Bezpečnostní audit počítačové sítě

Martin Soukup

semestrální práce předmětu Y36SPS

FEL ČVUT

Zadání práce

- Úkolem mé semestrální práce bylo provédst bezpečnostní audit počítačové sítě.
- Prováděl jsem scanování portů, zjišťování konfigurace firewallu, prohlížení topologie sítě.

Schéma sítě

- Přiloženo na stránkách

Připojení školy k Internetu

- Oficiální informace
  - 2Mbps
  - Technologie Wi-Fi

Server

- RedHat Linux
  - 4. roky starý systém
  - Předchozí byl vyměněn po úspěšném útoku hackera
  - Zprostředkovává:
    - Webový server
    - Poštovní server
    - DHCP server
    - DNS server
    - Sambu – přihlašování uživatelů + osobní soubory
    - Překlad ip adresy z „veřejné“ na neveřejné (masquerade)
    - Veřejná ip se na počítači tváří jako neveřejná, ale je na ní směrovaná veřejná adresa od zprostředkovatele Internetu

Klientské stanice

- Počet stanic se pohybuje okolo 40 PC
- Z 99% je na stanicích naistalován systém Windows XP
- Linux pouze na pár počítačích jako dualboot pro potřeby výuky (ukázka Linuxu)

Porty na serveru

- Na intranetové straně:
  - TCP
    - ftp, ssh, smtp, http, pop3, rpcbind, auth, netbios-ssn, imap, https, microsoft-ds, doom, imaps, pop3s
  - UDP
    - dhcp, dns
- Na veřejné straně
  - TCP
    - ftp, smtp, http, pop3, nntp, imap, https
  - UDP
    - dns

Bezpečnost serveru

- Největší možnosti ohrožení serveru jsou možně z intranetové strany (velké množství otevřených portů)
- Neočekává se však útok od studentů.
- Na Internetové straně je zbytečně otevřen pouze jeden port a to nntp (119/tcp)

- Firewall ve formě jak ho znám já (iptables) implementován neni.
- Prý je řešen jinak.

Wi-Fi

- Síť je šifrovaná pomocí WEP
- Nízká úroveň zabezpečení, zde však dostačující, jelikož AP má malý dosah (jen v budově) a pokud jste v budově, můžete si přečíst heslo napsané na stěně.

Navrhovaná řešení

- Server
  - Aktualizovat
  - Uzavřít zbytečné porty
  - Spustit firewall

- Wi-Fi
  - Změnit šifrování na WPA 2

Dotazy a Poděkování

- Nějaké otázky?

- Děkuju za pozornost