SECURIZAREA INFORMAȚIEI DE AUTENTIFICARE ÎN REȚELELE WIRELESS

Nicolae STURZA

Universitatea Tehnică a Moldovei

Abstract: *Tehnologiile moderne fără fir pot interconecta echipamentele (sau şi reţelele locale, LAN-urile) la distanţe mici, dar şi la distanţe mari. În pofida faptului că ele au adus multe avantaje, reţelele fără fir sunt cele mai vulnerabile la atacuri, deoarece este dificil de prevenit accesul fizic la aceste reţele, singurul avantaj este că atacatorul trebuie să se afle în apropierea acestor reţele. Pentru a putea menţine securitatea acestor tipuri de reţele un administrator trebuie să cunoască breşele de securitate şi tipurile de atacuri care ar putea profita de aceste vulnerabilităţi.*

Cuvinte cheie: *Securitate, vulnerabilitate, protocol, comenzi, cheie, firewall, wi-fi, reţele Wireless.*

1. Introducere

Problemele de securitate din orice reţea de calculatoare derivă dintr-o contradicţie fundamentală a Internetului şi anume caracterul public dorit de utilizatori pentru orice resursă informaţională şi nevoia de securizare a informaţiilor şi a reţelei în sine faţă de atacurile persoanelor rău-intenţionate care urmăresc compromiterea, preluarea, modificarea sau distrugerea informaţiilor ori întreruperea funcţionării reţelei.

Comunicaţiile Wireless prezintă un risc mai mare de atac în comparaţie cu cele efectuate prin cablu ceea ce impune aplicarea unor măsuri de securitate speciale pentru comunicaţiile prin undă radio, conform protocolului AAA (authentication, authorization, accounting). Cele mai mari riscuri de securitate apar în reţelele Wi-Fi publice, de tip sistem deschis, în care accesul este liber iar securitatea trebuie asigurată la nivelul serverelor şi al oricărui terminal, precum şi diferenţiat pentru fiecare client acolo unde se impune confidenţialitate. Totuşi şi informaţiile publice pot fi atacate în scopul inducerii în eroare a utilizatorilor prin modificarea datelor.

2. Vulnerabilitatea reţelelor wireless

Pentru a testa breşele de securitate a unei reţele Wireless se va utiliza un sistema de operare, şi anume BackTrack. BackTrack este un sistem de operare Linux, debían, utilizat pentru testarea , penetrarea securităţii şi depistarea vulnerabilităţilor din sistema, fiind dedicat hacking-ului. BackTrack poate fi instalat pe HardDisk, cu Windows, rulînd două sisteme de operare pe acelaşi PC sau poate fi utilizat de pe ”live SD”, stick USB sau poate fi utilizat într-o maşină virtuală(Virtual Box).

BackTrack este dedicat pentru diverse categorii de public de la utilizatori iniţiali pînă la profesionişti, venind cu o mulţime de pachete preinstalate pentru testarea securităţii. Astfel atît fiecare pachet, kernel-ul de configurare, script-ul şi patch-urile sunt doar cu scop de tester şi penetrare. În continuare va fi prezentat modul în care are loc testarea unei reţele Wireless pentru a depista punctele vulnerabile cît ţine de securitatea informaţiilor de autentificare.

Pentru a iniţia procesul de testare a reţelei WIRELESS vor fi necesare următoarele materiale**:**

- placă de reţea,
- un live CD,
- un stick usb cu Back Trak, sau un soft de virtualizare (VirtualBox),
- un calculator sau notebook, care dispune de o placă de reţea compatibilă.

1. Se bootează de pe live Cd, stick USB sau se crează bootarea în softul de virtualizare (VirtualBox**),**

2. Se dă comanda **„start x”** pentru a deschide sistemul de operare BackTrak.

3. Se deschide terminalul de comenzi a sistemului de operare BackTrak şi acum pot fi date anumite comenzi.

4. Se introduce comanda **airmon-ng** (se determină tipul reţelei şi se verifică dacă disponibilă).

5. Se introduce comanda **airmon-ng start wlan0 (**se porneşte Wireless wlan0 în mod monitorizat şi se obţine o interfaţă virtuală iniţializată ce poate monitoriza traficul).

