FELDERÍTÉS ÉS ANALÍZIS A PENETRÁCIÓS TESZTBEN I. INFORMÁCIÓGYŰJTÉSI TECHNIKÁK

RECONNAISSANCE AND ANALYSIS IN THE PENETRATION TEST I. INFORMATION GATHERING TECHNIQUES

Paráda István, Nemzeti Közszolgálati Egyetem, Katonai Műszaki Doktori Iskola, doktorandusz; Orcid: 0000-0002-3083-6015

Farkas Tibor PhD, Nemzeti Közszolgálati Egyetem, Hadtudományi és Honvédtisztképző Kar, egyetemi docens, Orcid: 0000-0002-8868-9628

paradaistvan@gmail.com; farkas.tibor@uni-nke.hu

Absztrakt

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 analízis szintjén lévő, információgyűjtési tevékenységek azonosítják (kockázati szintjen) a szervezetekhez kacsolódó, nyilvánosság számára hozzáférhető információkat. Az információgyűjtés a penetrációs teszt 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] „Jelen közlemény a Bolyai János Kutatási Ösztöndíj támogatásával készült”

Kulcsszavak: *Információgyűjtés, keresőmotorok, DNS, Whois,*

Abstract

This series of articles deals with the detection and analysis level 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 organizations. Gathering information is the first step in the penetration test implementation process, which involves gathering information about the target network and target environment. Using information gathering techniques, there are many opportunities for unauthorized access to the target organization's network. This allows you to create a security profile of the target organization's network, system, and partly the organization 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, it is worthwhile to carry out this phase in an organized manner. “This article was supported by the János Bolyai Research Scholarship of the Hungarian Academy of Sciences.”

Keywords: *Information Gathering, Search engines, DNS, Whois*

BEVEZETÉS

Az információgyűjtés lehet aktív és passzív. A passzív alatt közvetlen kölcsönhatás nélkül kerül sor az információk begyűjtésére. Főként akkor hasznos, ha nem kívánatos, hogy a cél tudjon az információgyűjtés tényéről. Ezek lehetnek: kereső motorokkal való információkeresés, domain név[1] ellenőrzés, helymeghatározási információk lekérdezése, információgyűjtés közösségi hálózati oldalakon keresztül, információgyűjtés a célról a pénzügyi szolgáltatásokon keresztül, a célszervezet szervezeti infrastruktúra adatainak összegyűjtése, információgyűjtés csoportok, fórumok és életrajzok felhasználásával, a célszervezet által használt operációs rendszerek meghatározása, a cél webhelyének forgalmának ellenőrzése, a cél online hírnevének nyomon követése. Az aktív esetén a célokról közvetlen interakcióval gyűjtik az információkat, a célpont felismerheti a folyamatban lévő információgyűjtési folyamatot, mivel nyíltan lépünk kapcsolatba a célhálózattal. Ezek lehetnek a cél közzétett névszervereinek lekérdezése, webes információgyűjtés tükröző eszközök (továbbiakban toolok) segítségével, információgyűjtés e-mail követés segítségével, Whois lookup[2], DNS[3] információ lekérdezések stb…

A KÖZZÉTETT ADATOK ELEMZÉSE

Az információgyűjtés-módszertan egy eljárás a célszervezettel kapcsolatos információk gyűjtésére az összes 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 domain nevek konkrét tartományát, elérhetőségi adatait és egyéb kapcsolódó információkat. [2]

Információgyűjtés keresőmotorok segítségével

A keresőmotorok a fő források a célszervezettel kapcsolatos kulcsinformációk megkereséséhez. A keresőmotorok fontos szerepet töltenek be a kritikus részletek felderítése terén, kinyerhetik a célokról szóló információkat, beleértve például technológiai platformokat, alkalmazottak adatait, bejelentkezési oldalakat, intranet portálokat, elérhetőségeket és így tovább. Ez az információ segíti a támadót a social engineering[5] és más típusú támadások végrehajtásában. A keresési eredmények böngészése 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

---

[1] A tartománynév (angolosan domainnév, illetve doménnév) az Internet egy meghatározott részét, tartományát egyedileg leíró megnevezés.
[2] A WHOIS-adatbázis a domainekkel kapcsolatos információkat tartalmaz
[3] A Domain Name System (DNS), egy hierarchikus, nagymértékben elosztott elnevezési rendszer számítógépek, szolgáltatások, illetve az internetre vagy egy magánhálózatra kötött bármilyen erőforrás számára.
[4] Az URL (*Uniform Resource Locator* [egységes erőforrás-hely] rövidítése), az interneten megtalálható bizonyos erőforrások szabványosított címe.
[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.

