



AUXILIUM
Cyber Security

Penetrační testy

digitální infrastruktury



Kdo jsem a co děláme?

- Vystudoval jsem kybernetickou bezpečnost na TU Berlín
- První praxe v Auxilium Cyber Security (Karlsruhe)
- Od roku 2019 vedu naší kancelář v Praze
- Pražská kancelář se specializuje na penetrační testy:
 - Vestavné systémy
 - Webové aplikace
 - Mobilní a desktopové aplikace
 - API
 - Podniková infrastruktura
- **Co je ten penetrační test?**



Penetrační test je metoda hodnocení zabezpečení počítačových systémů, která se provádí simulací reálného útoku na tento systém.



Kde bude obvykle prolomena kybernetická bezpečnost?





Řetěz je jen tak silný jako jeho nejslabší článek

- Platí dvojnásob v kybernetické bezpečnosti
- Skvělá podniková infrastruktura, ale...
 - ...jednofaktorová autentizace na VPN
- Bezpečnou aplikaci A a aplikaci B, ale...
 - ...jejich integrace není optimální
- Dovolte mi demonstrovat na případu eObčanky
- Zveřejněno v angličtině na konferenci QuBIT
- [QuBIT 2020: Virus Harvesting Czech eObčanka \(eID Card\) Identities](#)



Proces přihlášení eObčankou (2019)

NIA - Mozilla Firefox

NIA

Správa základních registrů (CZ) | https://eop.eidentita.cz/IPSTS

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB

eidentita.cz
KLÍČ K ELEKTRONICKÝM SLUŽBÁM
Friday, February 21, 2020

English

Login process is ongoing, please wait

Information

Firefox opening following link:
"czeeopauth://
mwid=896a7ea1-6a7b-4406-997f-
b5244d77bd93"

