HADMÉRNÖK
VÉDELMI INFORMATIKA

15. évfolyam (2020) 1. szám 159–182.
DOI: 10.32567/hm.2020.1.11

Paráda István,[1] Farkas Tibor[2]

Felderítés és analízis a penetrációs tesztben – 1. Információgyűjtési technikák

Reconnaissance and Analysis in the Penetration Test 1 Information Gathering Techniques

Jelen cikksorozat a penetrációs tesztek szakaszán belül a felderítés és analízis szintjeinek bemutatásával foglalkozik. Az egyik alapvető szemlélet szerint a kiberműveletekben és informatikában vett penetrációs tesztek felderítési és analízisszintjén lévő információgyűjtési tevékenységek azonosítják (kockázati szinten) a szervezetekhez kapcsolódó, nyilvánosság számára hozzáférhető információkat. Az információgyűjtés a penetrációsteszt-végrehajtás lépésének első szakasza, amely a célhálózatról és célkörnyezetről való információk begyűjtését takarja. Az információgyűjtési technikákat használva számos lehetőség nyílik a célszervezet hálózatának illetéktelen hozzáférésére. Ennek segítségével létrehozható egy biztonsági profil a célszervezet hálózatáról, rendszeréről és részben magáról a szervezetről is. Nincs egységes módszer az információgyűjtésre, hiszen azok számos módon beszerezhetők. Viszont a lehető legtöbb információt be kell gyűjteni, így érdemes ezt a fázist szervezett módon végrehajtani [1].

Kulcsszavak: **információgyűjtés, keresőmotorok, DNS, WhoIs**

This series of articles deals with the detection and analysis levels within the penetration tests section. One basic approach is that information gathering activities at the detection and analysis level of penetration tests in cybersecurity and information technology (at risk level) identify publicly available information related to organisations. Gathering information is the first step in the penetration test implementation process, which involves gathering information about the

[1] Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola, doktorandusz, e-mail: paradaistvan@gmail.com, ORCID: https://orcid.org/0000-0002-3083-6015

[2] Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar, egyetemi docens, e-mail: farkas.tibor@uni-nke.hu, ORCID: https://orcid.org/0000-0002-8868-9628

target network and target environment. Using information gathering techniques, there are many opportunities for unauthorised access to the target organisation's network. This allows you to create a security profile of the target organisation's network system, and partly the organisation itself. There is no standard way to collect information, as there are many ways to obtain it. However, as much information as possible must be collected, therefore, it is worthwhile to carry out this phase in an organised manner.

Keywords: **information gathering, search engines, DNS, Whois**

Bevezetés

Az információgyűjtés a penetrációsteszt-végrehajtás lépésének első szakasza, amely a célhálózatról és célkörnyezetről való nyilvános információk begyűjtését takarja, informatikai és informatikához kapcsolódó technikákon, módszereken keresztül. Az információgyűjtés e cikkben taglalt része magában foglalja a kibertéri műveletek közül az elektronikai felderítés OSINT[3]-fajtáját, amely a széles körben hozzáférhető, nyílt adatforrások felhasználásával gyűjt adatokat, illetve a számítógéphálózati műveletek felderítés fajtáját. „A számítógép-hálózati felderítés a hálózatok struktúrájának feltérképezését, az adatbázisokhoz való illetéktelen hozzáférést és a támadható pontok meghatározását jelenti. Megvalósulhat a szemben álló fél számítógépes rendszereibe való szoftveres vagy hardveres úton való behatolással. Célja az adatbázisokban tárolt adatokhoz, információkhoz való hozzáférés és azok felderítési céllal való hasznosítása, illetve a későbbi károkozással járó támadás kivitelezéséhez a hálózat támadható pontjainak és a támadás leghatékonyabb formáinak meghatározása. A felderítés az elszenvedő hálózat részéről általában nem észlelhető formában valósul meg, így a hálózat üzemeltetője és felhasználója számára a felderítés ténye többnyire nem ismert" [2].

A cikk egy lehetséges penetrációsteszt-módszertan felderítés és analízis első szintjének bemutatásával foglalkozik, ahol még nem feltétlenül a technikai megvalósításokon van a hangsúly, sokkal inkább a kibertér hatásáról a társadalomra, cégekre, nemzetekre. Ezeknek a hatásoknak és magának az információs társadalomnak a következményeként írhatunk olyan technikákat, olyan eljárásokat, amelyek magukban foglalják a penetrációs teszt módszertanának információgyűjtési egységét.

[3] Az OSINT (Open Source Intelligence) a nyílt forrású hírszerzés nemzetközileg is elfogadott angol nyelvű rövidítése. Az OSINT fő forrásait a NATO OSINT kézikönyve a következők szerint határozza meg:
nyomtatott és elektronikus média;
internet, beleértve a láthatatlan web információit;
kereskedelmi (fizetős) online szolgáltatók tanulmányai, adattárai;
„szürke irodalom", azaz nem publikált, de nem is minősített, szűk körben hozzáférhető, nyomtatott és digitális dokumentumok, tanulmányok;
személyes tapasztalatok;
kereskedelmi műholdak felvételei. Ezek pontossága a 21. században gyakran megközelíti a katonai műholdak teljesítményét;
tudományos kutatószervezetek, egyetemek.

Felderítés- és analízisszintek:

- Információgyűjtés;
  - A közzétett adatok elemzése;
    - információgyűjtés keresőmotorok segítségével,
    - információgyűjtés webszolgáltatásokon keresztül,
    - weboldal-információgyűjtés,
    - e-mail-információgyűjtés.
  - Alapvető hálózati információk lekérdezése;
    - WhoIs,
    - DNS-információk kibontása.
- Hálózat-feltérképezés;
  - célpontfelfedés,
  - Port Scan,
  - OS-ujjlenyomat,
  - hálózatiforgalom-elkapás, lehallgatás.
- Sérülékenység elemzése és értékelése.

Ahhoz, hogy a cikkben kontextusba tudjuk helyezni a bemutatni kívánt információgyűjtési metódusokat, gyakorlatokat és felkínált végrehajtási lehetőségeket, definiálni kell magát a tevékenység hatókörét, ami nem más, mint a kibertér. „Kibertér: felhasználók, eszközök, szoftverek, folyamatok, tárolt vagy átvitel alatt lévő információk, szolgáltatások és rendszerek gyűjtőfogalma, amelyek közvetlenül vagy közvetett módon számítógép-hálózathoz vannak kapcsolva” [3]. Ebből kiderül, hogy mivel sokféle elemet érintő, dinamikusan változó tartományról beszélünk, a benne végrehajtható információgyűjtés is több síkon értelmezhető. Például nyilvános adatok összegyűjtésének emberközpontú, emberi kapcsolati nézőpontjából vizsgálva vagy szervezeti, illetve intézményi szempontok alapján, valamint ezek technikai oldalú megközelítésén keresztül.

A közzétett adatok elemzése

A kiberműveletek képességein belül a számítógép-hálózatokba való bejutást, azok felderítését, az adatbázisokhoz való hozzáférést, azok módosítását, tönkretételét, a távközlési hálózatok lehallgatását a közzétett adatok elemzésével érdemes kezdeni.

Az információgyűjtés-módszertan egy eljárás a célszervezettel kapcsolatos információk gyűjtésére az összes kibertérben rendelkezésre álló forrásból. A közétett adatok elemzése megmutatja a célszervezettel kapcsolatos információkat, mint például az URL[4] helyét, a telephely adatait, az alkalmazottak számát, a domainnevek konkrét tartományát, elérhetőségi adatait és egyéb kapcsolódó információkat. Itt nem feltétlenül technikai információk begyűjtése a cél, inkább a keresési mechanizmus legjobb hatásfokkal való alkalmazása [4].

[4] Az URL (*Uniform Resource Locator* [egységes erőforráshely] rövidítése), az interneten megtalálható bizonyos erőforrások szabványosított címe.

Információgyűjtés keresőmotorok segítségével

Az internetes keresőmotorok a fő források a célszervezettel kapcsolatos kulcsinformációk megkereséséhez. A keresőmotorok kinyerhetik a célokról szóló információkat, beleértve például technológiai platformokat, alkalmazottak adatait, bejelentkezési oldalakat, intranetportálokat, elérhetőségeket és így tovább. Ezért fontos szerepet töltenek be a kritikus részletek felderítése terén, hiszen ezek a viszonylag egyszerűen kinyert információk képezhetik az alapját vagy előkészületét egy támadás indításának, egyfajta információs adatbázist képezhetnek, amelyből szükség esetén már összegyűjtve és nagyobb támadáshoz rendszerezve, előkészítve lehet meríteni a támadások támogatásához. Ez az információ segíti a támadót a social engineering[5] és más típusú támadások végrehajtásában. A keresési eredmények böngészései gyakran értékes információkat nyújtanak például a fizikai helyről, elérhetőségekről, a szolgáltatásokról, az alkalmazottak számáról és így tovább.

