Jiří Kalenský
kalenj1@fel.cvut.cz

Audit bezpečnosti počítačové sítě

Semestrální práce Y36SPS

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

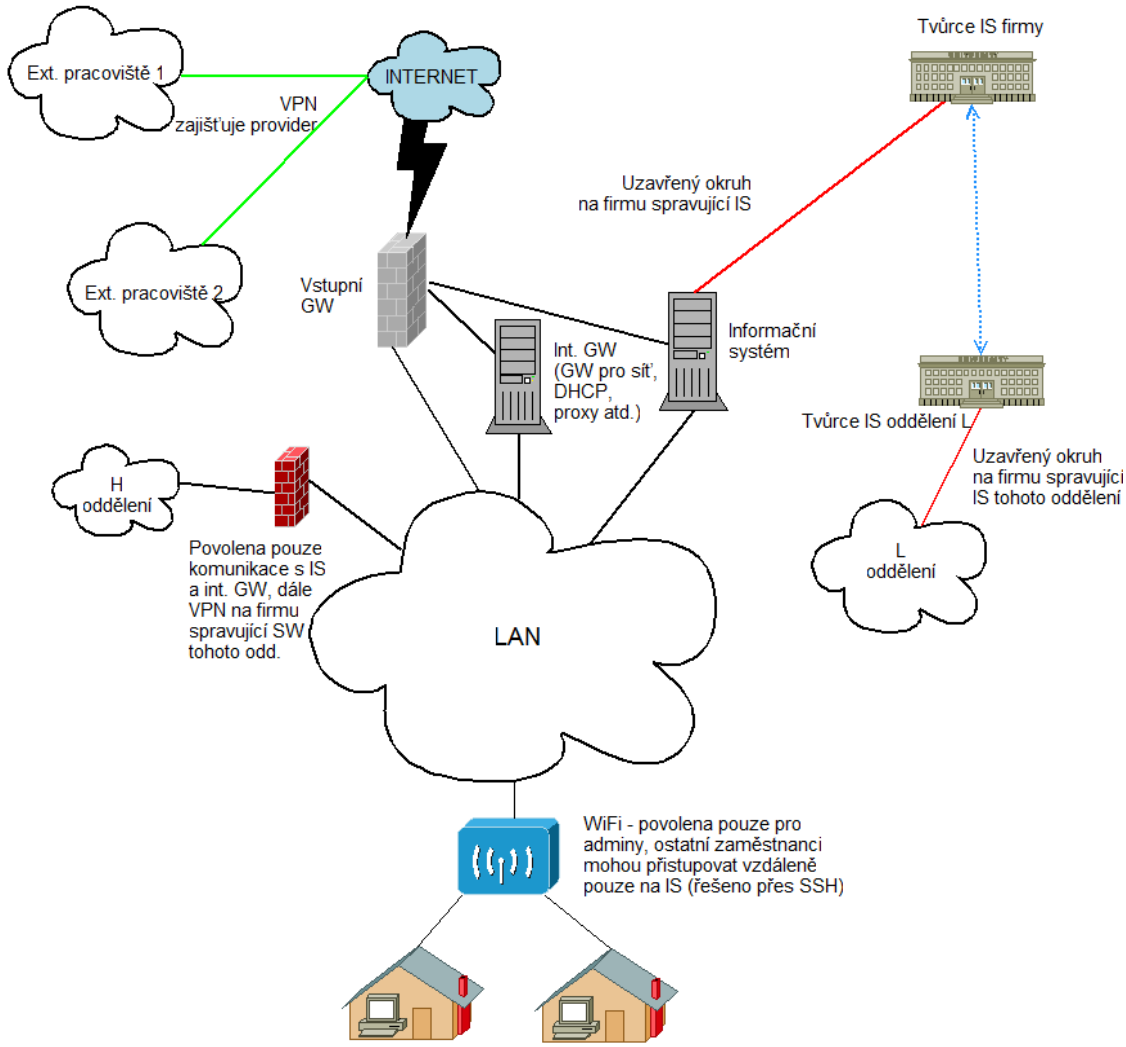
Topologie sítě

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 ☺

Výsledná topologie (mimo pokus o zjištění serverů pochází ze znalostí sítě vzhledem k tomu, že jsem měl povoleno pracovat pouze v části označené jako LAN).

Spojnice mezi vstupní GW a servery jsou zde z ilustrativního důvodu pro prezentaci.



Skenování serverů

- Pomocí programu LANGuard jsem prováděl sken portů serverů (IP adresy a/nebo názvy serverů byly zjištěny z nastavení počítačů)
- Po skenování bylo zvláštní, že 4 servery nabízejí zcela stejné služby a vlastnosti, nakonec zjištěno, že 1 serveru je přiděleno několik DNS záznamů a z historických důvodů tyt 4 záznamy směřují do 4 různých C-rozsahů…
- 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
    - ☠ WWW rozhraní pro zadávání SQL dotazů do IS běží pouze v nešifrované formě
- 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)
- Na serveru „231“ běží GW pro vnitřní síť
    - FTP (21), SSH (21), SMTP (25), DNS (53), HTTP (80), POP3 (110), SUNRPC (111), NetBIOS (139), HTTPS (443), Microsoft DS (445), Proxy (3128)
    - nebyly zjištěny žádné vážné nedostatky (SMTP je na autorizaci atd.)
    - tento server obsahuje instalace, aktualizace SW

Delegace práv

- Admini tvoří na serveru 231 ručně tabulku povolených MAC adres (sděleno od správce)
- Tři stupně oprávnění (což je ve firmě obecně známo)
    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 !

Testování delegace práv

- 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!!!

Zachytávání paketů

Na klientských stanicích byly zachytávány pakety. Zjištěné informace

- Spousta HUBů (i v řadě), tj. obsahu se ke klientovi dostane hodně ☹
- IS posílá každou změnu (tj. i stisknutí znaku) jako samostatnou událost, ale používá šifru, tj. pouhým zachytáváním se práce s IS nepřečte
- Díky velkému rozsahu je tam značné množství ARP dotazů – při „standardní“ práci pouze s IS tvořily ARP pakety 25% celkového množství paketů!

Zabezpečení klientských stanic

- Drtivá většina stanic jsou bezdiskové – zde po síti startuje FreeDOS spolu – tento je konfigurován na serveru a spouští se pouze klient IS. Klienti odpovídají pouze na ICMP, ostatní porty jsou uzavřeny (komunikují pouze se serverem)
- Cca 20 linuxových stanic. Bohužel jsem k ni neměl přístup, ale měly by být konfigurovány centrálně ze serveru. Opět odpovídají na ICMP a porty mají uzavřeny.

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 tí, že počítač neprovádí aktualizace)
- 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!

Přístup zvenčí

- Dříve popsaný server „230“
- Bezdisková stanice
- Zvenčí jsou otevřeny pouze tři porty:
    - SSH – autorizace se provede oproti IS a pokud je uživatel úspěšně autentifikován, otevře se tunel pro komunikaci s IS serverem
    - SMTP – pokud je email pro danou doménu, tak server email přijme (nekontroluje uživatele) a teprve po přijmutí emailu předává v rámci sítě email poštovnímu serveru.
    - WWW – předává na server 231 (PROČ, když to je jen mirror, web běží u providera!)
- Pokud skenuji porty moc rychle za sebou, tak server neodpovídá ani na tyto povolené porty

Závěr

- 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