Caleum

PENETRAČNÍ TESTY **PRO WI-FI**

Zvyšujeme přínos IT pro Vaši organizaci.

Wi-Fi připojení se stalo trvalou součástí našich životů a jeho význam stále roste. Bezdrátovým způsobem se připojujeme doma, v práci a také ve veřejných prostorách. Prostřednictvím Wi-Fi posíláme soukromé i pracovní e-maily, komunikujeme se svými blízkými, posíláme obrázky, videa, provádíme finanční transakce apod. Samozřejmě nechceme, aby nám tyto údaje někdo ukradl a zneužil. **Jsou však access pointy, na které přistupujeme bezpečné?** Jasnou odpověď na tuto otázku dostanete po provedení penetračních testů!

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

Odposlech WPA HASHe

- Přepnutím Wi-Fi karty do promiskuitního módu jsme schopni identifikovat uživatele také v síti, ke které nejsme připojeni.
- Vybereme si uživatele se silným signálem (čím silnější signál, tím rychlejší odposlech).
- Uživateli začneme zasílat tzv. deauth výzvu, čímž se na zlomek času odpojí od AP a pokusí se opětovně připojit (má-li zapnuté automatické připojování k síti).
- Po dobu trvání útoku se uživatel nedostane na internet a na první pohled se mu zdá, že má problémy se stabilitou signálu.
- Odposlechnutí WPA2 HASHe od uživatele ve stejné místnosti zabere přibližně 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 již nepracuje).
- Data z HTTP POST.
- Obrázky.
- Nešifrované přihlašovací údaje (dnes už je poměrně vzácné).

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 a pro pokračování musí uživatel souhlasit. Na velké weby s HSTS tento způsob již nefunguje – prohlížeče nedovolí uživateli pokračovat a varují před možností MITM útoku.
- Je z praxe dokázáno, že například hesla 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 zcela přirozeně.
- Tyto útoky jsou cílené na konkrétní operační systémy, lze dosáhnout na administrátorská práva v PowerShellu apod.
- Uživatele může tento způsob připravit o data, přístup k počítači, lze se dostat také na vzdálenou plochu.
- Tento útok je zpětně dohledatelný, uživatel si ho pravděpodobně všimne už během průběhu – vše se musí uskutečnit velmi rychle.

www.caleum.cz

Italská 438/36
130 00 Praha 3
+420 225 992 271
info@caleum.cz