A támadók az ezekkel a keresőmotorokkal elérhető speciális keresési operátorokat használhatják, és létrehozhatnak kötelező lekérdezéseket a célhoz kapcsolódó információk keresésére, szűrésére és rendezésére. A keresőmotorokat más, a nyilvánosság számára hozzáférhető információforrások forrásainak keresésére is használják. Például beírható a „Legjobb munkaportálok" elem, olyan főbb munkaportálok kereséséhez, amelyek kritikus információkat nyújtanak a célszervezetről. A Google[6] hackelés mint kifejezés, a fejlett Google keresési operátorok használatára utal, hogy összetett keresési lekérdezéseket hozzon létre az érzékeny vagy rejtett információk kinyerésére. Ezután a támadók a hozzáférhető információkat a sebezhető célok felkutatására használják. Az információgyűjtés fejlett Google-hackelési[7] [9] technikákkal történő összegyűjtésével a Google a keresési eredmények speciális szövegrészeit egy speciális operátor és a Google keresőmotorja segítségével hajtja végre. Google-operátorok segítenek megtalálni a szükséges szöveget és elkerülni az irreleváns adatokat, azaz segítenek a keresési lekérdezés szűkítése és a legrelevánsabb és pontosabb output elérésében.

[5] A social engineering amikor egy jogosultsággal rendelkező felhasználó jogosulatlan személy számára bizalmas adatokat ad át, vagy lehetőséget biztosít a rendszerbe történő belépésre a másik személy megtévesztő viselkedése miatt.

[6] A Google LLC egy részvénytársaság, aminek a nevéhez fűződik a Google keresőmotor kifejlesztése és üzemeltetése.

[7] A Google Dorking egy nagyon egyszerű módszer annak ellenőrzésére, hogy vannak-e biztonsági rések az adott hálózaton vagy számítógépen. A meghatározás szerint a Google dork lekérdezés egy olyan string típusú keresés, amely fejlett keresési operátorokat használ olyan információk megkeresésére, amelyek nem érhetők el könnyedén a weboldalon. Ebbe a körbe olyan információk tartoznak, amelyeket nem a nyilvánosság számára szántak, de nincsenek megfelelően levédve. Passzív támadási módszer esetén a Google dorking segítségével a következő adatokat lehet megszerezni: felhasználónevek és jelszavak, e-mail-listák, érzékeny dokumentumok, gazdasági információk (PIFI) és az adott weboldal sebezhetőségei. Az egész legális.

1. táblázat

Főbb operátorok [5]

Egyszerű operátorok	Haladó operátorok
Filetype: • Csak a megadott kiterjesztésű (például PPT, pdf) fájlokat adja vissza a Google.	Allintext/intext: • Az allintext kifejezést a keresés elején kell használni. Csak olyan oldalakat fog visszaadni a Google, ahol a szövegben minden szó szerepel, ami az allintext után van írva.
Site: • Csak a megadott domainen belül fog keresni és találatokat adni. A „site" operátort ki lehet egészíteni kifejezésekkel is, és akkor csak az adott oldalon belül fog keresni a megadott kifejezésekre.	Intitle /allintitle: • Működése teljesen hasonló az intext/allintext pároshoz, annyi a különbség, hogy itt a keresés a címben történik.
Related: • Ennek az operátornak a segítségével meg lehet találni egy adott oldalhoz hasonló oldalakat. Fontos megjegyezni, hogy csak domainekkel és URL-ekkel működik, keresőszavakkal nem. Illetve, ha a kettőspont után szóköz kerül, akkor csak egy sima keresés lesz. Ez főleg angol nyelvű oldalak esetében működik jól.	Inurl/allinurl: • Az előző kettőhöz hasonlít ezeknek az operátoroknak is a működése, viszont itt a keresés az URL-ben történik.
Cache: • Ennek az operátornak a segítségével meg lehet nézni egy adott oldalnak a Google által utoljára eltárolt (cache-elt) változatát. Hasznos lehet olyan oldalak esetében, amelyeket már esetleg valamilyen okból töröltek.	Inanchor/allinanchor • Ennek a párosnak az esetében pedig a keresés a horgonyszövegekben történik.
Define: • A keresett kifejezésnek a definícióját dobja ki a Google. Csak angol kifejezések esetében működik.	
Location: • Akkor érdemes ezt az operátort használni, hogyha egy adott földrajzi helyre szűkítve történik a keresés.	

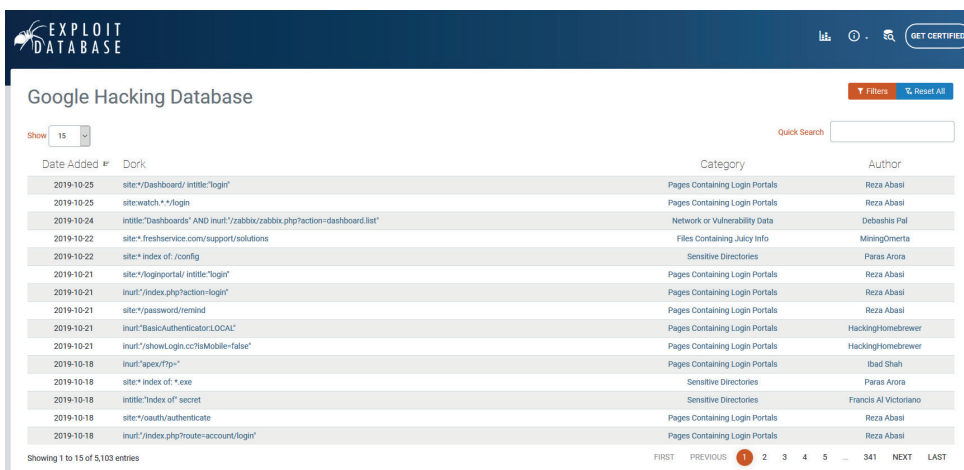
A támadó egyszerűen nem tud specifikus, részletes, mélyreható esetleg műszaki információt gyűjteni az információs oldalról, csak egy normál keresőmező segítségével, hiszen az rengeteg irreleváns információt is tartalmazna, amely nem teszi lehetővé a további hatékony feladatvégrehajtást. A bonyolult keresés számos egymással összefüggő feltételt érint. A Google speciális keresési funkciója segít a támadónak összetett internetes keresést végrehajtani. A Google Advanced Search és az AdvancedImage Search segítségével az interneten sokkal pontosabban lehet keresni. Ezeket a keresési funkciókat ugyanazon pontosság eléréséhez használhatja, ha fejlettebb operátorokat használ, de gépelés vagy emlékezet nélkül (1. táblázat).

A Google Hack-módszerek segítségével, egy esetleges támadó [3: 169–187.] összetett keresőmotor-lekérdezéseket hozhat létre a keresési eredmények nagy

mennyiségének szűrése érdekében. A támadók a Google-operátorokat használják, amelyek segítenek megtalálni az ilyen konkrét szövegsorokat a keresési eredmények között. Tehát egy támadó felfedezheti a kizsákmányolásra felhasználható webhelyeket és webes felhasználókat, valamint hozzárendeli őket a személyes, érzékeny információikhoz, például hitelkártyaszámok, szociális biztonsági számok, jelszavak és így tovább. Ha a kiszolgáltatott célt azonosítják, a támadók különféle lehetséges támadásokat próbálnak indítani, mint például puffer-túlcsordulások[8] és többek között SQL Injection.[9]

Ahogy az 1. ábra is mutatja, számos példa létezik a nyilvános kiszolgálókra hagyott érzékeny információkra, amelyeket a támadó a Google Hacking Database (GHOB) lekérdezéseivel kivonhat:

- érzékeny információkat tartalmazó hibaüzenetek;
- jelszavakat tartalmazó fájlok;
- érzékeny könyvtárak;
- a bejelentkezési portálokat tartalmazó oldalak;
- hálózati vagy sebezhetőségi adatokat tartalmazó oldalak;
- szerversérülékenységek;
- a szoftver verziószáma;
- webes alkalmazás forráskód.



1. ábra

Google hacking database [6], [10]

A keresőmotoros információgyűjtés napjaink egyik legalapvetőbb információbeszerzési módszere. Az internet széles körű elterjedése és globális tulajdonsága miatt

[8] A puffertúlcsordulás (buffer overflow) olyan szoftverhiba, sokszor biztonsági rés, amelynél egy processz a fix hosszúságú tömbbe (puffer) történő íráskor nem ellenőrzi annak határait, így azt túlírva a szomszédos memóriaterületet írja felül.

