and play games
online offline
My Friend Cayla
LEGO
9-14
STOMP & CHOMP
GRIMLOCK


Cestino
Microsoft Edge
Impostazioni
Dom
Account locale
Trova un'impostazione
Sistema
Dispositivi bluetooth
Rete e Internet
Personalizzazione
App
Account
Data/ora e lingua
Giochi
Accessibilità
Privacy e sicurezza
Windows Update
Account
DOM
Account locale
Amministratore
Rewards
• Accedi
OneDrive
• Accedi
Le tue info
Account usati da posta elettronica, calendario e contatti
Posta elettronica e account
Account usati da posta elettronica, calendario e contatti
Opzioni di accesso
Windows Hello, chiave di sicurezza, password, blocco dinamico
Famiglia e altri utenti
Accesso al dispositivo, utenti aziendali o dell'Istituto di istruzione, accesso assegnato a chiosco multimediale
Backup Windows
Esegui il backup dei file, app e preferenze per ripristinarli in tutti i dispositivi
Accedi all'azienda o all'istituto di istruzione
Risorse dell'organizzazione come posta elettronica, app e reti
Mostra desktop
15:22
23/11/2021

Information Security

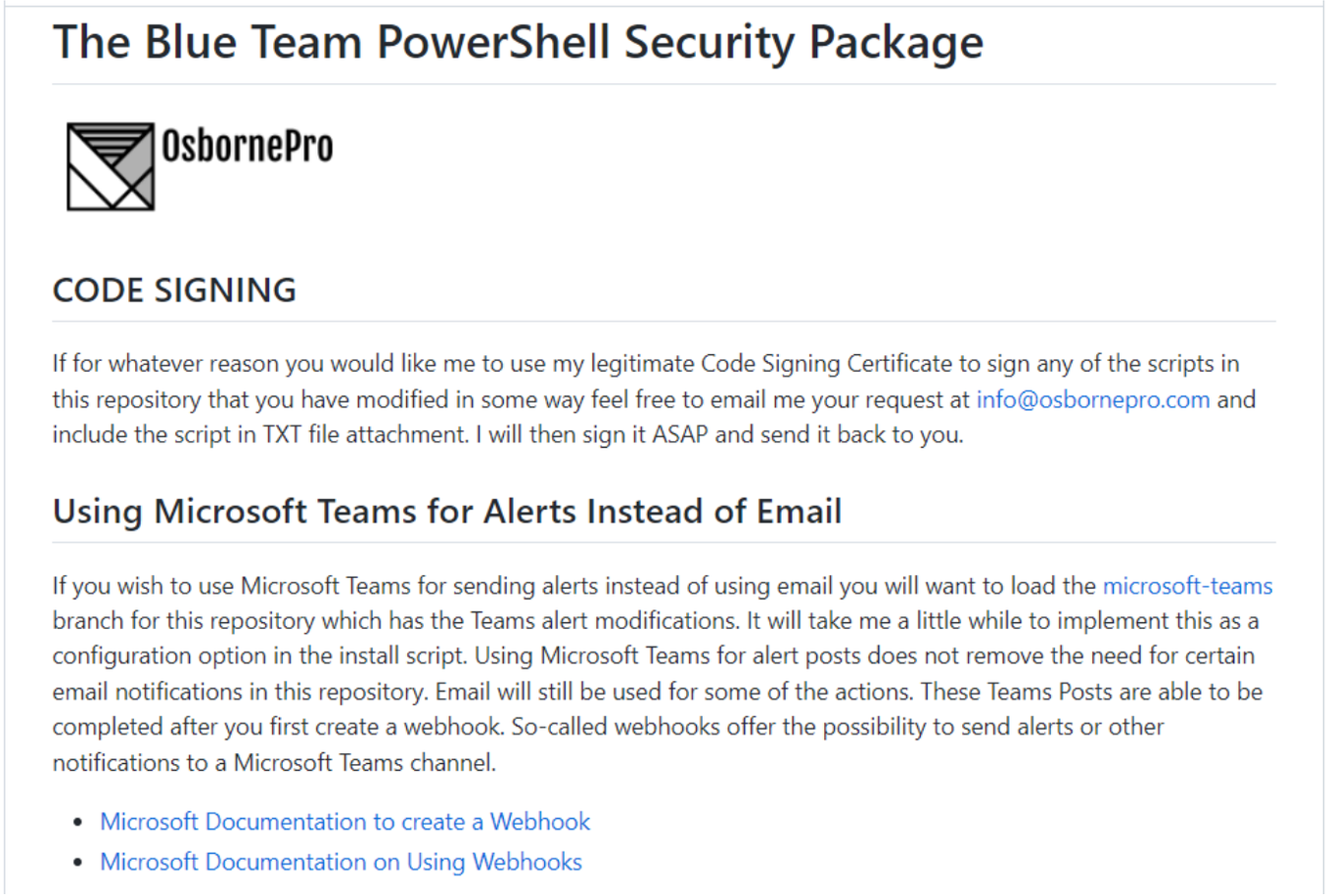
Active Directory

- Nasce con Windows 2000 Server, 15 dicembre 1999;
- Struttura gerarchica che archivia le informazioni sugli oggetti presenti nella rete;
- Computer, Utenti e tutto ciò che riguarda il dominio viene gestito tramite oggetti con delle proprietà;
- Gestione semplificata per gli amministratori;
- Solo relativamente ai criteri di gruppo, ci sono circa 4800 possibili configurazioni;
- Gli aspetti di sicurezza devono essere sempre tenuti in considerazione.

Errori più comuni

- Elevato numero di utenti con privilegi Amministrativi;
- Account di Servizio con privilegi Amministrativi;
- Password che non scadono;
- Password non richieste (autologon);
- Password salvate nelle proprietà dell'utente;
- Password Policy deboli;
- Controllo debole degli accessi;
- Sessioni RDP/console lasciate attive sulle VM
- Possibilità di lettura delle password in chiaro dalla memoria del processo LSASS;
- Possibilità di abusare dei permessi di delega tramite gli account che ne hanno i privilegi;
- Possibilità di creare ticket per la persistenza (golden/silver ticketing);
- Aggiornamenti e CU non applicati;
- Sistemi legacy;

The Blue Team PowerShell Security Package



The Blue Team PowerShell Security Package

OsbornePro

CODE SIGNING

If for whatever reason you would like me to use my legitimate Code Signing Certificate to sign any of the scripts in this repository that you have modified in some way feel free to email me your request at info@osbornepro.com and include the script in TXT file attachment. I will then sign it ASAP and send it back to you.

