Audit bezpečnosti počítačové sítě

Předmět: Správa počítačových sítí

Jiří Kalenský

kalenj1@fel.cvut.cz

Zadání

- Prověřit bezpečnost v dané počítačové síti (cca 180 klientských stanic)
- Nejsou povoleny destruktivní metody, zjišťování hesel hrubou silou atd.
- Není povoleno zjišťování jinde než v základní LAN (tj. do míst, kde síť spravují jiné organizace)
- Již jsem měl základní povědomí o topologii sítě, ale od mé poslední pracovní činnosti v organici se změnil IS a další…

Postup

1. Zjištění topologie sítě
2. Na základě zjištění skenování
   - služeb serverů a jejich problémů
   - zachytávání síťové komunikace
3. Další pokusy v síti a na IS
4. Průzkum klientských stanic
   - zabezpečení stanic
   - zajištění SW updatů atd.
5. Pokus o vstup z internetu

1. Topologie sítě

1. Programem SuperScan jsem provedl sken v rozsahu z přiděleného počítače.
   - ozvala se spousta počítačů
   - B-rozsah IP adres, značné plýtvání adresami
   - z uvedeného a názvů jejich stanic a přidělení oddělením jsem se pokusil určit
   - Totální chaos – IP adresa je přidělena na základě MAC adresy, ale jejich číslování je prováděno jak kdy – inkrementálně, dle oddělení i dle lokace a tato rozdělení jsou kombinována dle „nálady“ správce ☺

2. Skenování serverů

- Na serveru „200“ běží IS
  - množství otevřených UDP portů pro klienty
  - dále spousta služeb jako FTP (21), SSH (22), DNS (53), HTTP (80), LinuxConf (98), SunRPC (111), NetBios (139), Remote Login (513), Shell (514), Printer (515), NFS (2049)
  - Verze Samby s bezpečnostní chybou

    http://www.securityfoxus.com/bid/121
  - WWW rozhraní pro zadávání SQL dotazů do IS běží pouze v nešifrované formě

2. Skenování serverů

- Na serveru „230“ běží GW z vnějšího světa
  - z vnějšího světa má otevřené porty pro SMTP a SSH
  - Na této GW je taktéž konfigurovaná VPN linky pro externí pobočky (zbytek VPN je v kompetenci providera) – externí pobočky jsou pak plně začleněny do LAN (i přístup k internetu se řeší přes vnitřní síť)
  -  Z vnitřní sítě mají správci pro konfiguraci stroje povolený Telnet a FTP (versus SSH)

3. Delegace práv

- Admini tvoří na serveru 231 ručně tabulku povolených MAC adres
- Tři stupně oprávnění
  1. Plný přístup ke GW (pouze admini)
  2. plný přístup ke GW, ale zákaz některých IP / domén (několik vybraných uživatelů)
  3. Přístup na internet přes proxy server (kontextový, tj. „tunel“ neprojde, navíc je zde restrikce obsahu) + na GW povolen port 110 (což bylo dříve přes proxy)

Přes port 110 lze otevřít tunel ven !

3. Delegace práv + testování

- Pokud je DHCP serverem (231) přidělena IP adresa, je o tomto informován IS a ten otevře na serveru port pro klienta (číslo portu vyplývá z IP)
- Pokud si sám nastavím volnou IP, bránu atd., funguji v síti, ale nedostanu se na internet ani k IS
- Pokud někomu „ukradnu“ IP, tak se dostanu k internetu, ale nedostanu se k IS
- Pokud si zfalšuji MAC a odpojím uživatele, tak v případě, kdy má klient otevřenou seanci s IS (je přihlášen), tak sezení zůstává „otevřené“(funguje na UDP) a pracuji v IS pod jeho účtem!!!

4. Klientské stanice - Windows

!!! PROBLÉM !!!

- Dříve cca 40 stanic, dnes již méně
- Různé OS (od 95 až po Vista)
- Není žádný doménový server, tj. žádné uživatelské řízení přístupu, kdo si jak počítač nastaví, tak mu chodí!
- Po jednom virovém útoku, který složil celou síť, je nyní pouze centrálně distribuována a řízen NOD32 (uživatelé nemají oprávnění měnit jeho nastavení, ale mohou ho odinstalovat – což správce zjistí tím, že počítač neprovádí aktualizace)

4. Klientské stanice - Windows

- Chybí server, který by zajišťoval automatické instalace a aktualizace SW
- Správce si na stanice nahrál TightVNC (nešifrovaný kanál), které má vždy otevřený svůj port a případně se pouze na dálku připojí k PC a aktualizaci provede tak, že pro různé verze Windows má na serveru nastaveny různé aktualizační skripty, které ručně spustí
- Nastavení sdílení a přístupových práv je tak plně v kompetenci uživatele – tj. někde se dá podívat i na celý počítač, případě kompletně do dokumentů!

Závěrem

- Nevhodně provedená IP adresace
- Spousta HUBů, tj. komunikace lze dobře zachytávat
- Admini nemají svojí správu šifrovanou (SQL, FTP, Telnet)
- Oproti tomu IS (většina komunikace na síti) používá šifrovanou komunikaci
- Problematická je totální absence řízení Windows klientů
- Přístup zvenčí se zdá být v pořádku, ale nechápu zbytečné otevření přístupu pro interní www server