Házi Feladat 2. útmutató a

“Hálózatbiztonság” című tárgyhoz

2018-

A házi feladatot kidolgozta:

Bencsáth Boldizsár, Holczer Tamás, Ládi Gergely, Gazdag András

BME, CrySys Adat- és Rendszerbiztonsági Laboratórium

A 2. Házi feladat az órán tanult egyes technikák gyakorlati alkalmazását célozza meg.

Feladatok

- A hallgatónak saját infrastruktúrájában vagy az egyetem által biztosított környezetben telepítenie kell egy virtuális számítógépet linux operációs rendszerrel, javasoltan Debian vagy Ubuntu változatta
- A felhasználó kiválthatja ezt tetszőleges operációs rendszerrel és nem kötelező a virtualizáció használata sem, de javasoljuk a fenti beállításokat
- A telepített számítógépen be kell állítania egy OpenVPN klienst és becsatlakoztatni a házi feladat szervere felé. Ezzel a lépéssel akarjuk elérni, hogy minden végzett hallgatónak legalább egyszer legyen tapasztalata VPN beállításával, illetve ez megoldja a NAT problémáját is, a hallgató gépe és a szerver biztosan tud kommunikálni egymással.
- A második feladata a hallgatónak a saját gépén egy DNS szerver megfelelő beállítása. A beállítási paramétereket külön jelöljük
- A következő lépésben a hallgató saját „szerverén” SMTP levelezőprogramot kell beállítania megfelelően, és a szervernek képesnek kell levelet küldenie a teszt szerverünk felé.
- Levél küldésével tudja beindítani a hallgatónak a tesztet, a kiküldés megfelelősége esetén a házi feladat szerver ellenőrzi a DNS megfelelő működését és visszaigazolást ad a hallgatónak
- A hallgató feladata a házi feladat során létrehozott konfigurációk, kódok megosztása és a házi feladat elvégzésének mérés labor jellegű módon történő dokumentációja, majd annak beküldése

VPN beállítása

A VPN beállításához kliens oldali tanúsítványra van szükség, ezzel kell becsatlakozni a szerverre. Ehhez három egyedi fájlra lesz szüksége a hallgatónak: Kliens oldali tanúsítvány (cert fájl), Kliens oldali titkos kulcs (key fájl), a CA tanúsítványa a szerver ellenőrzésére (cacert fájl). Ezeket a hallgató a regisztrációs felületen történő jelentkezéssel tudja megszerezni.

Ennek helye: http://152.66.249.144:8010/

Név: neptun kód jelszó: crysys

A többi beállítás általános, minden hallgatóra azonos. A rejtjelező és hash algoritmus alapértelmezett, a szerver fog IP címet osztani a kliensnek egy /30-as tartományból, továbbá egy /24 címtartományra vonatkozó routing üzenetet is fog küldeni a kliens (hallgató) felé. A /24-es hálózatban lesz elérhető a szerver a további feladatok számára.

Pontosabb adatok: 10.105.24.0/24 –ben osztott címet kapsz, egy /30-as hálóra, amiben az egyik cím a tied a másik a szerveré. Nem konstans cím, újracsatlakozákor változhat.

Kapsz egy push route-ot a 10.105.25.0/24 tartományra, amiben a 10.105.25.1 a levelező szerver ami pingelhető is.

Nincs LZO tömörítés. UDP 1194 –es standard porton érhető el a szerver 152.66.249.144.

DNS beállítása

A hallgató feladata egy DNS szerver beállítása saját gépén, amely elérhető a standard 53-as porton át. A DNS szervernek kizárólag a crysys.hu domaint kell tudnia kiszolgálnia, de azt authorativ DNS szerverként. Másodlagos DNS szervert nem kell konfigurálni.

A DNS szervernek a neptunkod.crysys.hu rekordjában a hallgató NEPTUN azonosítóját kell TXT rekordként kiszolgálni, ezt a jegyzőkönyvben pl. dig paranccsal ellenőrizve be is kell mutatni.

A DNS szervernek definiálnia kell a mail.crysys.hu rekordot.

A mail.crysys.hu a /24-es tartományban levő következő címre kell mutatnia: 10.105.25.1

A DNS szervernek tartalmaznia kell **DMARC rekordot** (dmarc@crysys.hu-ra irányítva, tetszőleges logikus beállításokkal)

A DNS szervernek tartalmaznia kell **DKIM kulcsot**.

A DNS szervernek tartalmaznia kell **SPF rekordot**, a crysys.hu vonatkozásában kizárólag a fenti, mail.crysys.hu szerver küldhet ki levelet (bármilyen módon beállítható, IP, név, MX).

A DNS szervernek **DNSSec** segítségével aláírva kell működnie. Természetesen a domainre nem lesz DS rekord, tehát úgymond „önaláírt” DNSSec megoldást várunk el.

A levelező szerver beállítása

Tetszőleges levelező kiszolgáló használható, de javasolt az exim4 daemon heavy használata. A levelező szerver tetszőleges forrás domainbe kerülhet, a házi feladat szerver bármilyen ip címről, bármilyen reverse DNS-sel, bármilyen domainről elfogad leveleket.

Fontos, hogy a crysys.hu –ra küldendő leveleket a fent jelölt mail.crysys.hu teszt szerverre kell irányítani.

A szervernek **DKIM aláírást** kell raknia a levélre és **TLS kapcsolatot** is tudnia kell felépíteni a teszt szerver felé. Az aláírás kulcsparaméterei, szöveges paraméterei lényegtelenek, csak be legyenek állítva logikusan.

Amikor minden beállítás megfelelő, a hallgató küldjön levelet automatikusan vagy programmal az SMTP szerverén keresztül a teszt@crysys.hu címre.

Ebben a szöveg törzsében az alábbi üzenet szerepeljen:

Neptun: XXXXXX

ahol az X-ek helyére a hallgató neptun kódja kerüljön.

A szerver a levél feldolgozásával ellenőrzéseket fog beindítani, így kérjük, hogy a szerver még 10 percig minden beállítással üzemeljen.

Amennyiben időben és megfelelően ki tudjuk dolgozni a HF teszt oldali részét, úgy az automatikus teszt eredményéről a hallgató neptun kód szerinti email címére automatikus visszaigazolás fog érkezni.

Mint minden házi feladat, a kidolgozásakor ez is instabil lehet. Ha gond lenne, kérjük a hallgatót konzultájon a labor tagjaival, de egyeztethet diáktársaival is! Az előadás slide-jain részletes tanácsok voltak egyes megoldások konfigurálásához.

A telepített komponensek működésének ellenőrzésekor javasolt wireshark/tshark/tcpdump használata, ennek outputja a dokumentációba csatolható inline és csatolmány módon is.

Tiltott tevékenységek

Különösebben tiltott tevékenység nincsen, lehet tesztelni a szervert nmap-pal, lehet többször bekapcsolódni, és sok levelet küldeni (pár tucat). Természetesen automata támadásokat, DoS helyzetet, más hallgató akadályozását kérjük kerüljétek, és ha kész a házi feladat, kérjük a VPN-t ne használjátok tovább, saját biztonságunk és a használhatóság okán is.

Támogató dokumentumok

A szerverprogramok beállításához a megfelelő programok elérhető online dokumentációját javasolt használni.