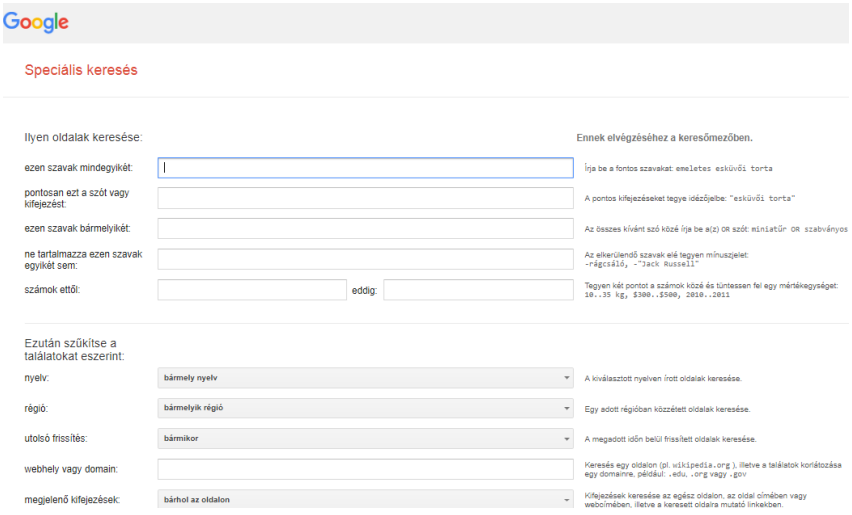
információkat nyújtanak a célszervezetről. A Google[6] hackelés mint kifejezés, a fejlett Google keresési operátorok használatára utal, hogy összetett keresési lekérdezéseket hozzon létre az érzékeny vagy rejtett információk kinyerésére. Ezután a támadók a hozzáférhető információkat a sebezhető célok felkutatására használják. Az információgyűjtés fejlett Google-hackelési technikákkal történő összegyűjtésével a Google a keresési eredmények speciális szövegrészeit egy speciális operátor segítségével, 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 elérése érdekében.

Egyszerű operátorok	Haladó operátorok
filetype: Csak a megadott kiterjesztésű (pl. 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, amit 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 URLekkel működik, keresőszavakkal nem. Illetve, ha a kettőspont után szóközt 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 (cachelt) változatát. Hasznos lehet, olyan oldalak esetén kíváncsi, amik már esetleg valamilyen okból törlésre kerültek.	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.	

1. ábra Főbb operátorok [3]

A támadó nem tud egyszerűen információt gyűjteni az információs oldalról, csak egy normál keresőmező segítségével. 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.

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



2. ábra Google speciális keresés [4]

Mit tehet egy támadó a Google Hack módszerek segítségével?
A támadó 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 hozzárendelni őket a személyes, érzékeny információiakhoz, például hitelkártya számok, szociális biztonsági számok, jelszavak és így tovább. Ha a kiszolgáltatott célt azonosítják, a támadók különféle lehetséges támadásokat próbálnak indítani, mint például puffer túlcsordulások[7], és, többek között SQLInjection[8]. Példák a nyilvános kiszolgálókra hagyott érzékeny információkra, amelyeket a támadó a segítség segítségével kivonhat a Google Hacking Database (GHOB) lekérdezései között szerepel:

- Érzékeny információkat tartalmazó hibaüzenetek
- Jelszavakat tartalmazó fájlok
- Érzékeny könyvtárak
- A bejelentkezési portálokat tartalmazó oldalak
- Hálózati vagy sebezhetőségi adatokat tartalmazó oldalak
- Szerver sérülékenységek
- A szoftver verziószáma
- Webes alkalmazás forráskód

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,

[7] A puffertúlcsordulás (buffer overflow)olyan szoftverhiba, sokszor biztonsági rés, melynél egy processz a fix hosszúságú tömbbe (puffer) történő íráskor nem ellenőrzi annak határait, így azt túlírva a szomszédos memóriaterületet írja felül.
[8] Az Sql injection egy olyan támadás,amivel sérülékeny sql szerverekből lehet kibányászni hasznos információkat pl.: felhasználóneveket, jelszavakat, jelszó hasheket.

