ComSource

Wi-Fi Pineapple - penetrační testy

Wi-Fi se stalo trvalou součástí našich životů. Bezdrátově se připojujeme v práci, ve veřejném prostoru, doma. Význam bezdrátového připojení roste. Přes Wi-Fi posíláme maily pracovní i soukromé. Píšeme si se svými blízkými, posíláme obrázky, videa, peníze, ... A nechceme, aby tyto údaje někdo ukradl a zneužil. Jsou však *access pointy*, na které přistupujeme bezpečné? Jasnou odpověď dostanete po provedení penetračních testů!

Přístupové penetrační testy

Phishing / sociální inženýrství
Získání citlivých údajů předstíráním identity/služby, kterou uživatel zná.

DWall
Nástroj, který slouží k odposlechu nešifrované komunikace uživatele.

Man-in-the-middle testy

Útok na WPS
Chytrý brute force útok na access point se zapnutou automatickou konfigurací.

SSL split
Penetrační test cílený na nepozorné uživatele či na weby, které mají self-signed certifikáty.

Výstupní auditní zpráva

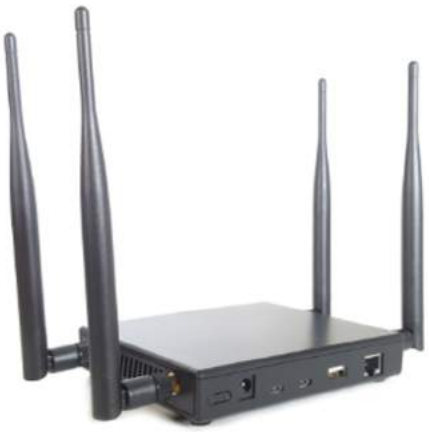
Odposlech Hash WPA
Identifikace uživatele, zaslání deauth výzvy, odposlechnutí hashe.

Útoky pomocí falešného webového portálu
Cíleno na konkrétní operační systémy, lze dosáhnout na administrátorská práva, apod...

ComSource s.r.o., Nad Vršovskou horou 1423/10, 101 00 Praha 10, IČ: 29059291
Zapsaná v obchodním rejstříku vedeném Městským soudem v Praze oddíl C, vložka 163642,
Bankovní spojení: 5576862001 / 5500 Raiffeisenbank, a.s.

ComSource

Přístupové penetrační testy



Phishing s využitím sociálního inženýrství

- Proskenování místní sítě a přístupových bodů.
- Replikace jednoho z bodů jako fake access point (AP).
- Kopie firemního webu, který zaměstnanci a uživatelé dobře znají.
- Výzva uživatelům k zadání přístupových údajů na základě smyšlené situace (například Update firmware, změna bezpečnostní politiky, podezření na zneužití účtu,...).
- Zaznamenání přístupových údajů a následné připojení uživatele k internetu.

Útok na WPS

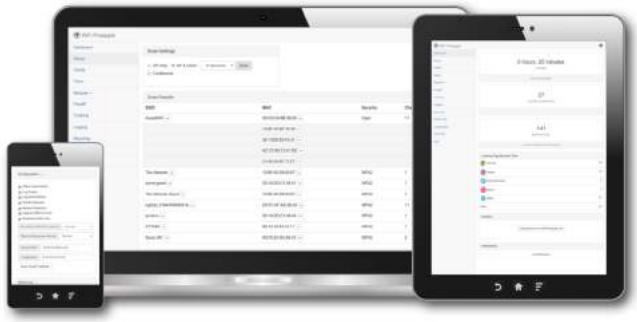
- Tento útok je možný jen na Wi-Fi řešení, které jsou určeny pro domácí použití, kde tato služba bývá defaultně zapnuta.
- Někteří vendoři používají jen omezenou množinu synchronizačních pinů, takový útok pak trvá jen pár minut.
- WPA2 AP s nestandardním PIN se například podařilo prolomit za cca pět a půl hodiny.

Odposlech WPA HASHe

- Přepnutím Wi-Fi karty do promiskuitního módu jsme schopni identifikovat uživatele i v síti, ke které nejsme připojeni.
- Vybereme si uživatele se silným signálem (čím silnější signál, tím rychlejší odposlech).
- Uživateli začneme zasílat deauth výzvu, čímž se odpojí na zlomek času od AP a pokusí se připojit znovu (má-li zapnuté automatické připojování k síti).
- Po dobu trvání útoku se uživatel nedostane na internet, na první pohled se mu zdá, že má problémy se stabilitou signálu.
- Odposlechnutí WPA2 HASHe od uživatele ve stejné místnosti zabralo například cca 4 minuty.
- Následně HASH můžeme prolomit s využitím software HASHCAT, který počítá na grafických kartách.
- HASHCAT lze využít k brute-force útoku, slovníkovému útoku nebo jejich kombinaci, například maskovaným útokem (znám počet znaků, požadavky na speciální znaky, počet a pozice cifer, apod.).
- Prolomení hesla pak trvá od vteřin až po dny dle složitosti.

Man-in-the-middle penetrační testy

DWall



- Při odposlechu nešifrované komunikace uživatele jsme schopni zachytit:
- HTTP URL.
- Cookies soubory (s jejich pomocí můžeme pokračovat v session i když uživatel třeba odešel domů).
- Data z HTTP POST.
- Obrázky.
- Nešifrované přihlašovací údaje (dnes už vzácnost).

SSLsplit

- Mířeno na nepozorné uživatele či na weby, které mají self-signed certifikáty (typicky firemní intranet, apod.)
- Komunikaci rozšifrujeme vlastním certifikátem, přečteme, opět zašifrujeme a odešleme na požadovaný server.
- Uživatel je varován, že web nemá důvěryhodný certifikát, pro pokračování musí uživatel souhlasit.
- Na velké weby s HSTS již nefunguje – prohlížeče nedovolí uživateli pokračovat a varují před možností MITM útoku.
- Otestováno, že hesla například na vnitrofiremní služby lze odposlechnout.

Útoky pomocí falešného webového portálu

- Místo výzvy pro vložení hesla na falešném webu jako u phishingu je uživatel vyzván spustit script.
- Pokud souhlasí, dostane přístup k internetu a vše vypadá normálně.
- Tyto útoky jsou cílené na konkrétní operační systémy, lze dosáhnout na administrátorská práva v PowerShellu apod.
- Uživatele může být připraven o data, přístup k počítači, lze se dostat na vzdálenou plochu.
- Tento útok je zpětně dohledatelný, uživatel si ho pravděpodobně všimne už během průběhu – vše musí proběhnout rychle.