[9] Az SQL-injection egy olyan támadás, amivel sérülékeny SQL-szerverekből lehet kibányászni hasznos információkat, például felhasználóneveket, jelszavakat, jelszó-hasheket.

a legkönnyebben és legegyszerűbben használható információforrás. A rajta lévő keresőmotoroknak információszerzésre való kifinomult, részletes és tudatos használata a penetrációs teszt feladatvégrehajtásában jelentős könnyítéseket, előkészületi fázisokat, annak a már-már készségszinten való használatát teszi lehetővé. A keresőmotorok megfelelő hatásfokkal való használata keresési időt, erőforrást takaríthat meg, valamint leszűrheti a lényegtelen, nem releváns információkat. Ezek a felesleges többletinformációk hátráltatást jelentenek egy munkafolyamat során. Egy kiberműveleti penetrációs teszt munkafolyamatának szemszögéből az effektív munkavégzést segíti.

Információgyűjtés webszolgáltatásokon keresztül

Az olyan webszolgáltatások, mint például a személyes keresési szolgáltatások érzékeny információkat szolgáltathatnak a célról. Az internetes archívumok bizalmas információkat is tartalmazhatnak, amelyeket eltávolítottak az internetről. Közösségi hálózati oldalak, a riasztások, pénzügyi szolgáltatások és munkahelyek biztosítanak információt egy célról, például az infrastruktúráról, fizikai helyről és az alkalmazottak adatairól. Sőt, a csoportok, fórumok és szervezetek segítenek a támadóknak érzékeny információk gyűjtésében, olyan célokról, mint például a nyilvános hálózati információk, rendszerinformációk és személyes adatok. Ezen információk felhasználásával a támadó penetrációs stratégiát készíthet, hogy betörjön a célszervezet hálózatába, és egyéb típusú fejlett rendszeri támadásokat hajtson végre.

A célpont legfelső szintű domainjei és aldomainjei

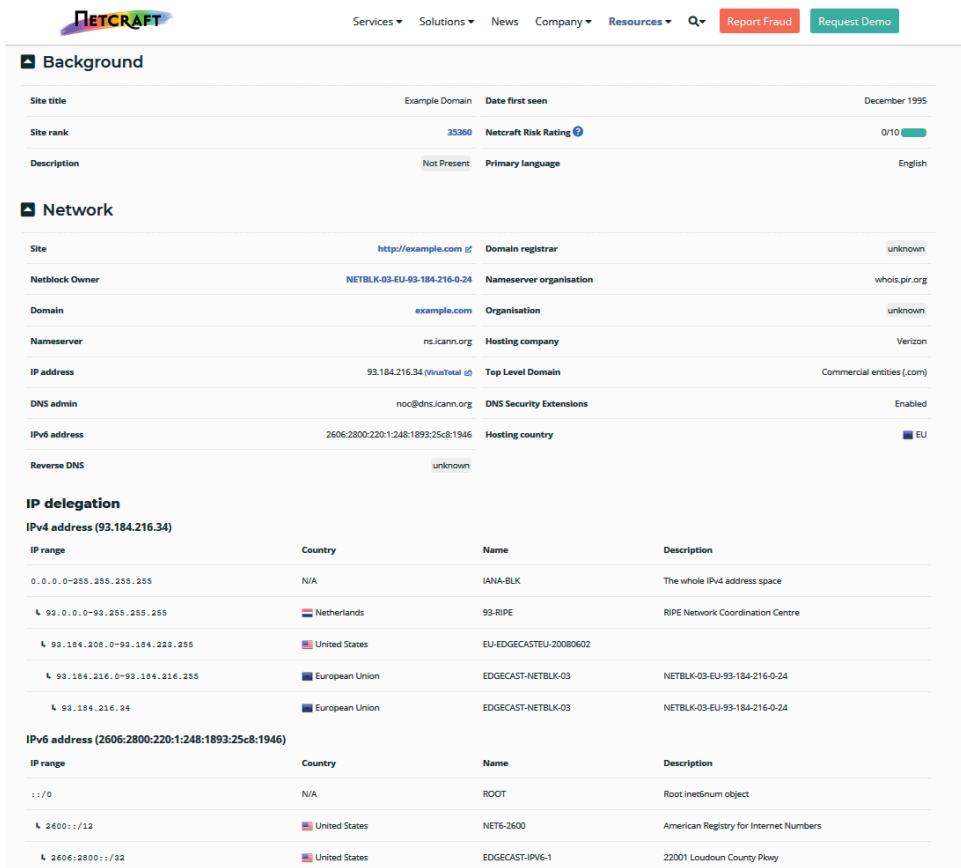
A vállalati felső domain és aldomainek sok hasznos információt nyújthatnak a támadó számára. A nyilvános webhelyeket arra tervezték, hogy megmutassák egy szervezet jelenlétét az interneten. Ingyenesen elérhetők és bárki el is érheti azokat, az ügyfelek és partnerek vonzására szolgálnak. Tartalmazhatnak olyan információkat, mint például a szervezeti előzmények, szolgáltatások és termékek, valamint elérhetőségi adatok. A cél külső URL-je megtalálható a keresőmotorok, például a Google vagy a Bing segítségével.

Az aldomainek csak néhány ember számára elérhetők. Ezek a személyek lehetnek foglalkoztatottak vagy egy osztály tagjai valamely szervezetnél. Az altartományok betekintést nyújtanak a célvállalat különböző szervezeti és üzleti egységeibe. A hozzáférési korlátozások a következők alapján alkalmazhatók: az IP-cím, domainalhálózat, felhasználónév és jelszó. A legtöbb szervezet általános formátumokat használ az altartományokhoz.

- Netcraft.com
  A Netcraft internetes biztonsági szolgáltatásokat nyújt, ideértve a csalás és az adathalászok, az alkalmazások tesztelését és a PCI-scanning[10] szolgál-

[10] A PCI-vizsgálat általában a negyedéves külső sebezhetőségi vizsgálatokra vonatkozik, amelyeket a PCI-jóváhagyott gyártónak kell elvégeznie. A PCI (Payment Card Industry) adatbiztonsági szabványa a Visa és a MasterCard közötti együttműködés eredményeként jött létre, hogy közös ipari biztonsági követelményeket hozzon létre.

tatásait is (2. ábra). Elemzi továbbá a webszerverek, az operációs rendszerek, a host-szolgáltatók és az SSL-tanúsító[11] hatóságok piaci részesedését és az internet egyéb paramétereit.

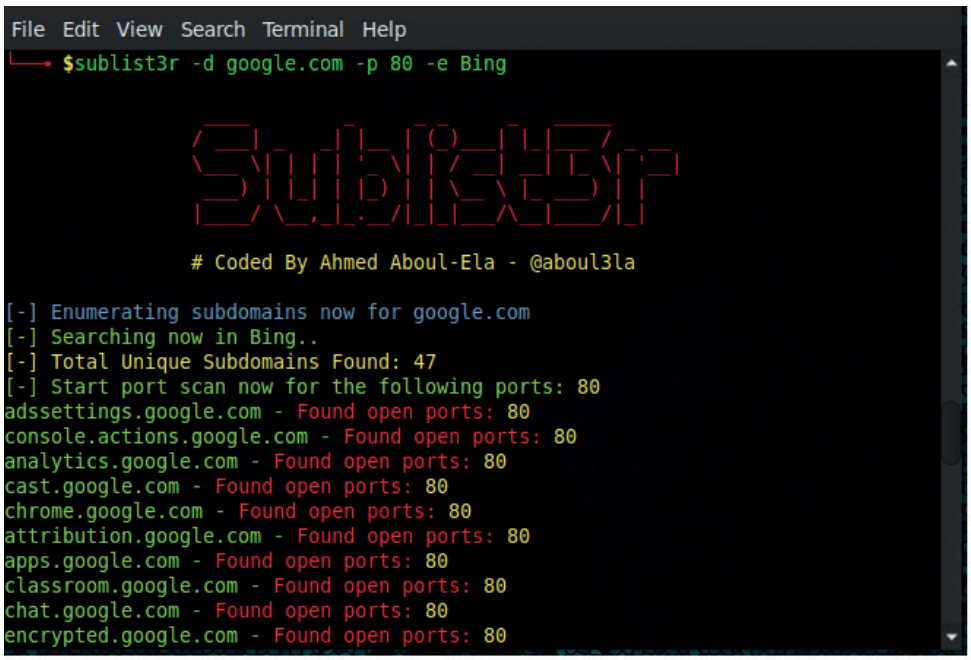


2. ábra
Netcraft az Example.com példán keresztül [7], [11]

- Sublist3er
  A Sublist3r egy python szkript, amely az OSINT használatával a webhelyek aldomaineinek felsorolására szolgál (3. ábra). Ez lehetővé teszi az aldomainek

[11] Az SSL tanúsítványok arra szolgálnak, hogy létrejöhessen egy biztonságos, titkosított csatorna a kliens és a szerver között. Bizonyos információknak, mint a hitelkártyaadatok, fiókbelépéshez szükséges adatok és egyéb kényes információk átvitelének titkosítás alatt kell történnie, hogy kizárjuk az adatok kiszivárgását.
SSL tanúsítvánnyal adataink titkosításon esnek át, mielőtt azok interneten keresztül átvitelre kerülnének. A titkosított adatot csak a célszerver képes lefordítani. Ez biztosítja, hogy a weboldalon megadott adatainkat nem tulajdoníthatják el.

felsorolását több forrásból egyszerre. Segít a penetrációs tesztelőknek és a hibakeresőknek a megcélzott domain domainjeinek összegyűjtésében.