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 webhelyet arra tervezték, hogy megmutassák egy szervezet jelenlétét az interneten. Ingyenesen elérhető és bárki el is érheti, az ügyfelek és partnerek vonzására szolgál. Tartalmazhat olyan információkat, mint például a szervezeti előzmények, szolgáltatások és termékek, valamint elérhetőségi adatok. A cél külső URL-je megtalálható a keresőmotorok, például a Google, a Bing segítségével. Az aldomainek csak néhány ember számára elérhető. Ezek a személyek lehetnek foglalkoztatottak valamely szervezetnél vagy egy osztály tagjai. Az altartományok betekintést nyújtanak a célvállalat különböző szervezeti és üzleti egységeibe. A hozzáférési korlátozások a következők alapján alkalmazhatók: az IP cím, domain alhálózat, felhasználónév és jelszó. Az altartomány segíti a szervezet magánfunkcióit. A legtöbb szervezet általános formátumokat használ az altartományokhoz.

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 Wi-Fi, amelyek valószínűleg egy módja annak, hogy elérjék a célszervezet hálózatát. A támadók, akik tudják a célszerv elhelyezésének 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[9] felhasználásával. A támadók ezt az információt felhasználhatják jogosulatlan hozzáféréshez az épületekhez, vezetékes és vezeték nélküli hálózatokhoz, rendszerekhez. Példa: Google Earth (https://earth.google.com)
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, 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 létrehozásáról.

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

[9] A Google a Google által fejlesztett ingyenes internetes térképszolgáltatás.

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 vizsgálata az Linkedln, a Facebook, a Twitter, a Google +, az lnstagram 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 funkciói. 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, célpont barátait, kollégáit és a körülöttük élő embereket. Ezeken a webhelyeken keresve személyes információkat érhetők el, például névről, beosztásról, szervezet nevéről, jelenlegi helyéről és oktatási képesítésekről. Ezenkívül olyan professzionális információk is találhat, mint például a vállalat vagy az üzleti vállalkozás, a telefonszám, e-mail, a fényképek, a 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 információk, 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 értesíti a felhasználókat, ha a hír, a biográfia és a beszélgetéscsoportok új tartalma megfelel a felhasználás által kiválasztott keresett kifejezések készletének. Ezek a szolgáltatások legfrissebb információkat jelentenek a versenytársakról és az iparról. Ezen toolok némelyike segíti a szervezet nevét, tagjainak nevét, weboldalát vagy 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[10] automatikusan értesíti a felhasználókat, ha új tartalom kerül fel, a hírekből, az internetről, az blogokról, video- és/vagy beszélgetőcsoportok megegyeznek a felhasználó által kiválasztott és a GoogleAlerts 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

[10] A Google Alerts egy tartalomváltozás észlelési és értesítési szolgáltatás, amelyet a Google keresőmotorja kínál.

számára adnak ismereteket - fórumok, blogok és csoportos beszélgetések során. A támadók előnyt kovácsolva ebből, érzékeny információkat gyűjtenek a célokról: publikus hálózati információkat, rendszerinformációkat és a személyes adatokat. A támadók hamis profilokkal regisztrálhatnak csoportokba és próbálhatnak csatlakozni a célszervezet munkavállalói csoportojaihoz, ahol megoszthatják a személyes és vállalati információkat. A támadók információs csoportokat, fórumokat és blogokat keresnek a hibás domain nevek, 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

Weboldal Információgyűjtés

A webhelyről való információgyűjtés a célszervezet weboldalának figyelemmel kísérésére és elemzése. 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 [11]Telnet vagy böngésző. Ezen felül szofisztikált segédprogramokat is minta Netcraft[12] ami összegyűjti a weboldal adatait, például az IP címet, a domain tulajdonos regisztrált nevét és címét, a domain nevet, 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 szoftver-verziót az készlet szoftver-alapú webhelyen.
- **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-ket, miközben a cél webhelyet 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 az szkript[13] platform, amely szerint a cél webhely használ.