OK

Identifikace občanským průkazem

Datum a čas
21.02.2020 16:01:36

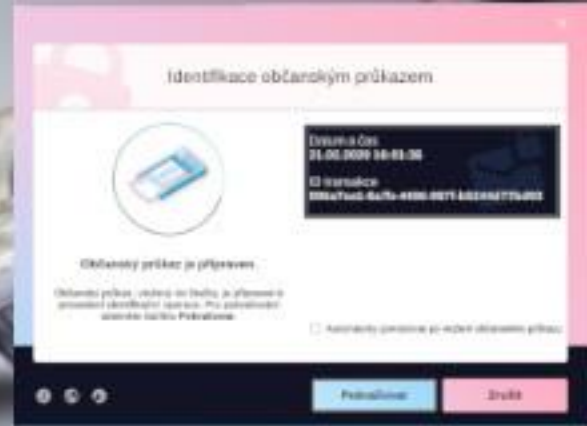
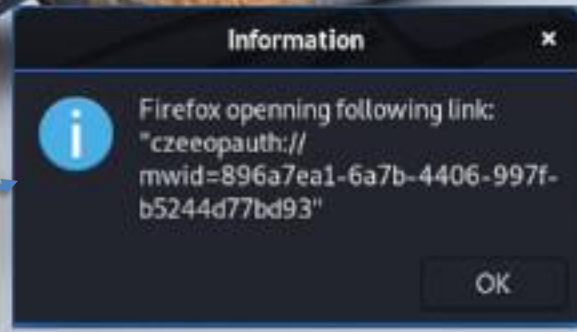
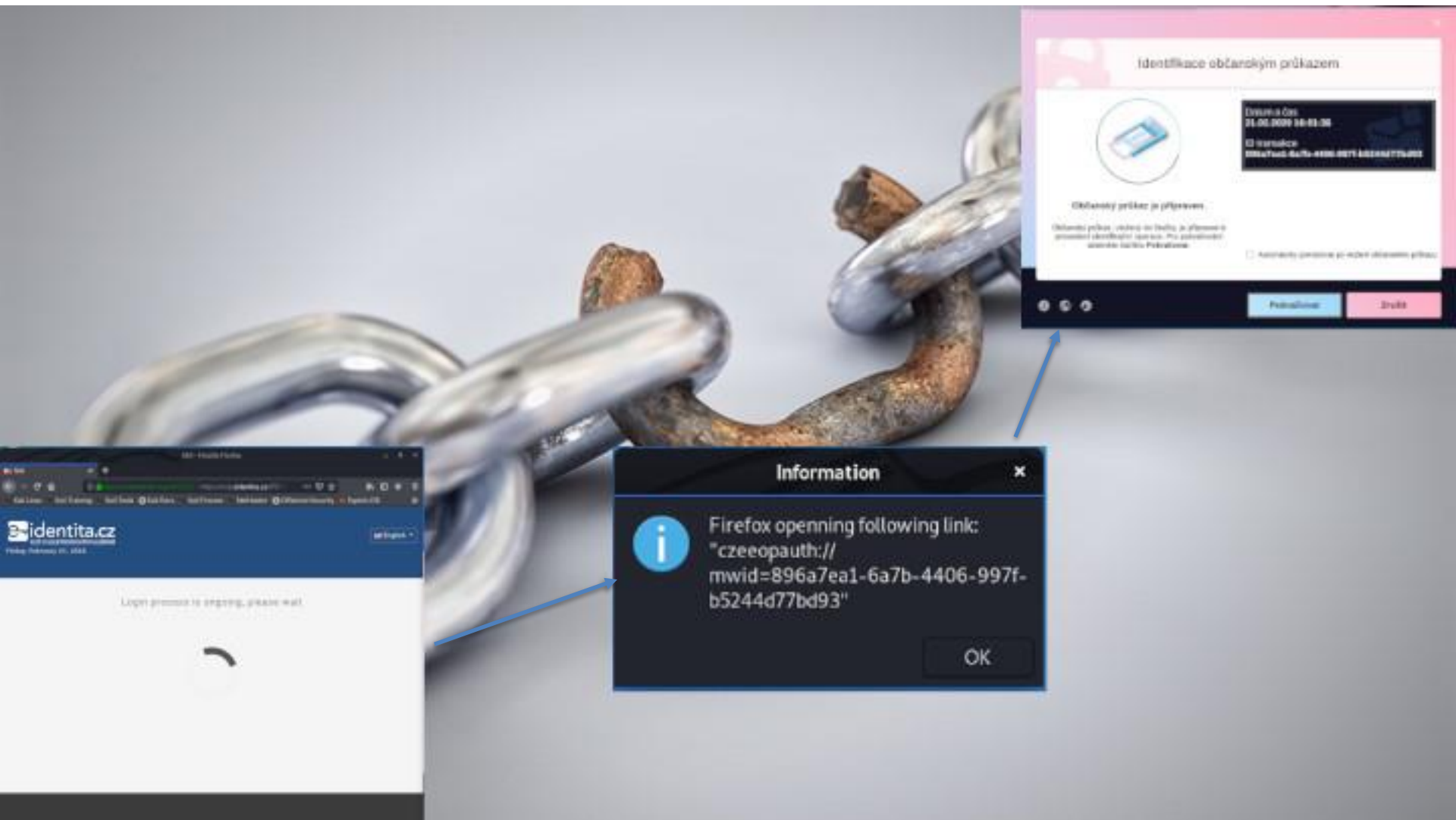
ID transakce
896a7ea1-6a7b-4406-997f-b5244d77bd93

Občanský průkaz je připraven.

Občanský průkaz, vložený do čtečky, je připraven k provedení identifikační operace. Pro pokračování stiskněte tlačítko **Pokračovat**.