Using Microsoft Teams for Alerts Instead of Email

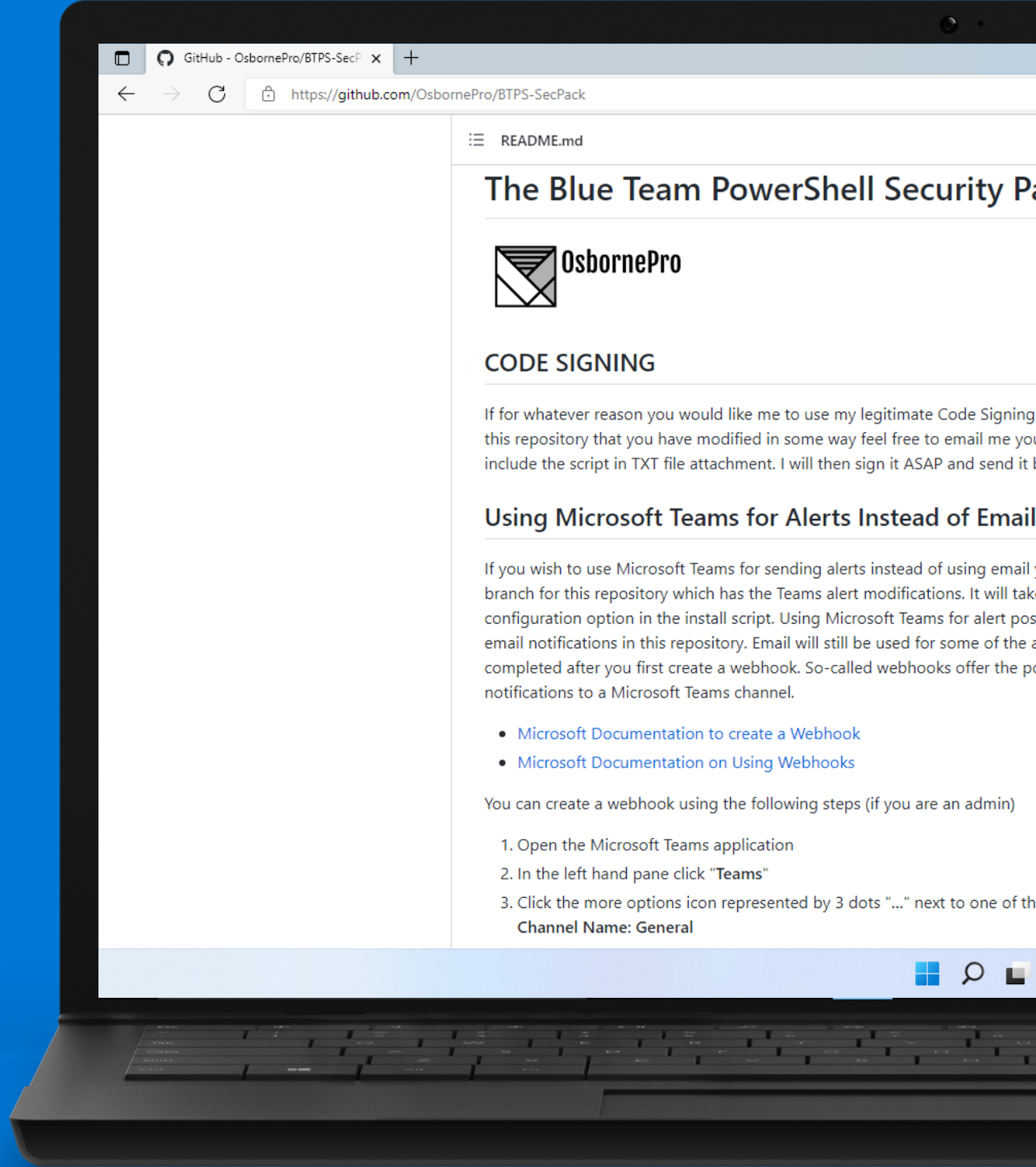
If you wish to use Microsoft Teams for sending alerts instead of using email you will want to load the microsoft-teams branch for this repository which has the Teams alert modifications. It will take me a little while to implement this as a configuration option in the install script. Using Microsoft Teams for alert posts does not remove the need for certain email notifications in this repository. Email will still be used for some of the actions. These Teams Posts are able to be completed after you first create a webhook. So-called webhooks offer the possibility to send alerts or other notifications to a Microsoft Teams channel.

- Microsoft Documentation to create a Webhook
- Microsoft Documentation on Using Webhooks

https://github.com/OsbornePro/BTPS-SecPack

DEMO

Blue Team Security Package



Cyber Security

CVE-2021-41379 - Windows Installer Elevation of Privilege Vulnerability

Questa vulnerabilità consente agli aggressori di effettuare local privilege escalation.

Per poter sfruttare questa vulnerabilità, l'attaccante deve prima ottenere un accesso al sistema operativo con un utente non privilegiato.

Questo tipo di azione viene effettuata grazie ad problema del servizio Windows Installer. L'attacco può essere fatto in modo da abusare del servizio per eliminare un file o una directory oppure per aumentare i privilegi ed eseguire codice arbitrario nel contesto di SYSTEM.

CVE-2021-1675, CVE-2021-34527 - Print Nightmare

Questa vulnerabilità, denominata Print Nightmare, riguarda il servizio Print Spooler, ovvero il servizio che permette la di ricercare una stampante ed eseguire l'azione di stampa.