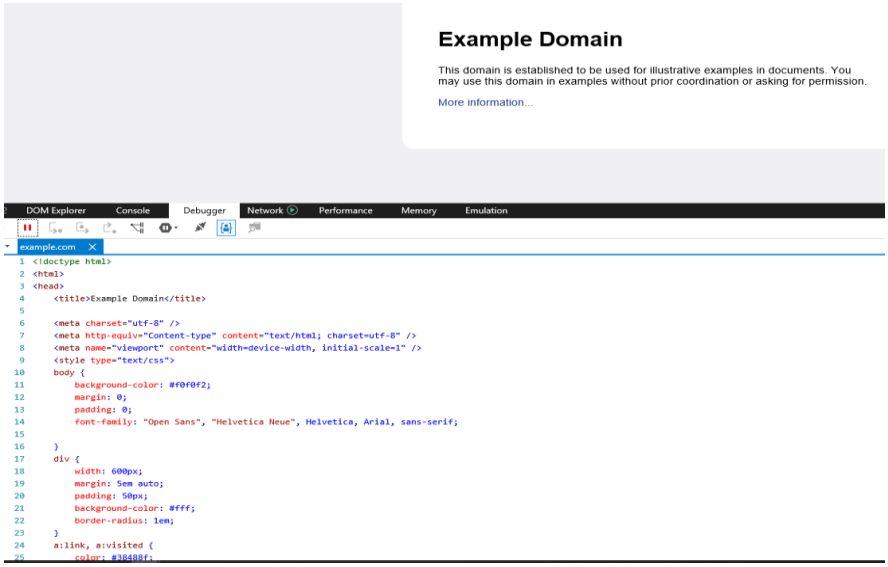
---

[11] A Telnet lényege, hogy a saját számítógépéről be tud jelentkezni egy másik (mindegy, hogy a világ melyik részén lévő) számítógépre.
[12] A Netcraft egy internetes szolgáltató cég, mely számos iparágban nyújt kiberbűnözés-megszakító szolgáltatásokat.
[13] Az informatikában a szkript névvel rövid programokat illetnek, amik gyakran egy-egy részfeladat automatizálására szolgálnak.

- **Kapcsolatfelvételi részletek és CMS[14]-adatok:** A kapcsolattartó oldalak szokásos részleteket tartalmaznak, például neveket, telefonszámokat, e-mail címeket és az adminisztrátorok vagy támogató személyek adatait. A támadó ezeket az adatokat felhasználhatja social engineering támadások végrehajtására.

A HTML[15]-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.



3. ábra HTML forráskód megjelenítése böngészőben (Saját szerkesztés)

Sütik[16] 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, domain méretére 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

---

[14] 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.
[15] A HTML (angolul: *HyperText Markup Language)* egy leíró nyelv, melyet weboldalak készítéséhez fejlesztettek ki.
[16] 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.

a cél webhelyen a robots.txt fájl található a gyökérkönyvtárban, a könyvtárak felsorolásával a bejárások megakadályozása érdekében.

Teljes webhely tükrözése

A webhely tükrözésnél az eredeti webhely pontos mását vagy klónját hozzák létre. A felhasználók a weboldalak másolatát a HTTrack Web Site Copier és az NCollector Studio tükröző tolljaival is elvégezhetik. Ezek az toolok letöltik a weboldalt egy helyi könyvtárba, rekurzív módon felépítve az összesen mappát, HTML, képek, flash, videók és egyéb fájlok a webszerverről egy másikra 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 adni a webszervernek

Metaadatok kibontása nyilvános dokumentumokból

A hasznos információk találhatók a célszervezet weboldalán pdf[17] dokumentumok, Microsoft Word[18] fájlok és egyéb formátumok formájában. Képesnek kell lenni az értékes adatok kinyerésére ideértve a metaadatokat és az ilyen dokumentumokból rejtett információkat is. Elsősorban rejtett információkat tartalmaz az elemzés céljából elemezhető nyilvános dokumentumokról, például az oldal címe, leírása, kulcsszavak, a létrehozási / módosítási adatok és a tartalom ideje, felhasználási címek és a célszervezet alkalmazottai e-mail címei.
A metaadat-kibontó segédprogramok automatikusan kinyerik a kritikus információkat, amelyek magukban foglalják az ügyfelek felhasználónevét, az operációs rendszereket (a kihasználások operációs rendszerekre vonatkoznak), e-mail címeket, a használt szoftverek listáját (verzió és típus), az szerverek és a dokumentumok létrehozását/módosítását dátumának, a weboldal szerzőinek listáját és így tovább.