Automaticky pokračovat po vložení občanského průkazu

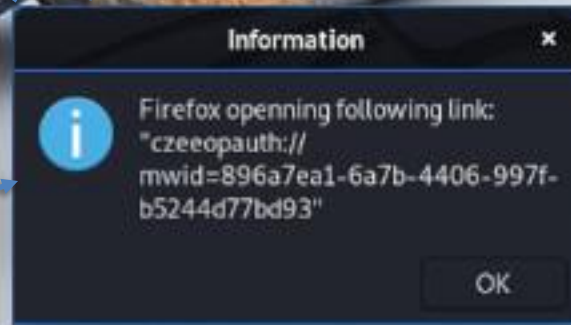
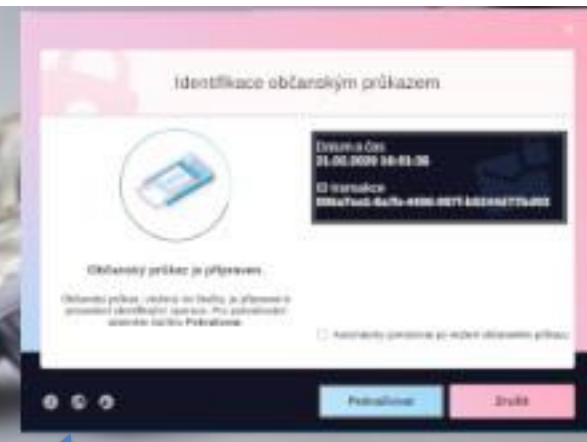
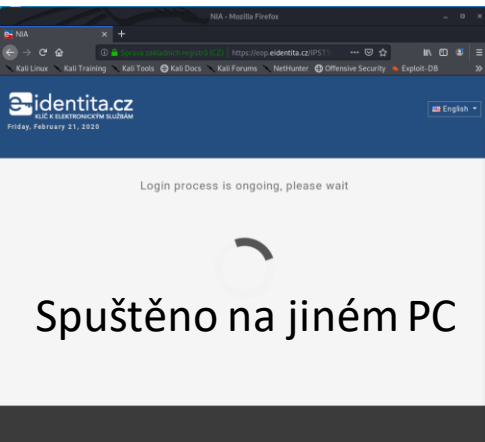
Pokračovat Zrušit





Řetěz přihlášení eObčankou

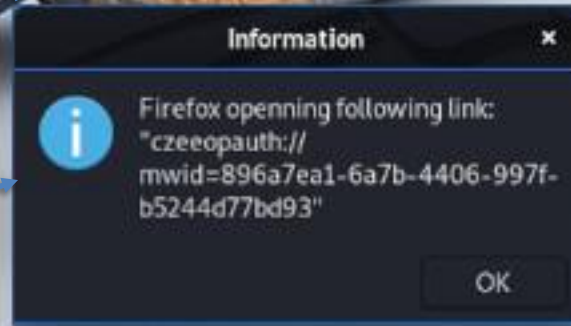
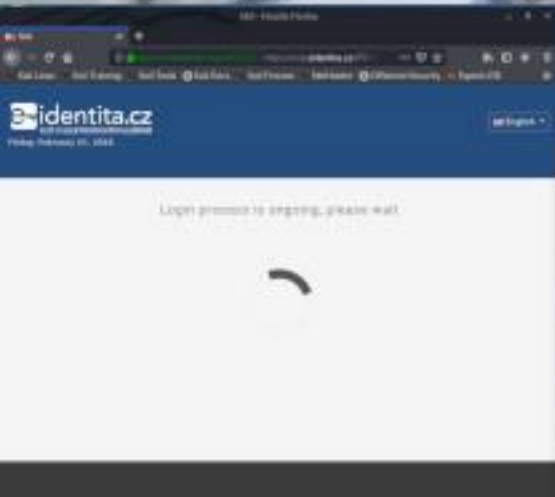
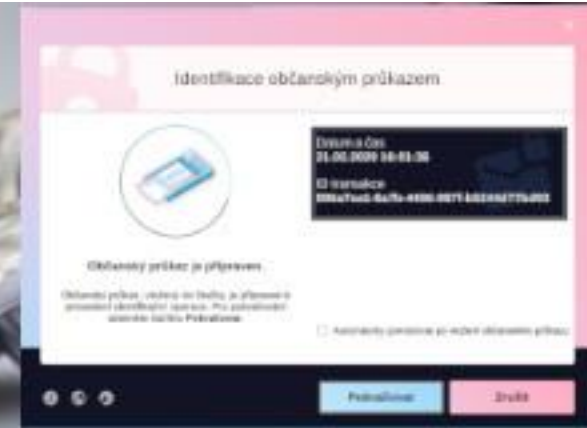
- Aplikace A: webová aplikace eidentita.cz (SSO)
- Aplikace B: eObčanka – Identifikace (komunikace s eOP)
- Obě aplikace velmi solidně vyvinuty
- Bohužel A předává B ID transakce přes nezabezpečený odkaz
- **Co se stane pokud toto ID bude „změněno“?**
- Uživatel jistě nic nepozná, jelikož ID transakce se nezobrazuje v A
- Vidí jej pouze v aplikaci B





