



16º SEMINÁRIO FEMIPA

FILANTRÓPICOS FORTALECIDOS, POPULAÇÃO BEM ASSISTIDA

19, 20 E 21 DE MARÇO 2024 - CURITIBA / PR

Cyberprobe: exploração técnica de resiliência de rede

Célio Ribeiro da Silva
Centro Hospitalar São Camilo

Introdução

Cibersegurança através de testes de vulnerabilidade e conscientização

- Qual empresa nos dias atuais não é sustentada por tecnologia?

Desde um simples controle de estoque, cadastro de clientes, controle de caixa, contas a pagar e receber.

- Seu cliente se conecta através de um WIFI dentro de sua empresa?
- É de costume utilização de flashdrives (Pendrive) para uma ou outra situação?

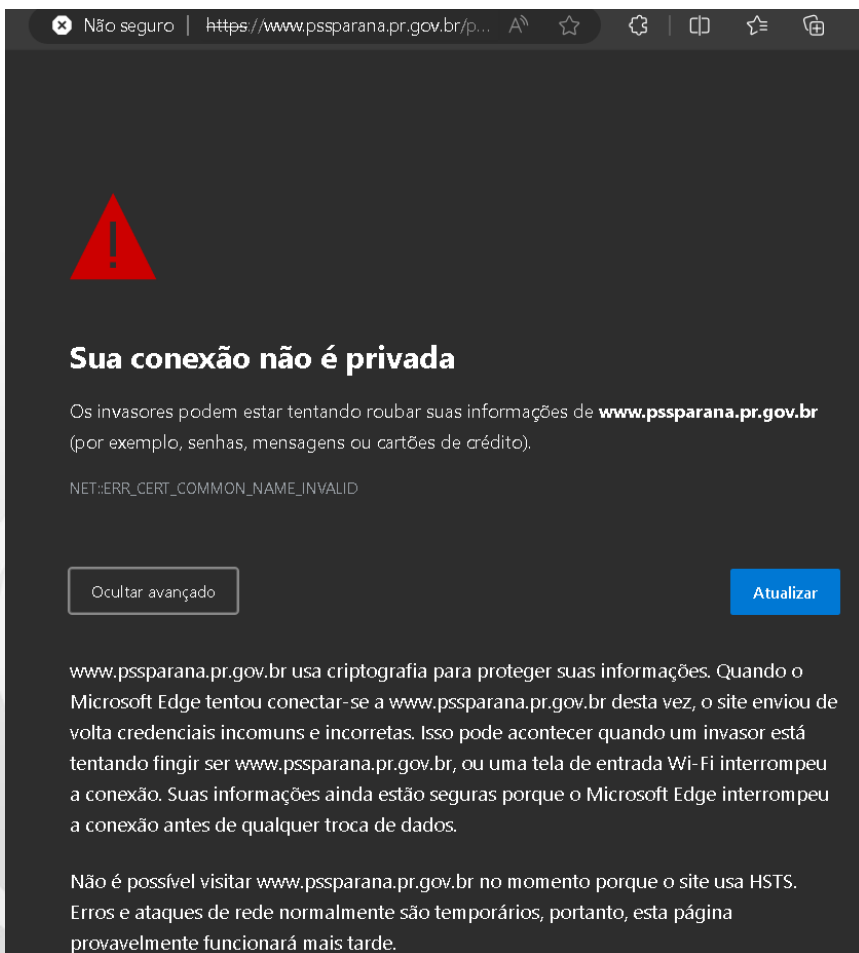
Análises

Testes de Vulnerabilidade com ESP32

- Analises da rede wifi para possíveis acessos aos servidores locais.
- Testes da rede de visitantes para possibilidade de cópias de SSID (nome) na rede aberta.
- Tentativas de ataque DDoS na própria rede para analise de impacto.
- Phising através de Rede Aberta criada dentro do mesmo local.



Análises



Sua conexão não é privada

Os invasores podem estar tentando roubar suas informações de **www.pssparana.pr.gov.br** (por exemplo, senhas, mensagens ou cartões de crédito).