E-mail Információgyűjtés

Az e-mail kommunikáció követése az Emailtracking[19] egy adott felhasználó e-mailjeit figyeli. Ez a fajta nyomon követés a digitális időbélyegzés révén lehetséges, amikor a célpont megkapja és megnyitja 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, Yesware, ContactMonkey 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.

---

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

- 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 a küldő
- Proxy[20] 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 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 email megnyitásához és olvasásához használt eszköz típusáról például: asztali számítógép, mobil eszköz vagy laptop.

Információ gyűjtése az E-mail fejlécből

Az e-mail fejléc tartalmazza a feladó adatait, az routing információkat[21], 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 fealdó e-mail szerverei által kapott adatok és idő
- A feladó e-mail szerverének által használt hitelesítési rendszer
- Az adatok és az üzenet elküldésének ideje,
- A mr.google.com által kiosztott egyedi szám, amely azonosítja az üzenet
- Feladó teljes nevét
- Feladó IP cím és cím, ahonnan az üzenet el lett küldve

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 levelező szerver, a feladó IP-címe és így tovább. Ezek az eszközök nem automatikusan küldik el a fájlokat, ha a címzettek megnyitják a levelet és adnak állapotinformációit arról, hogy az e-mail sikeresen kézbesítve lesz-e vagy sem. A támadók a kibontott információt használják, hogy megcélozzák a szervezetet rendszereit kártékony e-mailek küldésével.

---

[20] Számítógép-hálózatokban proxynak, helyesebben proxy szervernek 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.

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

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 az információ egynél több tool segítségével is kinyerhető, akkor megbízhatóbbak az információk. [6] [7]

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 domain nevet, egy IP cím blokkot vagy egy autonóm rendszert. Ez a protokoll a 43-as porton (TCP[22]) levő kérésekre vonatkozik. A regionális internetes nyilvántartások (RIR[23]) fenntartják a Whois-adatbázisokat, melyek a domaintulajdonosok személyes adatait tartalmazzák. Minden egyes erőforrás esetében a Whois-adatbázis szöveges nyilvántartásokat tartalmaz magáról az erőforrásról, valamint a meghatalmazottakról, regisztrálókról, valamint az adminisztrátori információkról (létrehozás és lejárati dátum).
Parancsa:

```
# whois example.com
```

A Whois-lekérdezés a következő információkat adja vissza:

- Domain név részletei
- Domain tulajdonos kapcsolattartási adatait
- Domain név szerverek
- Lejárati rekordok
- Utoljára frissített rekordok
- Domain létrehozásának dátuma

A támadó lekérdezi a Whois adatbázis-kiszolgálót, hogy információkat szerezzen a céltartomány névéről, 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 megtévesztheti a domain-tulajdonosokat social engineeringgel.

Whols keresési eredmény analízise

A Whois például a http://whols.domointools.com vagy a http://www.tamos.com segítségével segíthet a WhoIs-lookups lekérdezésekben. A domaintools.com szolgáltatás a Whols számára olyan információkat nyújt, mint például a regisztráló információ, az e-mail, az adminisztrátori kapcsolatinformáció, a létrehozott és az érvényességi idő, valamint a domain szerverek listája. A SmartWhois elérhető a http: //www.tomos webhelyen. .com megadja az inlonnatlont az anIP-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. Ezen kívül segít megtalálni a domain tulajdonosát, a tulajdonos elérhetőségét az IP-cím blokk tulajdonosát a domain regisztrált dátumát és így tovább.

---

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

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

Domain Name: EXAMPLE.NET
Registry Domain ID: 2328120_DOMAIN_NET-VRSN
Registrar WHOIS Server: whois.iana.org
Registrar URL: http://res-dom.iana.org
Updated Date: 2018-08-31T07:04:10Z
Creation Date: 1995-08-31T04:00:00Z
Registry Expiry Date: 2019-08-30T04:00:00Z
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

DNS-információk kibontása

Domain Name System információk kibontása információt szolgáltat a DNS zónaadatokról. 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-ra vonatkozó következő rekordok meghatározásában:

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 rendszergazdájának e-mail-címe, a tartomány sorozatszáma, a zóna frissítési 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-lekérdezéseknél 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)

4. ábra DNS rekordok [8]