Narušený řetěz přihlášení eObčankou

- Útok lze bohužel plně automatizovat
- Pro demonstraci útoku jsme vyvinuli 2 komponenty:
 1. Virus, který běží na PC kde se přihlašuje občan
 2. Webovou službu, která běží v cloudu
- V okamžiku spuštění aplikace B je volání zachyceno virem
- Webová služba vygeneruje nové přihlašovací ID a předá jej viru
- Vir změní přihlašovací ID uživatele za ID útočníka
- Nic netušící občan dokončí přihlášení zadáním PINu
- Útočník bude přihlášen jménem občana
- Občanův přihlašovací pokus neuspěje (timeout)





```
root@destiny:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 52:54:00:00:67:43 brd ff:ff:ff:ff:ff:ff
    inet 31.31.78.153/24 brd 31.31.78.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 2a02:2b88:2:1::6743:1/64 scope global
        valid_lft forever preferred_lft forever
    inet6 fe80::5054:ff:fe00:6743/64 scope link
        valid_lft forever preferred_lft forever
root@destiny:~# python3.5 apu3f.py
```

What Is My IP? Shows your real public IP address - IPv4 - IPv6 - Mozilla Firefox

What Is My IP? Shows your real public IP address - IPv4 - IPv6 - Mozilla Firefox

https://www.whatismyip.com

WhatIsMyIP.com

Your Public IPv4 is:
37.188.225.135

Your IPv6 is: Not Detected

Your Local IP is:
172.16.65.213

Location: Nachod, KR CZ

ISP: O2 Czech Republic A.S.

Ultrarychlý internet až 1 Gb/s

Ověřte dostupnost

Internet HD již od 349 Kč

Novinka: Internet na vaši adrese s rychlostí až 1000 Mb/s. Časové omezená nabídka.

Learn Build Browse



Proč se jedná o bezpečnostní riziko?

- Předpokladem je přihlašovací pokus ze „zavirovaného“ PC.
- Nedá se předpokládat, že by se útok vyplatil kvůli 1 oběti.
- Adopce eObčanky bude nejspíše do budoucna stoupat.
- Masové rozšíření viru tak může být výhledově zajímavé:
 1. Ekonomická motivace
 - Daňové vratky (daňový portál, ePortál ČSSZ)
 - Přístup k lékům na předpis (eRecept)
 2. Politická motivace
 - Ovlivnění či znevěrohodnění potenciálních online voleb




Co je reálným výstupem tohoto nálezu?

e-identita.cz
KLÍČ K ELEKTRONICKÝM SLUŽBÁM


8. června 2021

Česky ▾

Proces přihlašování probíhá, prosím, počkejte.
ID transakce: **deac8708-7268-42a2-9e63-ac478be19251**



Identifikace občanským průkazem



Zadejte identifikační osobní kód

Zadejte hodnotu IOK pomocí klávesnice počítače. Po zadání IOK stiskněte tlačítko **OK**

Datum a čas
08.06.2021 9:32:35

ID transakce
deac8708-7268-42a2-9e63-ac478be19251

Zadáním hodnoty IOK udělujete souhlas s provedením identifikace

OK Zrušit



Shrnutí penetračních testů

- Řetěz kybernetické obrany je jen tak silný jako jeho nejslabší článek
- Penetrační testování je o odhalování těchto slabých článků
- Penetrační test = den, týden, měsíc dlouhý útok na...
 - ...podnikovou infrastrukturu
 - ...aplikaci (web, API, mobil, desktop)
 - ...produkt (hlavní jednotka auta, domácí alarm, IoT)
- Výstupem je report a prezentace slabých článků (zranitelností)
- Technický přínos = robustnější produkt / infrastruktura
- Business přínos = útočník při stejném úsilí neuspěje (útok se nevyplatí)



Děkuji za pozornost

Auxilium Cyber Security

martin.pozdena@auxiliumcybersec.cz

+420 739 467 470