3. ábra
Sublist3r google.com példán keresztül [8]

A cél földrajzi helyzetének megkeresése

Az olyan információk, mint például a szervezet fizikai elhelyezkedése alapvető szerepet játszanak az információgyűjtés folyamatában. A fizikai elhelyezés mellett a támadók olyan információkat is gyűjthetnek, mint például a közeli nyilvános WiFi, amely valószínűleg egy módja annak, hogy elérjék a célszervezet hálózatát. A támadók, akik tudják a célszerv helyét, megkísérlik a szemétbúvárkodást, megfigyelést, social engineering-et, és egyéb nem technikai támadásokat további információk gyűjtése érdekében. Amint a támadók ismerik a cél elhelyezését, részletes műholdas képeket kaphatnak a helyről, az interneten elérhető különböző források, például a Google Maps[12] felhasználásával. A támadók ezt az információt felhasználhatják jogosulatlan hozzáféréshez az épületekhez, vezetékes és vezeték nélküli hálózatokhoz, rendszerekhez.

A Google Earth eszköz lehetővé teszi, hogy megtalálja a cél pontos lokációját, még hozzáférést is biztosít 30 képhez, amely a lakott Föld felületének nagy részét nagy felbontással és részletességgel ábrázolja. A részlet lehetővé teszi az utcakép,

[12] A Google által fejlesztett ingyenes internetes térképszolgáltatás.

a magasság és a koordináták megtekintését. Az olyan eszközök, mint a Google Maps, még az épület bejáratait, a biztonsági kamerákat és a kapukat is megtalálják. Ezek az eszközök interaktív térképeket, vázlatos térképeket, műholdas képeket és információkat nyújtanak a saját térképekkel való interakcióról és azok létrehozásáról. Példák webszolgáltatásra, amely alkalmas a cél földrajzi helyzetének megkeresésére

- https://earth.google.com;
- Wikimapia.org;
- www.bing.com/maps.

Információgyűjtés közösségi oldalakon keresztül

Egy adott személyre való keresés a közösségi oldalakon könnyebb, mint ahogy a legtöbb ember gondolná. Közösségi hálózati hálózatok: olyan online szolgáltatások, platformok vagy webhelyek, amelyek a társadalmi hálózatok kiépítésére vagy az emberek közötti társadalmi kapcsolatok elősegítésére koncentrálnak. Ezek a webhelyek olyan információkat tartalmaznak, amelyeket a felhasználók profiljukban nyújtanak. Segítik az emberek közvetlen vagy közvetett kapcsolatát egymással, olyan különböző területeken keresztül, mint a közös érdekek, a munkahely és az oktatási közösségek. A közösségi oldalak olyan online szolgáltatások, platformok vagy egyéb webhelyek, amelyek lehetővé teszik az emberek számára, hogy kapcsolatba lépjenek egymással és személyes kapcsolatokat építsenek ki. Az ilyen webhelyek például a LinkedIn, a Facebook, a Twitter, a Google, az Instagram stb. A közösségi oldalak lehetővé teszik az emberek számára az információk gyors megosztását, mivel valós időben frissíthetik személyes adataikat. Minden közösségi hálózati webhelynek megvan a maga célja és funkciója. Az egyik oldal kapcsolatba hozhatja a barátokat, ismerősöket, míg a másik segít a felhasználóknak megosztani a munkahelyi profilokat. A közösségi oldalak mindenki számára nyitva állnak. A támadók kihasználhatják ezt a lehetőséget, hogy érzékeny információkat gyűjtsenek a felhasználóktól, akár a felhasználók böngészésével, akár hamis profil készítésével.

Egyes webhelyek lehetővé teszik a felhasználók számára, hogy ellenőrizzék, aktív-e egy fiók, amely ezután információt nyújt a keresett személy állapotáról. A közösségi oldalak lehetővé teszik a támadónak, hogy név, kulcsszó alapján keressen embereket, társaságokat, iskolákat, a célpont barátait, kollégáit és a körülöttük élő embereket. Ezeken a webhelyeken keresve személyes információk érhetők el, például névről, beosztásról, szervezet nevéről, jelenlegi helyéről és oktatási képesítésekről. Ezenkívül olyan professzionális információkat is találhat, mint például a vállalat vagy az üzleti vállalkozás, a telefonszám, e-mail, fényképek, videók és így tovább. Szociális hálózati webhelyek, például a Twitter, tanácsok, hírek, aggodalmak, vélemények, pletykák, és tények gyűjtőhelye. A közösségi hálózati szolgáltatásokon keresztüli keresés révén a támadó kritikákat gyűjthet össze, olyan információkat, amelyek hasznosak a social engineering vagy más típusú támadások végrehajtásában.

A cél figyelése riasztással

A riasztások olyan tartalomfigyelő szolgáltatások, amelyek automatikusan frissítik a felhasználó preferenciáit, általában e-mailben vagy SMS-ben. A riasztások fogadásához a felhasználónak regisztrálnia kell a webhelyen, és e-mail-címet vagy telefonszámot kell megadnia. Online riasztási szolgáltatások automatikusan értesítik a felhasználókat, ha a hír, a biográfia és a beszélgetéscsoportok új tartalma megfelel a felhasználás által kiválasztott keresett kifejezések készletének. Ezek a szolgáltatások a legfrissebb információkat jelenítik meg a versenytársakról és az iparról. Ezen toolok némelyike segít a szervezet nevét, tagjainak nevét, weboldalát, illetve a fontos embereket vagy projekteket is kideríteni. A támadók rendszeresen összegyűjthetik a figyelmeztető szolgálatok által frissített információkat a célról, és felhasználhatják azokat további támadásokra. A Google Alerts[13] automatikusan értesíti a felhasználókat, ha új tartalom kerül fel a hírekből, az internetről, a blogokról, ha a videó- és/vagy beszélgetőcsoportok megegyeznek a felhasználó által kiválasztott és a Google Alerts szolgáltatás által tárolt keresési kifejezések halmazával.

Információgyűjtés fórumok, blogok segítségével

Sok internet-felhasználó veszi igénybe a csoportos blogokat és fórumokat tudásmegosztási célokra. Ezen okból kifolyólag a munkatársak gyakran csoportokra, fórumokra és blogokra összpontosítanak, hogy információkat találjanak a célszervezetről és annak embereiről. A szervezetek általában nem figyelik ezeket, amely esetben az alkalmazottak más felhasználók számára adnak ismereteket – fórumok, blogok és csoportos beszélgetések során. A támadók előnyt kovácsolva ebből, érzékeny információkat gyűjtenek a célokról, publikus hálózati információkat, rendszerinformációkat és személyes adatokat. A támadók hamis profilokkal regisztrálhatnak csoportokba és próbálhatnak csatlakozni a célszervezet munkavállalói csoportjaihoz, ahol megoszthatják a személyes és vállalati információkat. A támadók információs csoportokat, fórumokat és blogokat keresnek a hibás domainnevek, IP-címek alapján is. A munkavállalói információk, amelyeket a támadó csoportokból, fórumokból és blogokból gyűjthet:

- az alkalmazott teljes neve;
- a munka- és lakóhely;
- otthoni telefonszám, mobiltelefonszám vagy irodai szám;
- személyes és szervezeti e-mail-cím;
- képek a munkavállalói lakóhelyről vagy munkahelyről, amely azonosítható információkat tartalmaz;
- képek a munkavállalói díjakról és jutalmakról vagy a közelgő célokról.

A mai információs társadalom kibertérben történő jelentléte egyik részét képezi a webszolgáltatásokon való megjelenés. Az internet világot összekapcsoló hálózatos jellege miatt rengeteg olyan weben található szolgáltatás létezik, amely elősegíti az információ

[13] A Google Alerts egy tartalomváltozásészlelési és -értesítési szolgáltatás, amelyet a Google keresőmotorja kínál.

begyűjtését. Még mindig nem feltétlenül technikai információ begyűjtése a cél, sokkal inkább a környezet, a kapcsolatok, alapvető adatok, nevek, érdeklődési körök, webes megjelenés, fizikai elhelyezkedés. Ezek a közétett adatokkal összefésülve puzzle- vagy építőkocka-szerűen egészítik ki egymást, így az esetleges hiányokat információs átfedésekkel egy komplexebb információt kaphatunk a célról és a célhoz kapcsolódó pontokról. Egyfajta profilozást lehet szintről szintre végrehajtani a weben található szolgáltatások, a keresőmotorok helyes kihasználásával.

