WI-FI SECURITY TOOL

Martin Hala
Bachelor Degree Programme (3), FIT BUT
E-mail: xhalam04@stud.fit.vutbr.cz

Supervised by: Matej Kačic
E-mail: ikacic@fit.vutbr.cz

Abstract: The main purpose of this tool is testing wireless networks security level for both personal and commercial use. It is based on latest knowledge about security of wireless networks. Key features are: portability - implemented on live linux distro, simple manipulation - well aranged GUI, testing - rich options of tests selection, security level evaluation - recommendations consequent on NIST standard.

Keywords: wireless security, wifi, WST, testing tool, aircrack, network sniffer

1 ÚVOD

Většina firem v současnosti se jen stěží dokáže obejít bez Wi-Fi sítí. Stoupající zájem o Wi-Fi sítě se projevuje i u domácích uživatelů, kteří je využívají pro připojení svých bezdrátových zařízení. Tato technologie je v posledních letech velmi oblíbená a snadno dostupná i pro běžné uživatele, kteří nemají dostatečné znalosti na jejich kvalitní zabezpečení.

Právě nedostačující úroveň zabezpečení je jednou z hlavních iniciativ pro vytvoření nástroje, který bude administrátora sítě kontrolovat, zda nastavená úroveň zabezpečení je dostatečná. Bude také informovat o tom, jestli síť splňuje doporučení vyplývající ze standardu NIST [1].

2 SPECIFIKACE POŽADAVKŮ

Nástroj pro testování bezpečnosti Wi-Fi sítí (Wi-Fi Security Tool) má posloužit jako uživatelsky přívětivá aplikace, která otestuje uživatelem vybranou síť na vybrané typy známých útoků, upozorní na slabá místa sítě a poradí administrátorovi, jak případnou danou bezpečnostní díru napravit. Po dokončení testů se zobrazí kompletní výsledky s konkrétními návrhy, jak zvýšit bezpečnostní úroveň.

3 ŘEŠENÍ

Vytvořil jsem live linuxovou distribuci, která vychází z distribuce BackTrack. Ta již v sobě zahrnuje veškeré nástroje, které jsou potřebné pro práci testovacího nástroje. Díky této implementaci je zajištěna bezproblémová přenositelnost.

3.1 SKENOVÁNÍ WI-FI SÍTÍ

Skenování Wi-Fi sítí je v nástroji rozděleno do tří částí. Uživatel si vybere možnost, která je pro něj nejvhodnější.

1. Skenování viditelných Wi-Fi sítí - Skenování probíhá pomocí nástroje *iwlist*, ze kterého se zjišťují veškeré potřebné informace o sítích, které mají povolené vysílání SSID. Lze využít interaktivní režim, při kterém se budou pomocí nástroje *tcpdump* odchytávat beacon packety

a informace z obsahu se promítnou do tabulky (dynamické změny úrovně signálů, přidávání a odebírání sítí, atd.).

2. Skenování Wi-Fi sítí se skrytým SSID - Pokud je SSID skryté, nástroj odchytává okolní provoz a rozluští skryté sítě. Využívá se přitom nástroje *Airdump*. Aplikace si sama zajistí přepnutí do monitor módu.
3. Ruční zadání SSID - Uživatel zadá název SSID sítě ručně do připraveného okna. Lze otestovat, zda zadaný název sítě vysílá SSID a tudíž je síť viditelná. Pokud ano, zobrazí se základní informace v přehledné tabulce.

3.2 Typy útoků

Jednotlivé útoky lze vybrat zvlášť nebo nastavit úroveň testování. V takovém případě se dle vybrané úrovně přidávají jednotlivé typy útoků. Využívá se útoků implementovaných v aplikacích typu *Aircrack-ng*, atp. Výsledkem testovaní není odhalení hesla pro vstup do sítě, ale varování o nízké úrovni zabezpečení a o následném prolomení ochrany.

Typ ochrany	Typy útoků
WEP	packet replay attack, Caffe Latte, Korek, Fake authentication, Hirte, Wesside
WPA/WPA 2	slovnik + rouge AP attack, wpa/wpa2 handshake capture, cracking WPA

Tabulka 1: Typy zabezpečení a možné typy útoků

V tabulce 1 jsou uvedeny typy zabezpečení Wi-Fi sítí a možné typy útoků na otestování úrovně zabezpečení.

V každém případě lze využít Brute-force útok na prolomení hesla. V tom případě je slovníkový útok rozdělen do 3 částí. V první části se vyzkouší slovník, složený z 500 nejhorších hesel zveřejněný v knize Perfect Password [2]. Další dvě části jsou složeny z českého a anglického slovníku, které jsou volně ke stažení.

Pokud nástroj prolomí ochranu sítě, oskenuje připojené uživatele a zobrazí otevřené porty uživatelů (pomocí nástroje *nmap*). Také vyzkouší útok na administraci access-pointu pomocí přihlašovacích údajů z továrního nastavení [3].

