DNS Professional services

Penetrační testování interní a externí infrastruktury

Penetrační testování interní a externí infrastruktury metodikou OSSTMM, PTEST, NIST.

Rozsah této služby lze rozdělit na testování Interní a Externí infrastruktury a dále lze zvolit hloubku testování a vybrat pouze Základní anebo Pokročilé testování. Případně lze upravit rozsah dle individuálních potřeb konkrétního prostředí a klienta.

Služba obsahuje:

- Projektový management – činnosti zahrnuté ve všech službách včetně doplňkových služeb
    - zahájení, plánování, provádění a ukončení projektu, včetně koordinace zdrojů dodávek a komunikace se zúčastněnými stranami
- Předinstalační služby a příprava:
    - konzultace a získání informací o stávajícím stavu infrastruktury
    - konzultace přínosu penetračního testování
    - definice rozsahu a omezení (testování během dne/mimo pracovní dobu, kritické stroje, které se nesmí testovat, komunikační matice, způsob realizace – fyzicky, skrze VPN, apod.)
- Základní testování interní infrastruktury:
    - testování formou black-box, grey-box či white-box
    - identifikace a sběr informací o síťových zařízení, informačních systémů
    - a provozovaných služeb
    - automatizované bezpečností testy neinvazivního charakteru
    - enumerace zranitelností a slabin v infrastruktuře (následná exploitace)
    - odposlech síťové komunikace v rámci LAN sítě
    - využití veřejně dostupných nástrojů
    - Prezentace a report obsahující manažerské shrnutí, popis zranitelností a doporučená nápravná opatření
- Pokročilé testování interní infrastruktury:
    - testování formou black-box, grey-box či white-box
    - identifikace a sběr informací o síťových zařízení, informačních systémů
    - a provozovaných služeb
    - automatizované bezpečností testy neinvazivního charakteru
    - enumerace zranitelností a slabin v infrastruktuře (následná exploitace)
    - manuální hledání zranitelností a jejích následná exploitace
    - exfiltrace dat, hledání citlivých informací na serverech a zařízení
    - pivoting, eskalace práv na prolomených systémech
    - síťové útoky typu MITM, ARP poisoning, DHCP spoofing či DOS na konkrétní servery

- crackování hesel s pomocí na míru vygenerovaných slovníků
- využití veřejně dostupných, komerčních a vlastních nástrojů
- Prezentace a report obsahující manažerské shrnutí, popis zranitelností a doporučená nápravná opatření

- Základní testování externí infrastruktury:
  - testování formou black-box, grey-box či white-box
  - identifikace a sběr informací o síťových zařízení, informačních systémů
  - a provozovaných služeb
  - enumerace domén a subdomén, ověření DNS záznamů
  - automatizované bezpečností testy neinvazivního charakteru
  - využití veřejně dostupných nástrojů
  - Prezentace a report obsahující manažerské shrnutí, popis zranitelností a doporučená nápravná opatření

- Pokročilé testování externí infrastruktury:
  - testování formou black-box, grey-box či white-box
  - identifikace a sběr informací o síťových zařízení, informačních systémů
  - a provozovaných služeb
  - enumerace domén a subdomén, certifikátů, ověření DNS záznamů
  - zjištění informací na základě veřejně dostupných zdrojů
  - hledání uniklých účtů na darkwebu a ověření jejich aktuálnosti
  - automatizované bezpečností testy neinvazivního charakteru
  - manuální hledání zranitelností a jejích následná exploitace
  - využití veřejně dostupných, komerčních a vlastních nástrojů
  - Prezentace a report obsahující manažerské shrnutí, popis zranitelností a doporučená nápravná opatření

Doplňkové služby (volitelné):

- 4h. Engineer time – navazující na místě/vzdálená práce na činnostech související s touto implementací, které nejsou součástí této služby anebo doplňkových služeb

Pro úspěšnou instalaci a implementaci je nutná spolupráce a příprava na straně příjemce služby! Během zahájení služby může být příjemce služby požádán např. o zajištění IP rozsahů, DNS záznamů, vzdáleného přístupu pro konfiguraci, fyzický přístup k racku vč.manipulačního prostoru, vhodného racku pro instalaci hardware, dostatečného počtu napájecích zásuvek a kapacity UPS, připravených kompatibilních uplink portů do LAN/Management sítě apod. Rozsah zajištění připravenosti může být upřesněn během zahájení projektu.

V případě nepřipravenosti nebo nezajištění podmínek pro úspěšné zahájení a doručení části nebo celé služby, nemůže být garantováno dokončení této služby, včetně domluveného harmonogramu. Dojde-li v tomto důsledku k prodloužení času stráveného na místě instalace, může být dodatečně fakturován čas strávený nad rámec této služby v rozsahu min.4hod. a max.8hod. Engineer time a to i opakovaně při dalších pokusech o doručení služby.

Služba je doručována konzultantem s odpovídající certifikací výrobce anebo 5+ let zkušenostmi v dané oblasti. Služba je doručována vzdáleně (kromě instalace hardware), v pracovní dny, v čase od 8 do 17hod.

Služba je platná v rámci České republiky.