Weboldal-információgyűjtés

A webhelyről való információgyűjtés a célszervezet weboldalának figyelemmel kísérése és elemzése. Itt már technikai információk kinyerése is a célok között szerepel. A támadó elkészítheti a weboldal szerkezetének és architektúrájának részletes térképét anélkül, hogy a rendszergazda gyanúját felkeltené.

A támadók alapvető toolokat is használnak, amelyek az operációs rendszerek beépített egyszerű programjai is lehetnek, mint például Telnet[14] vagy böngésző. Ezenfelül szofisztikált segédprogramokat is, mint a Netcraft,[15] ami összegyűjti a weboldal adatait, például az IP-címet, a domaintulajdonos regisztrált nevét és címét, a domainnevet, a webhely hosztját és az operációs rendszer részleteit. Habár nem biztos, hogy megadja ezeket az adatokat minden webhelyre vonatkozóan.

A céloldal böngészése jellemzően a következő információkat nyújtja:

- használt szoftver és verziója: A támadó könnyedén megtalálja a használt szoftververziót;
- használt operációs rendszer: Általában a használt operációs rendszer is meghatározható;
- alkönyvtárak és paraméterek: A keresések feltárják az alkönyvtárakat és a paramétereket azáltal, hogy feljegyezik az URL-eket, miközben a célwebhelyet böngészik;
- fájlnév, elérési út, adatbázis-mezőnév vagy lekérdezés: A támadó gyakran alaposan vizsgál minden olyan lekérdezést, amely fájlnév, elérési út, adatbázis-mezőnév vagy lekérdezésnek tűnik, annak ellenőrzése érdekében, hogy az lehetőséget kínál-e az SQL-injection támadásra;
- szkripting platform: A szkriptfájlnév-kiterjesztések segítségével, például.php,. asp vagy.jsp, könnyen meghatározható a szkript[16] platform, amelyet a célwebhely használ;
- kapcsolatfelvételi részletek és CMS[17]-adatok: A kapcsolattartó oldalak szokásos részleteket tartalmaznak, például neveket, telefonszámokat, e-mail-címeket

[14] A Telnet lényege, hogy a saját számítógépéről be tud jelentkezni egy másik (mindegy, hogy a világ melyik részén lévő) számítógépre.

[15] A Netcraft egy internetes szolgáltató cég, amely számos iparágban nyújt kiberbűnözés-megszakító szolgáltatásokat.

[16] Az informatikában a szkript névvel rövid programokat illetnek, amelyek gyakran egy-egy részfeladat automatizálására szolgálnak.

[17] A CMS magyarul tartalomkezelő rendszer, az elnevezésből pedig következik, hogy segítségével a tartalmaidat tudod létrehozni vagy változtatni. A CMS tulajdonképpen egy webes szoftvercsomag a weboldalad kezeléséhez.

és az adminisztrátorok vagy támogató személyek adatait. A támadó ezeket az adatokat felhasználhatja socialengineering-támadások végrehajtására.

A HTML[18]-forráskód vizsgálata

A támadók érzékeny információkat gyűjthetnek a HTML forráskódjának megvizsgálásával, valamint a manuálisan beillesztett vagy a CMS-rendszer által létrehozott megjegyzések követésével. A megjegyzések utalást adhatnak a háttérben futó eseményekre. Ez akár a webes fejlesztő vagy az adminisztrátor részletes adatait is tartalmazhatja. A fájlrendszer struktúrájának feltérképezése érdekében az összes hivatkozást és képcímkét meg kell őrizni. Néha lehetséges a forráskód szerkesztése.

Sütik[19] vizsgálata

A futó szoftver és annak viselkedése meghatározásához meg lehet vizsgálni a szerver által beállított sütiket. Azonosítani lehet a szkriptplatformokat munkamenetek és más támogató sütik megfigyelésével. A sütik nevére, értékére, domainméretére vonatkozó információk szintén kibonthatók.

Web spider programok használata

A web spider (más néven webbejáró vagy webrobot) egy olyan program vagy automata szkript, amely módszeresen böngészi a webhelyeket, hogy összegyűjtse a meghatározott információkat, például a munkavállalók nevét, e-mail-címét és így tovább. A támadók ezután felhasználják az összegyűjtött információkat különböző támadások végrehajtására. A webes spider elbukik, ha a célwebhelyen a robots.txt fájl található a gyökérkönyvtárban, a könyvtárak felsorolásával a bejárások megakadályozása érdekében.

Példák a webspider-programokra:

- Webextractor (www.webextractor.com);
- Spiderfoot (www.spiderfoot.net);
- Scrapy (https://scrapy.org);
- Screaming Frog (www.screamingfrog.co.uk);
- Beam Us Up SEAo SpiderSEO (http://beamusup.com).

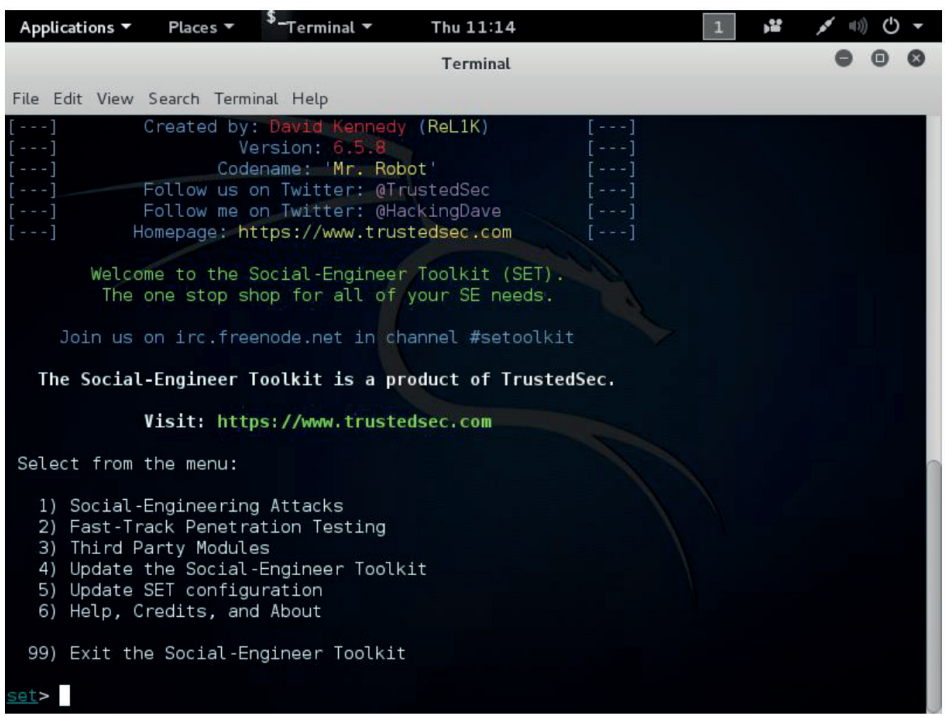
[18] A HTML (angolul: HyperText Markup Language) egy leíró nyelv, amelyet weboldalak készítéséhez fejlesztettek ki.

[19] A HTTP-süti (általában egyszerűen süti, illetve angolul cookie) egy információcsomag, amelyet a szerver küld a webböngészőnek, majd a böngésző visszaküld a szervernek minden, a szerver felé irányított kérés alkalmával.

Teljes webhely tükrözése

A webhelytükrözésnél az eredeti webhely pontos mását vagy klónját hozzák létre, ahogy az a 4. ábrán is látható, ahol saját teszt során végeztem el ezt a műveletet. A felhasználók a weboldalak másolatát a HTTrack Web Site Copier és az NCollector Studio tükrözőtolljaival is elvégezhetik. Ezek az toolok letöltik a weboldalt egy helyi könyvtárba, rekurzív módon felépítve az összes mappát (HTML, képek, flash, videók és egyéb fájlok) a webszerverről egy másik számítógépre. A webhely tükrözésének a következő előnyei vannak:

- hasznos az offline böngészéshez;
- támogatja a támadót abban, hogy több időt töltsön el a weboldal megtekintésében és elemzésében a sebezhetőség szempontjából;
- elősegíti a címtárszerkezet és más értékes információk megtalálását a tükrözött másolatból, anélkül, hogy több kérést kellene adnia a webszervernek.



