Petr Krčmář

Nebezpečné staré protokoly a co s nimi

(LinuxExpo, 20. dubna 2010)

ROOT.CZ

Lokální vs. vzdálená bezpečnost

- Dnes se běžně chrání lokální systém
- Hesla, antiviry, osobní firewally
- Nebezpečné protokoly méně *(řekni historku)*
- Staré i 40 let (FTP a SMTP z roku 1971)
- Při návrhu funkčnost, ne bezpečnost
- Ke všem existují náhrady nebo nadstavby
- Chybí osvěta mezi běžnými uživateli i adminy

Hlavní principiální problémy

- Možnost odposlechu přihlašovacích údajů
- Možnost odposlechu přenášených dat
- Náchylnost k MITM
- Falšování přihlašovacích údajů

- Jakákoliv bezpečnostní opatření jsou marná

Jediné řešení = šifrování!

ROOT.CZ

Odposlech velmi snadný

- Hotová řešení ke stažení z internetu
- Wireshark/Ethereal (jdem.cz/eupy5)
- dumpcap, dsniff a mnohé další
- Možnost odposlechu na Wi-Fi
- Stejně tak na Ethernetu (ARP spoofing)
  - jdem.cz/eup45
  - Příkaz arpspoof (balík dsniff)
  - Možnost data na „routeru“ pozměnit
-

Praktický výstup automatu

```
dsniff: using netdump
-----------------
04/19/10 21:46:35 tcp 192.168.1.102.38278 ->
zeus.webzdarma.superhosting.cz.21 (ftp)
USER mujwebikdomaci
PASS heslickotajne

-----------------
04/19/10 21:46:35 tcp 192.168.1.102.60382 →
plch.iinfo.cz.80 (http)
GET / HTTP/1.1
Host: bugzilla.iinfo.cz
[krcmar:mamamelemaso]
```

- Umí FTP, telnet, SMTP, HTTP, POP, NNTP, IMAP, NFS, X11, IRC, ICQ, AIM, PostgreSQL, SMB a další.

ROOT.CZ

FTP bohužel nejčastější

- FTP stále nejčastěji využívaný pro web
- Dokonce třetina čtenářů Roota (jdem.cz/euqe4)
- Standardně nezabezpečuje heslo ani data
- Použitelné jen u veřejných úložišť
- **Řešení:** FTPS nebo SFTP
- SSL nebo přenos přes SSH
- Odbočka: Total Commander a hesla

ROOT.CZ

POP3 a IMAP4

- Mýtus: „IMAP je vždy bezpečnější než POP“
- Velmi často je stále používán POP3
- Řada serverů stále bez SSL
- Gmail už ne-SSL varianty nepodporuje
- Namátkou: Seznam.cz a Centrum.cz ano(!)
- **Řešení:** POP3S a IMAP4S

HTTP

- Standardně zcela nezabezpečeno
- Velmi často přenáší citlivá data
- Včetně přihlašovacích údajů
  - Formuláře, Apache heslo,...
- **Řešení:** HTTPS, nebo alespoň SSL formuláře
  - challenge response (jdem.cz/euqu4)

To nejsou zdaleka všechny!

- Naštěstí od mnohých se ustoupilo (telnet)
- Další postupně mizí (starší ICQ)
- Správci serverů: nenabízet nebezpečné protok.
- Správci sítí: hlídat a blokovat použití
- Cokoliv opouští počítač by už mělo být zabezpečené!
- Nikdy nevíte, kdo může poslouchat.

Děkuji za pozornost

Petr Krčmář
www.root.cz, www.debian-linux.cz
petr.krcmar@iinfo.cz
GPG: 9FBEA4F5

ROOT.CZ