6. Se introduce comanda **wash –i mon0** (se scanează rețelele wi-fi disponibile), se copie SSID-iul unui router găsit și se introduce în următoarea comandă**.**

Figura 1 Rețelele wi-fi disponibile

7. Se introduce comanda **reaver -i mon0 -b 54:E6:FC:BD:18:A7** (SSID-ul) și se adaugă**–d** (pentru a reduce timpul) și **–vv** (pentru a vedea pe viu procesul în întregime).

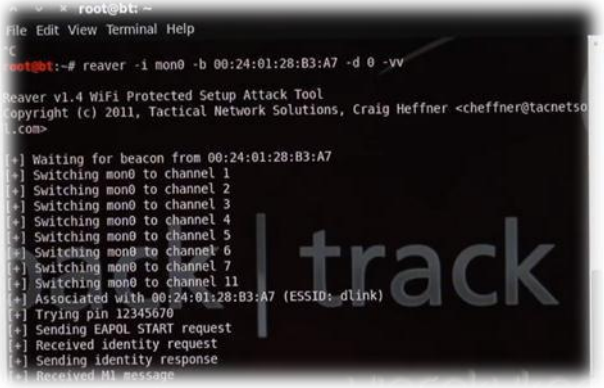

Figura 2 Procesul de ghicire a pinurilor

8. După finisarea acestui proces de ghicire a pinurilor, în terminal va apărea informația referitoare la: **WPS PIN, WPA PSK**, aceasta este informația cu care se poate de logat la o rețea wi-fi străină[2].

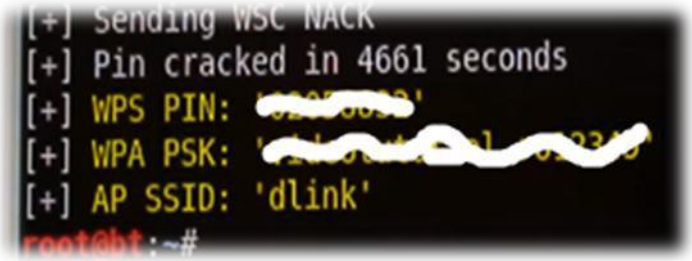

Figura 3 WPS PIN, WPA PSK ghicite după procesul de scanare[2]

3. Implementarea unei rețele Wi-Fi ultra-sigure

Pentru a implementa o rețea ultra-sigură e nevoie de ținut cont de următoarele aspecte de siguranță referitoare la rețeau wi-fi:

1. *Locația și accesul fizic*
2. *Configurarea AP-ului*
3. *Design-ul rețelei*
4. *Implementarea unei politici de securitate moderne*

3.1 Locaţia şi accesul fizic

Plasamentul unui AP este critic pentru securitatea unei reţele wireless. Aici trebuie de luat în consideraţie două aspecte: accesibilitatea şi puterea semnalului.

AP-ul ar trebui plasat într-o locaţie greu accesibilă unui atacator, pentru ca acesta să nu-l poată modifica cu propriile setări, conectîndu-se cu un laptop prin intermediul unui port USB unde poate să configureze cheile WEP.

Semnalele folosite de reţelele wireless sunt semnale radio, ce oferă de obicei o rază mai mare decăt cea furnizată de producători. Ideal ar fi ca semnalul să fie puternic în limitile zonei de acoperire acceptate şi foarte slab în afara ei pentru a putea preveni atacurile reţelelor wi-fi.

3.2 Configurarea AP-ului

Acest aspect ţine cont de configurarea AP-ului. Fiecare producător foloseşte o interfaţă de configurare diferită, cu aceleaşi concepte de bază, aici ar fi o greşeală mare dacă vor fi schimbate setările prestabilite şi vom introduce dispozitivul în reţea, chiar dacă schimbăm ESSID-ul şi numele AP-ului care pot fi aflate uşor cu ajutorul unui utilitar de tip sniffer.

Cheile WEP de 128 biţi ar trebui de asemenea să fie activate, deşi un atacator le poate sparge în cîteva ore totuşi reprezintă un pas important pentru o reţea securizată, recomandabil ar fi ca cheia să fie schimbată periodic.

Un alt serviciu disponibil pe majoritatea AP-urilor este DHCP (Dynamic Host Configuration Protocol) care asigură adresele IP clienţilor dintr-o reţea, configurarea manuală cu atenţie a severului DHCP ce asignează adresele IP. În acest fel este mult mai uşor să urmărim atacurile deoarece fiecare utilizator este asociat cu o adresă IP.

