Curs 12

Servicii de acces la distanță

Gestiunea serviciilor de rețea (GSR)

12 ianuarie 2017

Departamentul de Calculatoare, Comunitatea RLUG

Cuprins

,,Perimetrul" unei organizații

- accent pe securitate
- access doar din cadrul perimetrului
- serviciile și sistemele accesibile doar în cadrul perimetrului
- există servicii publice, dar nu fac parte din perimetru

Punct de intrare in perimetru

- accesul din exterior
  - pe baza unor reguli
- din punct de vedere logic/topologic cel din exterior este în perimetru
- în general acces securizat (criptat)
- un canal/tunel securizat pentru accesul în perimetru prin intermediul punctului de intrare

Forme de acces în perimetru

- deschiderea unui canal pentru un serviciu: SSH
- crearea unui canal prin care o stație întreagă este văzută ca parte a perimetrului: VPN
  - despre concentratorul pentru VPN
  - VPN selectiv

Two-factor authentication

- Two-factor authentication (2FA) este o metodă de a confirma identitatea utilizatorului folosind două componente diferite
- 2FA este o formă de multi-factor authentication
- Scopul este acela de a garanta ca în spatele tasturii se află (fizic) un utilzator legitim și nu un atacator
- 2FA protejează de asemenea împotriva mișcarii laterale în perimetru (accesarea unor alte mașini folosind un nod compromis)

Opțiuni de autentificare pentru 2FA (1)

- OTP
  - Ușor de folosit
  - Interoperabil
  - Un device extern generează numere (time sau sequence-based)
  - Util pentru utilizare non-frecventa (consumer usecases)
- Biometrics
  - Dificil de folosit
  - Interoperabiltate redusă
- Smartcarduri
  - Suport limitat pentru readere
  - Configurare și management dificile

Opțiuni de autentificare pentru 2FA (2)

- Token-uri USB
  - Ușor de folosit
  - Pot funcționa ca device-uri OTP sau ca o cheie privata a utilzatorului
  - În mod OTP, pot emula o tastatură, permitând folosirea unor coduri OTP lungi
  - Ușor de configurat și de folosit
  - Pierderea device-ului reprezintă un risc

Exemplu de token USB: Yubikey (1)

https://www.yubico.com/wp-content/uploads/2015/11/YK4-In-Use-3-crop-third-444x224-1-444x224.png

Exemplu de token USB: Yubikey (2)

- Oferă suport pentru FIDO U2F, PIV, PGP, OTP
  - FIDO U2F (Universal 2nd Factor) este un standard de autentificare deschis, dezvoltat de Google, Yubico și NXP, cu suport în Chrome, Firefox, Mozilla
  - PIV (Personal Identity Verification) permite realizarea de operații de semnare/decriptare RSA sau ECC folosind o cheie privată stocată pe device-ul USB, prin intermediul unei interfețe standard
  - OpenPGP este un standard deschis pentru semnare și criptare. Permite operații de semnare/criptare RSA sau ECC folosind o cheie privată stocată pe device-ul USB

Tunele

- un canal sigur de comunicare prin care trece trafic
- traficului îi este oferită impresia prezenței în perimetru
- tunelare Layer 2, Layer 3, Layer 7 (doar spre anumite aplicatii exista acces)

Cuprins

VPN

- Virtual Private Network
- roluri, obiective, cazuri de utilizare

Tipuri de VPN

- IPSec VPN
- SSL VPN

IPsec (1)

- Protocol standard de creare a tunelelor securizate între:
  - două locații distincte sau două rețele distincte: `Site to Site`
  - între un dispozitiv și o locatie: `Client to Site`
- este un protocol standardizat folosit în Internet

IPSec (2)

- Ridicare unui tunel se efectuează în doi pași (sau două faze):
  - `Phase1`: autentificarea capetelor de tunel folosind `pre-shared key` (PSK) sau certificate digitale, și agreearea parametrilor de criptare
  - `Phase2`: setarea tunelelor și a `Security Associations` (SA), 2 per tunel, câte una pe sensul de trafic

SSL VPN

- Folosește protocolul TLS pentru încapsularea traficului de interes
- Foarte popular pentru că poate funcționa chiar și prin Proxy

Tunelare Layer 3

- despre încapsulare
- pachetele de nivel 3 sunt trecute prin tunel
- se lasă impresia apartenenței la aceeași rețea logică

StrongS/WAN

- Implementare `Open Source` a standardelelor `IPSec`
- Permite crearea de tuneluri de tip `Remote Access` între clienți și rețeaua locală
- Fișierul de configurare este de obicei `/etc/strongswan/ipsec.conf`

Cuprins

Remote Desktop access

- cazuri de utilizare
  - accesarea de la distanță a unui desktop în mediu grafic pentru administrare

Implementări de remote desktop

- `RDP`: folosit exclusiv pentru stații și servere Windows. Permite folosirea de `gateway`-uri, astfel încat dinspre Internet să fie deschis un singur port; iar clientul să poată accesa oricât de multe desktop-uri din interiorul rețelei
- `VNC`: protocol multiplatformă, poate fi folosit pe aproape orice sistem de operare care are un `GUI`

Cuprins

Acces la distanță

- perimetru sigur
- punct de acces în perimetru
- tunel, canal sigur
- VPN

Implementări de acces la distanță

- SSH
- VPN: IPsec si OpenVPN
- Remote Desktop Protocol