4. ábra

SET-toolkit website klónozás egyik lehetséges példája [6]

Példák tükröző toolokra:

- Pavuk (http://pavuk.sourceforge.net);
- BackStreet Browser (www.spadixbd.com);
- SurfOffline (www.surfoffline.com);

- BlackWidow (www.softbytelabs.com);
- NCollector Studio (www.calluna-software.com);
- Teleport Pro (www.tenmax.com);
- Portable Offline Browser (www.metaproducts.com);
- Offline Explorer Enterprise (www.metaproducts.com);
- Website Ripper Copier (www.tensons.com).

Metaadatok kibontása nyilvános dokumentumokból

Hasznos információk találhatók a célszervezet weboldalán pdf[20]-dokumentumok, Microsoft Word[21]-fájlok és egyéb formátumok formájában. Képesnek kell lennie a támadónak az értékes adatok kinyerésére, ideértve a metaadatokat és az ilyen dokumentumokba rejtett információkat is. Elsősorban rejtett információkat tartalmaznak az elemzés céljából elemezhető nyilvános dokumentumokról, például az oldal címét, leírását, kulcsszavakat, a létrehozási/módosítási adatokat és a tartalom idejét, felhasználási címeket és a célszervezet alkalmazottainak e-mail-címeit.

A metaadat-kibontó segédprogramok automatikusan kinyerik a kritikus információkat, amelyek magukban foglalják az ügyfelek felhasználónevét, az operációs rendszereket (a kihasználások operációs rendszerekre vonatkoznak), az e-mail címeket, a használt szoftverek listáját (verzió és típus), a szerverek és a dokumentumok létrehozásának/módosításának dátumát, a weboldal szerzőinek listáját és így tovább.

- ExtractMetadata (www.txtroctmetadata.com);
- FOCA (www.tkvenpoths.com);
- Meta Tag Analyzer (www.seocentro.com);
- BuzzStream (http://tools.bullstream.com);
- Analyse Metadata (www.exodium.com);
- Web Data Extractor (www.webextractor.com).

A weboldal-információgyűjtés technikailag kifejezetten http adatkapcsolati kérésekben működő weboldalszoftverek és programnyelvek, beállítások által kinyert információkat takarnak, amely paraméterekkel már könnyebb behatárolni a kihasználható sérülékenységeket, vagy legalábbis realizálni a nem frissített, elavult megoldásokat használó célpontokat. Ezenfelül a könyvtárstruktúrából következtetéseket lehet levonni, például hogy az elérni kívánt különböző prioritású adatok hol találhatók.

E-mail-információgyűjtés

Az e-mail-kommunikáció követése, az Emailtracking[22] egy adott felhasználó e-mailjeit figyeli. Ez a fajta nyomon követés a digitális időbélyegzés révén lehetséges, amikor

[20] A Portable Document Format (PDF) az Adobe Systems által kifejlesztett, dokumentumok tárolására alkalmas fájlformátum.
[21] A Microsoft Word a Microsoft által készített dokumentumszerkesztő program.
[22] E-mail-követés.

a célpont megkap és megnyit egy adott e-mailt. Az e-mail-nyomkövető toolok lehetővé teszik a támadó számára az információk gyűjtését, például IP-címeket, e-mail-kiszolgálókat és az e-mail küldésében részt vevő szolgáltatót.

Az e-mailek nyomon követésének tooljai közé tartozik az eMailTrackerPro, a Yesware, a Contact Monkey stb. Információk az áldozatokról az emailtrack-toolok segítségével:

- címzettrendszer IP-címe: lehetővé teszi a címzett IP-címének nyomon követését;
- helyzet: megbecsüli és megjeleníti a címzett helyét a térképen, és kiszámíthatja a távolságot a támadó helyétől;
- érkezett és olvasott e-mail: értesíti, hogy mikor fogadja és olvassa el az e-mailt a címzett;
- olvasás időtartama: az az időtartam, amelyet a címzett a küldött levél olvasására fordít;
- proxy[23] észlelése: információt szolgáltat a címzett által használt kiszolgáló típusáról;
- linkek: ellenőrzi, hogy ellenőrizték-e a címzettnek e-mailben elküldött linkeket;
- operációs rendszer és a böngésző adatai: információkat jelenít meg a fogadó által használt operációs rendszerről és böngészőről. A támadó ennek az információnak a felhasználásával meg tudja találni az operációs rendszer és a böngésző verzióját, hogy további támadásokat indítson;
- e-mail-továbbítás: meghatározza, hogy a felhasználónak küldött e-maileket továbbítják-e egy másik személynek;
- eszköz típusa: információt nyújt az e-mail megnyitásához és olvasásához használt eszköz típusáról, például asztali számítógép, mobileszköz vagy laptop.

Információ gyűjtése az e-mail-fejlécből

Az e-mail-fejléc tartalmazza a feladó adatait, a routing-információkat,[24] a dátumot, a tárgyat és a címzettet. Mindegyik kiváló információforrás a támadó számára a cél elleni támadások indításához. Az e-mail-fejléc megtekintésének folyamata a különböző e-mail-programoktól függ. Az e-mail fejléce a következő információkat tartalmazza:

- a feladó e-mail-szerver;
- a feladó e-mail-szerverei által kapott adatok és idő;
- a feladó e-mail-szervere által használt hitelesítési rendszer;
- az adatok és az üzenet elküldésének ideje;
- az mr.google.com által kiosztott egyedi szám, amely azonosítja az üzenetet;
- a feladó teljes neve;
- a feladó IP-címe és a cím, ahonnan az üzenet el lett küldve.

[23] Számítógép-hálózatokban proxynak, helyesebben proxyszervernek nevezzük az olyan szervert (számítógép vagy szerveralkalmazás), amely a kliensek kéréseit köztes elemként más szerverekhez továbbítja. A kliens csatlakozik a proxyhoz, majd valamilyen szolgáltatást (fájlt, csatlakozást, weboldalt vagy más erőforrást) igényel, ami egy másik szerveren található.

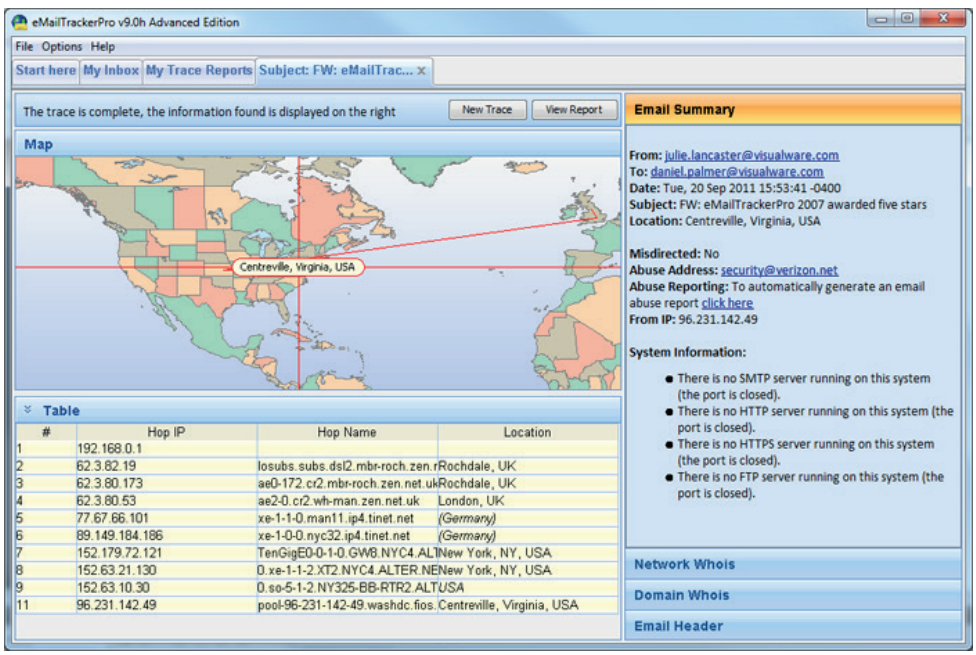
[24] Az útválasztás, hálózati forgalomirányítás vagy routing az informatikában annak kiválasztását jelenti, hogy a hálózatban milyen útvonalon haladjon a hálózati forgalom.

A támadó a teljes e-mail fejlécének részletes elemzésével nyomon tudja követni és összegyűjti ezeket az információkat.

E-mail-követő toolok

Az e-mail-követő toolok lehetővé teszik a támadónak egy e-mail nyomon követését és olyan információk kinyerését, mint például a feladó azonosítója, a levelezőszerver, a feladó IP-címe és így tovább. Ezek az eszközök nem automatikusan küldik el a fájlokat, ha a címzettek megnyitják a levelet és adnak állapotinformációt arról, hogy az e-mail sikeresen kézbesítve lesz-e vagy sem. A támadók a kibontott információt használják, hogy megcélozzák a szervezetet és annak rendszereit kártékony e-mailek küldésével.