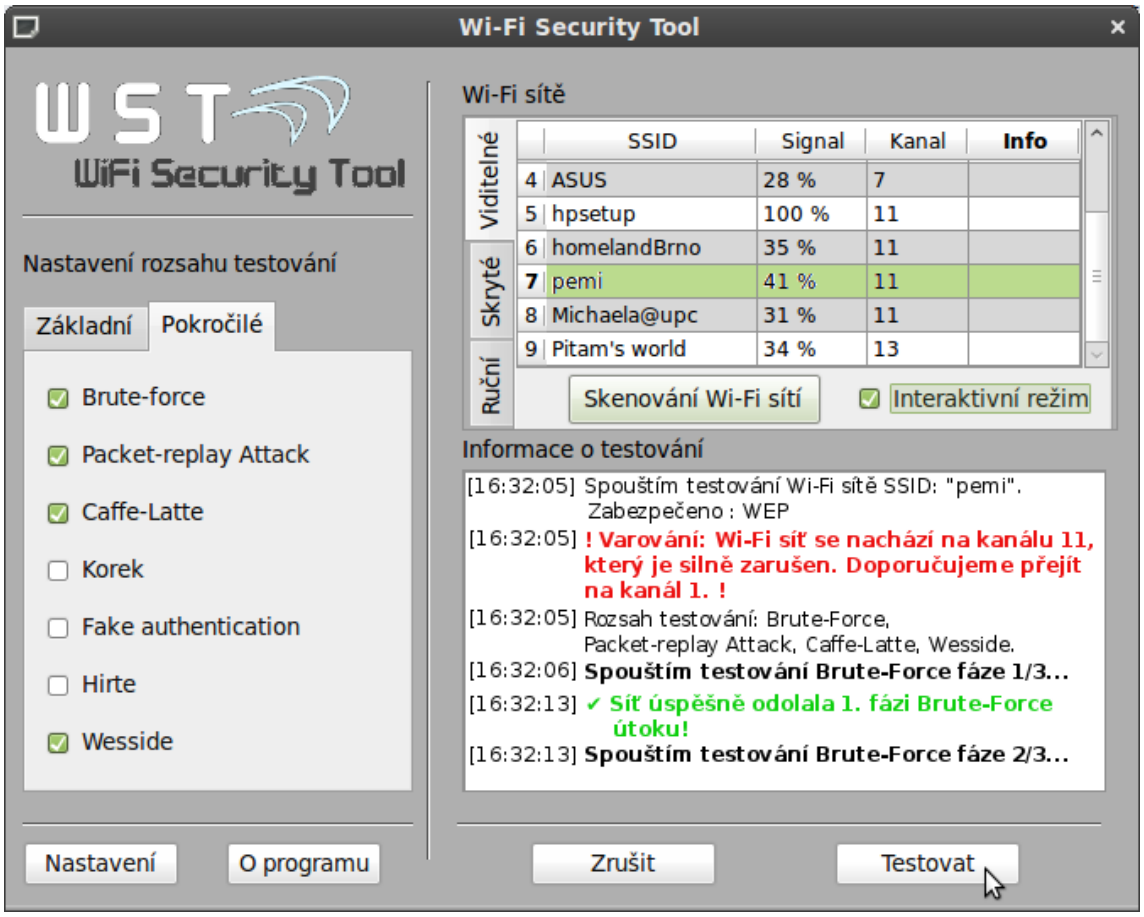
3.3 Security checklist

Volně přeloženo do češtiny "Seznam hodnotící zranitelnost Wi-Fi sítí"[4]. Jak již z názvu vyplývá, jedná se o seznam úkolů, které mají za úkol snížit zranitelnost bezdrátové sítě. Seznam se rozděluje do základních 6 kategorií, z nichž se větví na další podkategorie.

Tento checklist je základní kostrou celého testování. Podle daného pořadí dochází k postupnému ověření vlastností dané sítě, a to nejen z bezpečnostního hlediska. Případné nedostatky nástroj vyhodnotí po ukončení testů.

3.4 Uživatelské rozhraní nástroje

Uživatelské rozhraní je vytvořeno v QT a celý nástroj napsán objektově v jazyce C++. Cílem uživatelského rozhraní je přehlednost a jednoduché ovládání. V nastavení lze vybrat bezdrátové rozhraní, ze kterého se mají provádět veškeré operace. Veškeré informace se vypisují přehledně v informačním okně. Důležité zprávy jsou barevně odlišeny pro větší přehlednost. Po dokončení testování se otevře okno s konečnými výsledky. Také dojde k výpisu seznamu doporučení, která zlepší bezpečnostní úroveň sítě.



Obrázek 1: Obrázek uživatelského rozhraní nástroje.

4 ZÁVĚR

Aplikaci jsem úspěšně implementoval a splnil tak veškeré stanovené požadavky. Snažil jsem se o využití nejnovějších bezpečnostních znalostí v oblasti bezdrátových sítí. Využití této aplikace je velmi široké a doufám, že bude přínosem. Může se hodit běžným uživatelům, kteří nevědí, jak bezpečně nastavit svou domácí síť, ale mohou ji využívat i profesionální administrátoři pro dostatečné zabezpečení podnikových Wi-Fi sítí.

REFERENCE

[1] SCARFONE, Karen, et al. *Guide to Securing Legacy IEEE 802.11 Wireless Networks* [online]. 1. vydání. Gaithersburg : NIST, 2008 [cit. 2011-02-28]. Dostupné z WWW: <http://csrc.nist.gov/publications/nistpubs/800-48-rev1/SP800-48r1.pdf>.

[2] BURNETT, Mark. *Perfect Password : Selection, Protection, Authentication.* 1. vydání. Kanada : Syngress, 2005. 182 s. ISBN 978-1597490412.

[3] *Default Password List* [online]. 2010-10-22 [cit. 2011-03-01]. Default Password List. Dostupné z WWW: <http://www.phenoelit-us.org/dpl/dpl.html>.

[4] LISA, Phifer. *SearchNetworking.com* [online]. 2006 [cit. 2011-03-02]. Wi-Fi vulnerability assessment checklist. Dostupné z WWW: <http://searchnetworking.techtarget.com/feature/Wi-Fi-vulnerability-assessment-checklist>.