Penetračné testy Wi-Fi sietí

AEC

Súčasťou infraštruktúry každej väčšej spoločnosti musí byť v dnešnej dobe aj bezdrôtová sieť, ktorá dovoľuje zamestnancom konektivitu z notebookov alebo mobilných zariadení z ľubovoľného miesta budovy. Bezdrôtové siete však tiež poskytujú nové vektory útokov pre potenciálneho útočníka s cieľom kompromitovať zamestnancov alebo internú sieť spoločnosti.

Penetračné testy pomôžu odhaliť možné slabiny alebo konfiguračné nedostatky v týchto sieťach, ktoré môžu byť následne podľa odporučení odstránené, čo útočníkom znemožní tieto vektory zneužiť a zvýši bezpečnosť a odolnosť siete voči reálnemu kybernetickému útoku.

Z dôvodu, že útočník sa pre prístup k bezdrôtovej sieti nemusí nachádzať bezprostredne v budove spoločnosti, ale iba v dosahu siete, ide o kritickú časť pre zabezpečenie.

Penetračné testy Wi-Fi technológií simulujú útok na prístup do vnútornej siete organizácie prostredníctvom bezdrôtového signálu Wi-Fi sietí. Po získaní prístupu bude preverená kvalita filtrovania prevádzky medzi sieťovým segmentom Wi-Fi klientov a zvyškom interných sietí.

Súčasťou testov je tiež analýza konfigurácie pripojenia k bezdrôtovej sieti na strane klientskych zariadení. Výstupom testu bude prehľad a zmapovanie prevádzkovaných Wi-Fi sietí a zoznam bezpečnostných nálezov s následným dopadom na vnútornú sieť organizácie.

Realizácia penetračných testov zahŕňa najmä nasledujúce kategórie:

- Mapovanie a analýza dostupných Wi-Fi sietí v areáli spoločnosti.
- Detekcia možných Rogue AP.
- Previerka zamestnaneckých Wi-Fi sietí.
- Pokus o získanie prístupu.
- Analýza filtrovania medzi Wi-Fi a LAN segmentmi siete.

www.aec.sk

Penetrační testy Wi-Fi sítí

Mapovanie a analýza dostupných Wi-Fi sietí v areáli spoločnosti

Cieľom je zmapovanie a analýza dostupných Wi-Fi sietí vnútri areálu spoločnosti. Analýza je zameraná na zmapovanie jednotlivých Access pointov a použitie technologických a kryptografických mechanizmov použitých na zabezpečenie autentizácie a prenášaných dát.

Detekcia možných Rogue Access Point (AP)

Ako Rogue Access Point (AP) je označovaný neautorizovane nasadený Access Point v priestoroch a najbližšom okolí spoločnosti. Rogue AP býva útočníkom najčastejšie nasadený s cieľom útoku na zabezpečenie súčasnej bezdrôtovej siete – v takom prípade útočník duplikuje nastavenie cieľovej siete. Druhou častou možnosťou je nasadenie otvorenej bezdrôtovej siete s cieľom následného útoku voči pripojeným staniciam či cieľom odpočúvania prístupových údajov.

Previerka návštevníckych Wi-Fi sietí

Fáza má za cieľ analyzovať zabezpečenie návštevníckych Wi-Fi sietí. Tieto siete sú obvykle nakonfigurované s otvoreným prístupom a autentizáciou pomocou captive portálu alebo so zabezpečením typu Personal (WEP, WPA-PSK s TKIP, WPA2-PSK s CCMP).

Previerka zamestnaneckých Wi-Fi sietí

Fáza má za cieľ analyzovať zabezpečenie zamestnaneckých Wi-Fi sietí. Tieto siete sú obvykle nakonfigurované ako WPA Enterprise s autentizáciou podľa štandardu 802.1X, výnimočne so zabezpečením typu Personal (WEP, WPA-PSK s TKIP, WPA2-PSK s CCMP).

Pokus o získanie prístupu

Postup útoku s cieľom získania neautorizovaného prístupu sa líši podľa použitého zabezpečenia siete. Existujú rôzne známe útoky na zabezpečenie WEP, WPA-PSK, WPA2-PSK alebo WPA-Enterprise, ktoré sú počas tejto fázy testované. Pre zabezpečenie WEP existuje mnoho zdokumentovaných útokov ako KoreK chopchop attack, Fragmentation Attack, ARP-request replay attack a ďalšie.
Pre WPA2-PSK to môže byť napríklad offline prelamovanie zdieľaného hesla alebo zneužitie povolenej WPS metódy autentizácie. V prípade WPA-Enterprise s použitím autentizácie podľa štandardu IEEE 802.1X je sieť preverovaná na výskyt slabých autentizačných metód (EAP-MD5, Cisco LEAP). Je tu overená správna konfigurácia a hardening siete a klientskych zariadení. Ďalej sú skúmané možnosti odchytenia citlivých dát, ako používateľských mien alebo hesiel.

Analýza filtrovania medzi Wi-Fi a LAN segmentmi siete

V tejto fáze dochádza k autorizovanému prihláseniu do všetkých testovaných Wi-Fi sietí spoločnosti pod poskytnutými používateľskými účtami. Následne je preverovaná dôslednosť oddelenia sieťového segmentu Wi-Fi klientov od iných citlivých segmentov siete (DMZ, produkcia…). V prípade prítomnosti rôznych VLAN je taktiež preverené vyššie uvedené

Naše prednosti

- Patríme medzi zavedené české security firmy, na trhu úspešne pôsobíme už dlhšie než 30 rokov.
- Máme viac než 10 rokov skúseností na poli bezpečnosti infraštruktúry a bezdrôtových sietí.
- Široký tím certifikovaných etických hackerov so skúsenosťami z niekoľkých desiatok vykonaných penetračných testov ročne.
- Sme držiteľmi certifikácií eMAPT, CISSP, OSCP, OSCE, CEH a celého radu ďalších.
- Prevádzkujeme vlastné hackerské laboratórium na výskum aj v oblasti rôznych druhov bezdrôtových sietí.
- Načúvame klientom a prispôsobujeme testy ich potrebám a časovým možnostiam.
- Sledujeme moderné trendy v oblasti bezpečnosti bezdrôtových sietí.
- Pri testovaní kladieme dôraz na manuálny prístup, ktorý vedie k odhaleniu väčšieho množstva chýb a minimalizácii false-positive nálezov.

Bratislava – AEC s. r. o., Prievozská 6, 821 09 Bratislava, tel.: +421 254 410 283
Praha – AEC a.s., Voctářova 20a, 180 00 Praha 8, tel: +420 226 229 133
Brno – AEC a.s., Veveří 102, 616 00 Brno, tel: +420 541 235 466