Unele AP-uri pot filtra pachetele luînd decizii pe baza adresei MAC (Media Acces Control), ceea ce înseamnă că se vor putea conecta la reţea doar clienţii care apar într-o listă de adrese MAC specificată de administratorul de reţea[3].

3.3 Design-ul reţelei

Este foarte important de ştiut că nu doar reţeaua wireless ar trebui de securizat, pentru că întreaga reţea este supusă riscului cînd este activ un AP wireless.

Pentru designul unei reţele super – sigure AP-ul va fi separat de restul reţelei cu un firewall configurat cu reguli stricte, ceea ce înseamnă că utilizatorii se vor conecta la o subreţea separată de restul reţelei, iar atacatorul nu va avea acces la datele personale, important, chiar dacă reuşeste să spargă cheia WEP, iar dacă se doreşte să fie şi mai securizată se plasează un dublu firewall, apoi se plasează serverul VPN într-o zona DMZ (Demilitarized Zone) unde nu are acces fizic la reţea şi se plasează un echipament pentru detectarea intruşilor (IDS) în aceaşi reţea în care se află şi AP-ul.

3.4 Implementarea unei politici de securitate moderne

Avînd reţeaua configurată ea poate fi activată pentru utilizare, însă trebuie de ţinut cont de politica de securitate din companie, întreprindere sau domiciliu.

Este recomandabil de a nu plasa AP-urile în reţeaua internă, e necesar de a explica utilizatorilor riscul la care este supusă acea întreprindere dacă nu se repectă politica stabilită, trebuie de explicat faptul că cheile WEP se schimbă foarte des, periodic în regim manual sau automat pe fiecare staţie sau sunt trimise criptat[1].

4. Concluzii

1. Efectuînd acest articol am sistematizat informaţia şi aşa termeni ca: firewall, MAC, DMZ, IDS, wireless, wi-fi e.t.c. Toţi aceşti termeni sunt utilizaţi de ficare din noi practic în fiecare zi, iar noi nici nu ne dăm seama cît de importanţi sunt ei pentru păstrarea confidenţialităţii şi integrităţii informaţiei cu caracter personal.

2. La fel pot concluziona gradul de securizare a fluxului informaţional ce circulă pe internet în special securizarea reţelelor wi-fi, care după părerea mea sunt cel mai slab securizate la momentul actual prin experimentul demonstrat în partea practică a acestui articol.Este foarte important să fie bine structurată politica de securizare a informaţiei într-o societate aflată în apogeul progresului ştiinţific, unde 70% din vînzări se fac prin intermediul magazinelor virtuale, majoritatea transferurilor bancare, servicii şi o mulţime de modalităţi de comunicare se realizează prin internet. Noi nici nu ne imaginăm ce risc ne asumăm atunci cînd, procurăm produse, servicii, comunicăm cu cineva fiind conectaţi la o reţea wireless necunoscută de noi sau care nu ne aparţine.
3. Reţelele wireless au fost create cu scopul de a mări aria de conectare a dispozitivelor la internet, dar nu pentru a înlocui reţeau LAN cu cea wi-fi, de aceea trebuie să ţinem cont de implementarea procedeelor de securizare, trebuie să utilizăm pe larg softul sau dispozitivul firewall care are funcţia de a proteja calculatorul nostru sau întreaga reţea prin filtrarea pachetelor de date pentru a bloca unele atacuri de tip DDoS (Distributed Denial of Service). Paravanele de protecţie nu ne asigură 100% securitate a informaţiei noastre, au şi ele o limită de fitrare a pachetelor primite şi transmise, de aceea trebuie luate în consideraţie că există şi alte dispozitive, software şi hardware care trebuie implementate în procesul de securizare a reţelelor fără fir.

Bibliografie

1. Markus Feilner „Open VPN – Building and Integrating Virtual Private Networks”, Packt Publishing, BIRMINGHAM – MUMBAI
2. http://www.agir.ro/buletine/865.pdf
3. http://www.securitatea-informatiilor.ro/vulnerabilitati-informatice/folosirea-wps-in-securitatea-wi-fi-pune-in-pericol-utilizatorii/.