- eMailTrackerPro (www.emailtrackerpro.com)
  Az eMailTrackerPro elemzi az e-mailek fejléceit, és olyan információkat tár fel, mint például a feladó földrajzi elhelyezkedése, IP-címe és így tovább (5. ábra). Ez lehetővé teszi a támadó számára, hogy később megtekintse a nyomokat a korábbi nyomok mentésével.



5. ábra
eMailTrackerPro [12]

További széles körben elterjedt toolok:

- PoliteMail(www.politemail.com);
- Yesware (www.yesware.com);

- ContactMonkey (https://contactmonkey.com);
- Zendio (www.zendio.com);
- ReadNotify (www.readnotify.com);
- DidTheyReadIt (www.didtheyreadit.com).

Az e-mail-információgyűjtés a technikai és nem technikai adatok gyűjtésébe is beletartozik, hiszen a technikai oldalról közelítve a dolgot ezen információk felhasználásával jelentős támadásokat lehet előkészíteni. Mint például e-mail-fejléccsere, ezáltal másnak kiadni magunkat, levelezőszerver IP-címe DoS[25]-támadásokra, linkek beágyazva rosszindulatú kódokkal, malware-ekkel. Ezenfelül, szintén átfedve az előző kettő kategóriát, személynevek, cégnevek, a levél tartalmából kapcsolatok, kontextusok nyerhetők ki. Folyamatos e-mailnyomonkövető-eszközökkel a kiberműveleti penetrációs munkafolyamatok az információktól függően frissíthetők, változtathatók a támadási irányvonalak. Ezzel a négy közétett adat elemzésével egy összeségében olyan információhalmaz állítható össze, amely egy általános képet ad a célpontról, és ennek birtokában haladhatunk az összetettebb, komplexebb és technikai információk begyűjtéséhez.

Alapvető DNS-információk lekérdezése és vizsgálata

Ebben a fejezetben látható, hogy számos tool használható, amelyek hasonló eredményeket generálnak, ennek oka az, hogy ellenőriznünk kell az összegyűjtött információkat. Ha azok egynél több tool segítségével is kinyerhetők, akkor megbízhatóbbak. A felsorolt lehetőségek főként nyílt forráskódú szoftvereken, toolokon keresztül alapvető technikai információk begyűjtésére szolgálnak, amelyek így a közétett adatokkal összhangban egy optimális, várhatóan elegendő információhalmazt hoznak létre. Ezután a kiberműveleti penetrációs teszt munkafolyamatában tovább lehet haladni a még részletesebb hálózat-feltérképezésre, illetve sérülékenységelemzésre [7], [8].

WhoIs

A tervezésnél fontos összegyűjteni a hálózattal kapcsolatos információkat, például a „WhoIs"-információkat a célszervezetről. A WhoIs egy lekérdezési és válaszprotokoll, olyan adatbázisok lekérdezésére, amelyek tárolják a regisztrált felhasználókat vagy internetes erőforrások jogosultjait, például egy domainnevet, egy IP-cím-blokkot vagy egy autonóm rendszert. Ez a protokoll a 43-as porton (TCP[26]) lévő kérésekre vonatkozik. A regionális internetes nyilvántartások (RIR[27]) fenntartják a WhoIs-adatbázisokat, amelyek a domaintulajdonosok személyes adatait tartalmazzák. Minden

[25] A szolgáltatásmegtagadással járó támadás (Denial of Service vagy DoS), más néven túlterheléses támadás, illetve az elosztott szolgáltatásmegtagadással járó támadás (Distributed Denial of Service, DDoS) informatikai szolgáltatás teljes vagy részleges megbénítása, helyes működési módjától való eltérítése.

[26] A Transmission Control Protocol (TCP) az internet gerincét alkotó TCP/IP-protokollcsalád egyik fő protokollja.

[27] A regionális internetes regiszter (RIR) olyan szervezet, amely az IP-címek blokkjait földrajzi hatáskörébe helyezi.

egyes erőforrás esetében a WhoIs-adatbázis szöveges nyilvántartásokat tartalmaz magáról az erőforrásról, valamint a meghatalmazottakról, regisztrálókról és az adminisztrátori információkról (létrehozás és lejárati dátum).

Parancsa:
#whois example.com

A WhoIs-lekérdezés a következő információkat adja vissza:

- domainnév részletei;
- domaintulajdonos kapcsolattartási adatai;
- domainnévszerverek;
- lejárati rekordok;
- utoljára frissített rekordok;
- domain létrehozásának dátuma.

A támadó lekérdezi a WhoIs adatbázis-kiszolgálót, hogy információkat szerezzen a céltartomány nevéről, a tulajdonos elérhetőségeiről, a lejárat dátumáról, a létrehozás dátumáról és így tovább. A WhoIs pedig a kérelemre válaszol a kért információkkal. Ezen információk felhasználásával a támadó elkészítheti a szervezet hálózatának térképét, és megtéveszthet a domaintulajdonosokat social engineeringgel.

WhoIs keresési eredmény analízise

A WhoIs például a http://whois.domaintools.com vagy a www.tamos.com segítségével segíthet a WhoIs-lookups-lekérdezésekben. A domaintools.com szolgáltatás a WhoIs számára olyan információkat nyújt, mint például a regisztráló információ, az e-mail, az adminisztrátori kapcsolatinformáció, a létrehozott és az érvényességi idő, valamint a domainszerverek listája. A SmartWhois elérhető a www.tamos.com webhelyen. Megadja az információt az IP-címről, hosztnévről vagy domainről, ideértve az országot, az államot vagy a megyét, a várost, a telefonszámot, a faxszámot, a hálózati szolgáltató nevét, az adminisztrátort és a műszaki támogatás elérhetőségét. Ezenkívül segít megtalálni a domain tulajdonosát, a tulajdonos elérhetőségét az IP-cím-blokk tulajdonosát, a domain regisztrált dátumát és így tovább.

Domain Name: EXAMPLE.COM
Registry Domain ID: 2336799_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.iana.org
Registrar URL: http://res-dom.iana.org
Updated Date: 2019-08-14T07:04:41Z
Creation Date: 1995-08-14T04:00:00Z
Registry Expiry Date: 2020-08-13T04:00:00Z
Registrar: RESERVED-Internet Assigned Numbers Authority
Registrar IANA ID: 376
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:

Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Name Server: A.IANA-SERVERS.NET
Name Server: B.IANA-SERVERS.NET
DNSSEC: signedDelegation

DNS-információk kibontása

Domain Name System információk kibontása információt szolgáltat a DNS-zóna-adatokról. A DNSzone-adatok tartalmazzák az DNS-domainneveket, a számítógépneveket, az IP-címeket és sok más részletet a hálózatról.

Az DNS-információk kibontása segít a cél DNS-re vonatkozó következő rekordok meghatározásában (2. táblázat):

2. táblázat
DNS-rekordok [4]

A	Rámutat a hoszt IP címére
MX	Rámutat a domain levelező szerverére
NS	Rámutat a hoszt név szerverére
CNAME	Kanonikus elnevezés lehetővé teszi az alias nevek használatát a hoszt
SOA	Irányadó információk a DNS-zónáról; az elsődleges névkiszolgáló, a tartomány rendszengazdájának e-mail-címe, a tartomány sorozatszáma, a zóna frissitési időközei.
SRV	Általános szolgáltatás-helymeghatározó rekord, újabb protokollok számára, elkerülendő a protokoll-specifikus rekordokat, mint az MX.
PTR	Kanonikus névre mutat. A CNAME-től eltérően nem történik további DNS-beli feldolgozás, maga a név a visszatérési érték. Leggyakrabban reverse DNS-lekérdezéseknel használják, de pl. az Apple DNS-SD-jében is használják.
RP	A tartományhoz rendelt felelős személy. Általában egy e-mail-cím, amiben a @ karaktert helyettesíti.
TXT	Text rekord (szöveges rekord)

A DNS-lekérdező toolok (például a www.dnsstuff.com) és a DNS-rekordok (http://network-tools.com) lehetővé teszik a felhasználó számára a DNS-adatok információgyűjtésének végrehajtását. A DNSstuff információkat gyűjt az IP-címekről, e-mail kiszolgáló-kiterjesztésekről, DNSlookupokról, WhoIs-keresésekről és így tovább. Ha a célhálózat lehetővé teszi az ismeretlen, jogosulatlan felhasználók számára a DNS-zónaadatok továbbítását, akkor a támadónak könnyű megismerkednie a DNS-ről szóló információkkal, a segédprogramok segítségével.

host

Miután megkaptuk a DNS-kiszolgáló adatait, a következő lépés egy host IP-címének megismerése:

#host www.example.com

A parancs eredménye a következő:

A www. example.com *címe 192.0.43.10*
A www.example.com *IPv6 címe 2001:500:88.200:10*

Az eredményt tekintve ismerjük az IPv4 és IPv6 címeit a www.example.com nevű hosztnak.