NET:ERR_CERT_COMMON_NAME_INVALID

Ocultar avançado Atualizar

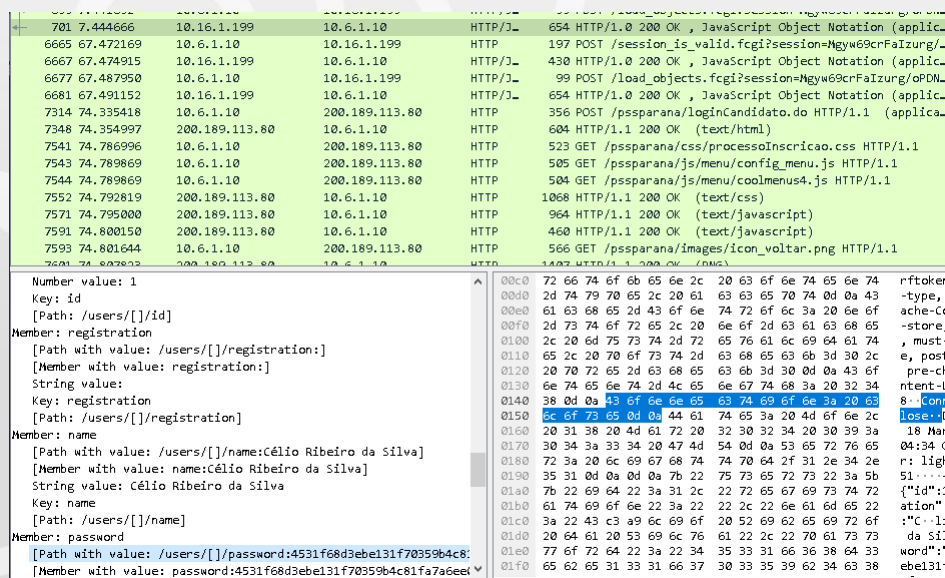
www.pssparana.pr.gov.br usa criptografia para proteger suas informações. Quando o Microsoft Edge tentou conectar-se a www.pssparana.pr.gov.br desta vez, o site enviou de volta credenciais incomuns e incorretas. Isso pode acontecer quando um invasor está tentando fingir ser www.pssparana.pr.gov.br, ou uma tela de entrada Wi-Fi interrompeu a conexão. Suas informações ainda estão seguras porque o Microsoft Edge interrompeu a conexão antes de qualquer troca de dados.

Não é possível visitar www.pssparana.pr.gov.br no momento porque o site usa HSTS. Erros e ataques de rede normalmente são temporários, portanto, esta página provavelmente funcionará mais tarde.

- Sites com esse aviso que começam com o http://

Senhas são facilmente visualizadas sem criptografia alguma, com uma simples análise de pacote com ferramentas gratuitas, pode-se descobrir a senha para esses portais.

- Recomendação: não utilizar a mesma senha em vários sites e se possível autenticação em dois fatores.



Time	Source IP	Destination IP	Protocol	Method	Status	Content-Type
701	7.444666	10.16.1.199	HTTP/1.1	GET	200	OK
6665	67.472169	10.6.1.10	HTTP	POST	200	OK
6667	67.474915	10.16.1.199	HTTP/1.1	GET	200	OK
6677	67.487950	10.6.1.10	HTTP/1.1	POST	200	OK
6681	67.491152	10.16.1.199	HTTP/1.1	GET	200	OK
7314	74.335418	10.6.1.10	HTTP	POST	200	OK
7348	74.354997	200.189.113.80	HTTP	GET	200	OK
7541	74.786996	10.6.1.10	HTTP	GET	200	OK
7543	74.789869	10.6.1.10	HTTP	GET	200	OK
7544	74.789869	10.6.1.10	HTTP	GET	200	OK
7552	74.792819	200.189.113.80	HTTP	GET	200	OK
7571	74.795000	200.189.113.80	HTTP	GET	200	OK
7591	74.800150	200.189.113.80	HTTP	GET	200	OK
7593	74.801644	10.6.1.10	HTTP	GET	200	OK

```

Number value: 1
Key: id
[Path with value: /users/[]/id]
Member: registration
[Path with value: /users/[]/registration:]
[Member with value: registration:]
String value:
Key: registration
[Path: /users/[]/registration]
Member: name
[Path with value: /users/[]/name:Célio Ribeiro da Silva]
[Member with value: name:Célio Ribeiro da Silva]
String value: Célio Ribeiro da Silva
Key: name
[Path: /users/[]/name]
Member: password
[Path with value: /users/[]/password:4531f68d3ebe131f70359b4c81fa7a6eeet]
[Member with value: password:4531f68d3ebe131f70359b4c81fa7a6eeet]
  
```

Testes físicos de vulnerabilidade nas portas USB (Conscientização) com Raspberry Pi Pico Rp 2040

- Criado um pendrive com script automático que copia informações da vítima e envia para o email do autor.
- Quem de nós costuma salvar senhas do email?



Vídeo e Conclusão

Testes físicos de vulnerabilidade nas portas USB (Conscientização)

- Cibersegurança não é investimento.

The image shows a Windows desktop environment. On the left, there are desktop icons for 'Importantes' (Important) and 'Lixeira' (Recycle Bin). The main area is a video player displaying a graphic titled 'Os 5 momentos para a higienização das mãos' (The 5 moments for hand hygiene). The graphic features a central illustration of a patient in a hospital bed with two healthcare workers. Five red arrows point to specific moments: 1. 'Antes de contato com o paciente' (Before contact with the patient); 2. 'Antes da realização de procedimento asséptico' (Before aseptic procedure); 3. 'Após risco de exposição a fluidos corporais' (After risk of exposure to body fluids); 4. 'Após contato com o paciente' (After contact with the patient); 5. 'Após contato com áreas próximo ao paciente' (After contact with areas near the patient). At the bottom of the video player, the logo for 'CENTRO HOSPITALAR SÃO CAMILO' is visible, along with the name 'Diretor técnico Daniela Mattar CRM/PR 13352'. The system tray at the bottom shows the taskbar with various application icons, the system clock at 07:44, and the date 18/03/2022.

OBRIGADO!

Célio Ribeiro da Silva

Email: ti@saocamilopg.com.br

Celular: 42 – 98442 0668