Az DNS lekérdező toolok, (például a http://www.dnsstuff .com) és a DNS Rekordok (http://network-tools.com) lehetővé teszik a felhasználó számára az DNS adatok információgyűjtésének végrehajtását. A DNSstuff információkat gyűjt az IP-címekről, e-mail kiszolgáló-kiterjesztésekről, DNSlookup-okról, Whois-keresésekről és így tovább. Ha a célhálózat lehetővé teszi az ismeretlen, jogosulatlan felhasználók számára az DNS-zónaadatok továbbítását, akkor a támadónak könnyű megismerkednie az DNS-ról 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 a 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 domain név mellett bármilyen lehetőséget megadna, a dig parancs csak a domain A rekordját adja vissza. Bármely más DNS-rekordtípust szükséges megadható a típus opció a parancssorban.

```
# dig example .com
; <<>> DiG 9.8.4-rpz2+rl005.12-P1 <<>> example .com
„ global options: +cmd
„ Got answer:
„ ->>HEADER<<- opcode : QUERY, status: NOERROR, id : 3786
„ flags: qr rd ra; QUERY: l, ANSWER : l, 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 20 08:53:09 2013
„ MSG SIZE      rcvd : 45
```

dnsenum

Információkat gyűjthetünk egy DNS-kiszolgálótól a dnsenum segítségével. A DNS az összegyűjthető 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 ki azok hálózati tartományait.
- Fordított keresést végez a hálózati tartományokban.
- Szálakat használ a különböző lekérdezések feldolgozásához.

Parancsa:

```
# dnsenum example.com
```

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

```
dnsenum.pl 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
Information Gathering
[
```

Fierce

A Fierce tool egy DNS-felsoroló tool, amely több technikát használ az összes megkereséséhez a cél IP címeinek és hosztneveinek. Úgy működik, hogy először lekérdezi a rendszer DNS-kiszolgálója a cél-DNS-kiszolgálóhoz; ezután a cél-DNS-kiszolgálót használja. Azt támogatja a felhasználó által megadott szavak listáját az aldomainnevek megtalálására. Ezt megteszi rekurzív módon mindaddig, amíg az összes szólista elem nem lesz tesztelve. A fierce fő jellemzője, hogy nem szomszédos IP-helyek és hosztnevek keresésére használható meghatározott tartományok ellen.

```
# fierce -h
# fierce -dns example.com -threads 3
```

Dmitrij

A DMitry (mélyreható információgyűjtő tool) minden egyben információ gyűjtő tool. A következő információk összegyűjtésére használható:

- A hoszt Whois-rekordja az IP-cím vagy domain név használatával
- Gazdainformációk a Netcraft.com webhelyről
- Aldomainek a céltartományban

- A céltartomány e-mail címe
- Megnyitja, szűri vagy zárja a portok listáját a célgépen a portkeresés

```
# dmitry -iwnse targethost
# dmitry -p targethost -f -b
```

KÖVETKEZTETÉSEK

A kiberműveletekben és informatikában az információgyűjtési tevékenységek azonosítják a szervezetekhez kacsolódó, 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 illetve vizsgálata olyan fontos elemek, melynek részletes tanulmányozásával Penetrációs tesztünk kezdő fázisa elindítható és jelentős eredmények érhetőek 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.

FELHASZNÁLT IRODALOM

[1] [. P. István, „Basic of cybersecurity penetration test,” *Hadmérnök ISSN1788-1929*, pp. 435-442, september 2018.

[2] [. S.-P. Oriyano, Certified Etichal Hacker, ISBN-10: 1119252245 , ISBN-13: 978-1119252245, 2016..

[3] [. G. Search, „ Google Search: a keresési operátorok teljes listája https://thepitch.hu/google-keresesi-operatorok-listaja/,” (letöltve 2019.08.16).

[4] [. G. s. keresés, „Google speciális keresés https://www.google.com/advanced_search,” (letöltve 2019.08.10.).

[5] [. S. forrás.

[6] T. H. S. A. [6] LEE A, Kali Linux – Assuring Security by Penetration Testing, ISBN 978-1-84951-948-9; pp. 89-102., Birmingham, 2014.

[7] [. R. W. BEGGS:, Mastering Kali Linux for Advanced Penetration Testing ISBN 978-1-78216-312-1 pp. 47-52., Birmingham, 2014.

[8] A. S. Tanenbaum, Computer Networks ISBN-10: 0132126958 ISBN-13: 978-0132126953, 2010.