Alapértelmezés szerint a host parancs megkeresi a tartomány A-, AAAA- és MX-rekordjait. Bármely rekord lekérdezéséhez csak meg kell adni az -a opciót a parancshoz.

 # host -a example.com
Trying „example.com"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 25153
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 2
;; QUESTION SECTION:
;example.com. *IN ANY*
;; ANSWER SECTION:
example.com. *3201 IN SOA* dns1.icann.org.
hostmaster.icann.org. *2012080782 7200 3600 1209600 3600*
example.com. *46840 IN NS* a.iana-servers.net.
example.com. *46840 IN NS* b.iana-servers.net.
;; ADDITIONAL SECTION:
b.iana-servers.net. *1401 IN A 199.43.133.53*
a.iana-servers.net. *1401 IN A 199.43.132.53*

dig

A host parancson kívül a dig parancsot is használhatja a DNS-lekérdezéshez. A dig előnyei a hoszthoz viszonyítva a rugalmasság és a tiszta kimenet. A dig segítségével megkérhető a rendszer, hogy dolgozza fel a keresési kérelmek listáját fájlból.

Anélkül, hogy a domainnév mellett bármilyen lehetőséget megadna, a dig parancs csak a domain A-rekordját adja vissza. Bármely más DNS-rekordtípus szükséges, megadható a típus opció a parancssorban.

 # dig example.com
;<<>> DiG 9.8.4-rpz2+rl005.l2-Pl <<>> example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY,status: NOERROR, id:3786
;; flags: qr rd ra;,QUERY: I,ANSWER: I,AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:

;example.com. *IN A*
;; ANSWER SECTION:
example.com. *41023 IN A 192.0.43.10*
,, Query time: 14 msec
,, SERVER:10.17.3.245#53(10.17.3.245)
,, WHEN:Mon;May 13 18:33:09 2019
,, MSG SIZE rcvd:45

dnsenum

Információkat gyűjthetünk egy DNS-kiszolgálótól a dnsenum segítségével. Az összegyűjthető DNS-információk a következők:

- a host IP-címek;
- a domain DNS-szervere;
- a domain MX-rekordja.

A DNS-információk beszerzésén túl a dnsenum a következő tulajdonságokkal is rendelkezik:

- további nevek és aldomainek szerezhetők be a Google keresőmotorjával;
- az aldomainek nevét megtudhatja úgy, hogy brute forcing kikényszeríti a neveket a szöveges fájlokból;
- elvégzi a WhoIs-lekérdezéseket a C-osztályú tartományi hálózati tartományokban és kiszámítja azok hálózati tartományait;
- fordított keresést végez a hálózati tartományokban;
- szálakat használ a különböző lekérdezések feldolgozásához.

A dnsenum alapértelmezett beállításaival információkat szerezhetünk a hoszt címéről, a névszerver és a levelezőszerver IP-címéről. dnsenum.pl example.com

#dnsenum example.com
dnsenum.pl *VERSION:1.2.2*
—- example.com —-
Host's addresses:

_____

Name Servers:

_____

ns1.isp.com *10771 IN A 172.168.1.2*
ns0.isp.com *7141 IN A 172.168.1.1*
Mail (MX) Servers:

_____

hermes1.example.com *86400 IN A 192.168.10.3*
hermes.example.com *3600 IN A 192.168.10.2*
Trying Zone Transfers and getting Bind Versions:

_____

Trying Zone Transfer for example.com *on* ns0.isp.com …

AXFR record query failed: NOERROR
ns0.isp.com *Bind Version:*
DNS server

Az előzőkben alkalmazott parancsok a technikai DNS-információk lekérdezésére alkalmasak. Ezáltal olyan információkhoz segít hozzáférni, amelyek akár kulcsfontosságúak is lehetnek egy teszt vagy támadás felépítése, de legalábbis előkészítése során. Kinyerjük, hogy melyik szervezetnél regisztrált domain-nevet, mi a szerver IP-címe, mi a levelezőszervere, mi a névszervere, mikor regisztrált, mikor jár le a regisztráció, ki a kontakt és még pár nagyon hasznos információ, amelyeket a közzétett adatok elemzésével együtt használva egy erős információs adatbázist képezhet a munkafolyamat első lépcsőjében.

Következtetések

A kiberműveletekben és informatikában az információgyűjtési tevékenységek azonosítják a szervezetekhez kapcsolódó, nyilvánosság számára hozzáférhető információkat. Az információgyűjtési technikákat használva számos lehetőség nyílik a célszervezet hálózatának illetéktelen hozzáférésére. Nincs egységes módszer az információgyűjtésre, hiszen azok számos módon beszerezhetők. Viszont a lehető legtöbb információt be kell gyűjteni, így érdemes ezt a fázist szervezett módon végrehajtani. Jelen cikk összefoglalja ennek lehetőségeit, az alkalmazott technika alapján kategorizálja azokat, és konkrét megvalósítási példákat is felsorakoztat a megértés érdekében. A közzétett adatok elemzése, illetve az alapvető DNS-információk lekérdezése, valamint vizsgálata olyan fontos elemek, amelyeknek részletes tanulmányozásával penetrációs tesztünk kezdő fázisa elindítható, és jelentős eredmények érhetők el egy ilyen teszt módszertanának végrehajtásánál.

Következtetésként az információgyűjtési technikák bár sokrétűek és sokfélék, az egyszerűbb információgyűjtéstől haladva a nehezebb, már toolokat alkalmazó gyűjtés felé, minél több forrásból nyerjük ki az információkat, annál nagyobb hatásfokkal indítható el maga a penetrációs teszt módszertanának folyamata. Ezeket a megfelelő struktúrába rendezve és gyűjtve egy munkafolyamat első lépését lehet megtenni, amely hozzájárul az eredményes és effektív feladatvégrehajtáshoz. Levonható következtetésként, hogy a kibertérben zajló és teszthez kapcsolódó műveletek sokrétegűek, és nemcsak technikai információgyűjtést foglalnak magukban, hanem az emberi, szervezeti információk halmazára is irányulnak. Ötvözve és összefésülve a közzétett adatok elemzésekor, illetve az alapvető DNS-információk lekérdezésekor kapott információkat, egy biztos alapot kapunk az általunk végrehajtani kívánt teszthez, támadáshoz.

Hivatkozások

[1] I. Paráda, „Basic of Cybersecurity Penetration Test," *Hadmérnök,* 13. évf. 3. sz., pp. 435–442., 2018.

[2] Zs. Haig, *Információs műveletek a kibertérben.* Budapest: Dialóg Campus kiadó, 2018.

[3] L. Kovács, *A kibertér védelme.* Budapest: Dialóg Campus Kiadó, 2018.

[4] S.-P. Oriyano, *CEH™v9.* [Certified Ethical Hacker] 2016. DOI: https://doi.org/10.1002/9781119419303

[5] „Google Search: a keresési operátorok teljes listája," *thepitch.hu,* [Online]. Elérhető: https://thepitch.hu/google-keresesi-operatorok-listaja/ (Letöltve: 2019. 08. 16.)

[6] I. P. István Bodnár, „Jelszó ellopás social engineering, e-mail spoofing és fake url segítségével," *Hírvillám,* 7. évf. 1. sz., pp. 139–147., 2016. [Online]. Elérhető: http://comconf.hu/kiadvany/hirvillam_7evfolyam_1szam.pdf (Letöltve: 2019. 08. 16.)

[7] T. Heriyanto, L. Allen and S. Ali, *Kali Linux – Assuring Security by Penetration Testing.* Birmingham: Packt Publishing, 2014.

[8] R. W. Beggs, *Mastering Kali Linux for Advanced Penetration Testing.* Birmingham: Packt Publishing, 2014, pp. 47–52.

[9] „A Google dorking hackelési technika veszélyei és megelőzésének lehetőségei," *szoftver.hu,* 2016. [Online]. Elérhető: https://szoftver.hu/hirmorzsak/a-google-dorking-hackelesi-technika-veszelyei-es-megelozesenek-lehetosegei (Letöltve: 2020. 01. 07.)

[10] "Google hacking database," *exploit-db.com,* [Online]. Elérhető: www.exploit-db.com/google-hacking-database (Letöltve: 2020. 01. 07.)

[11] "Site report for http://example.com," *sitereport.netcraft.com,* [Online]. Elérhető: https://sitereport.netcraft.com/?url=http%3A%2F%2Fexample.com (Letöltve: 2020. 03. 03.)

[12] "Tracing an email header," *emailtrackerpro.com,* [Online]. Elérhető: www.emailtrackerpro.com/support/v9/tutorials/traceheader.html (Letöltve: 2020. 03. 03.)