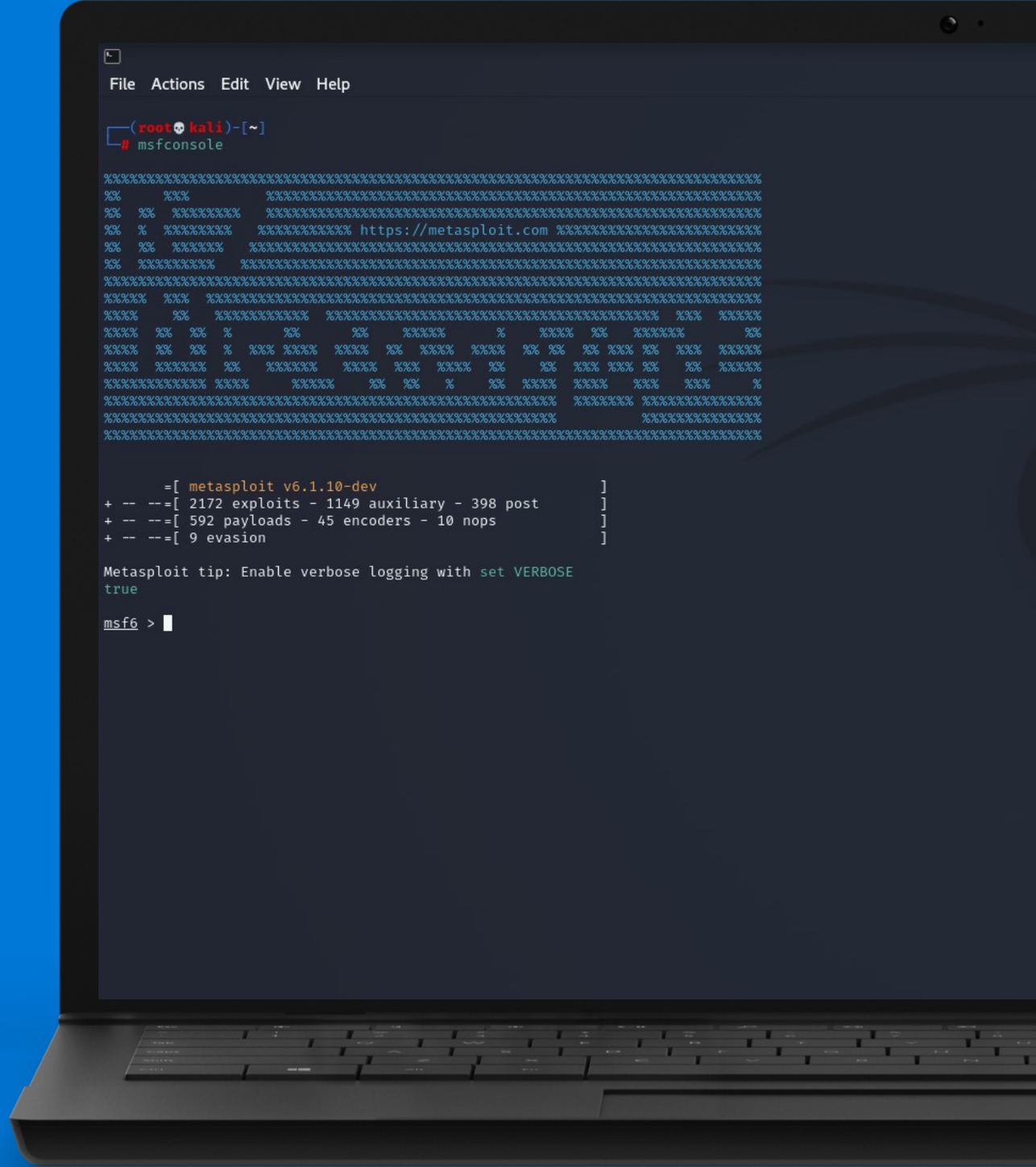
Print Spooler Remote Code Execution Vulnerability

Sono state rilasciate da Microsoft diverse patch per risolvere questa problematica ma, ad oggi, ci sono ancora dei casi in cui questa vulnerabilità è sfruttabile da un attaccante.

In questo caso, il problema si verifica quando il servizio Printer Spooler tenta di installare/utilizzare i driver di una stampante ubicati in una directory locale oppure via SMB. Questi driver possono contenere codice arbitrario che viene eseguito con privilegi di SYSTEM e possono essere eseguiti da qualsiasi utente sia in grado di autenticare la chiamata al servizio Print Spooler.

DEMO

A way to...


File Actions Edit View Help
(root kali)-[~]
msfconsole
https://metasploit.com
=[metasploit v6.1.10-dev]
+ -- --=[2172 exploits - 1149 auxiliary - 398 post]
+ -- --=[592 payloads - 45 encoders - 10 nops]
+ -- --=[9 evasion]
Metasploit tip: Enable verbose logging with set VERBOSE
true
msf6 >

Conclusioni

Persone: Formazione, Postura, Preparazione

Processi: Monitoraggio, Analisi, Risoluzione Incidenti

Tecnologia: Servizi, Prodotti, Sistemi

ICT POWER.IT

Microsoft

Grazie

Domenico Caldarelli
Head of Cyber Security
domenico.caldarelli@itisistemi.it