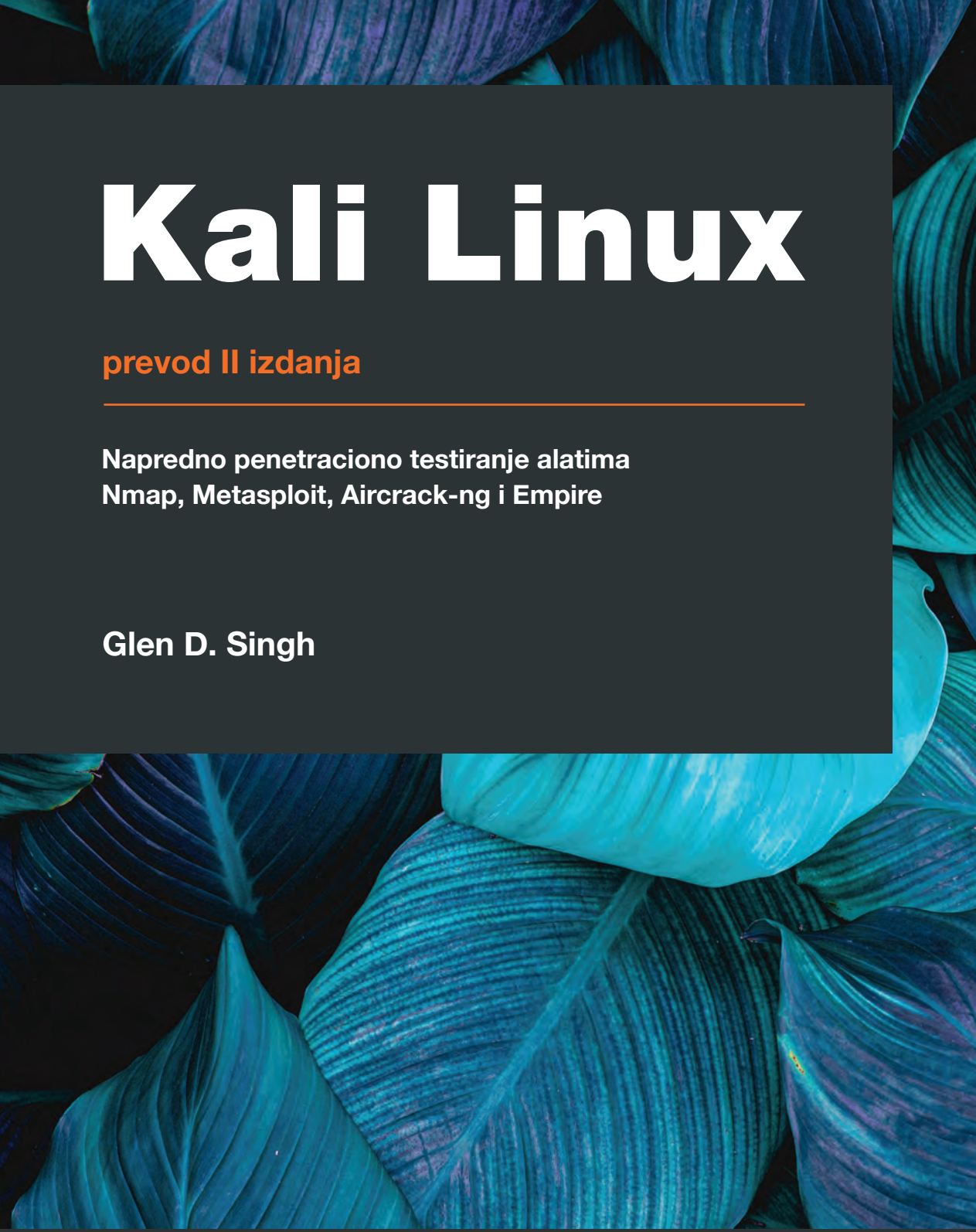
Kali Linux

prevod II izdanja

Napredno penetraciono testiranje alatima Nmap, Metasploit, Aircrack-ng i Empire

Glen D. Singh



kompjuter biblioteka

Kali Linux

Skenirajte QR kod, registrujte knjigu i osvojite nagradu

prevod II izdanja

U svetu sajber bezbednosti, Kali Linux je najpopularnija i najnaprednija Linux distribucija za penetraciono testiranje. Pomoću Kali Linuxa, profesionalac za sajber bezbednost može da izvrši napredno pen testiranje žičanih i bežičnih mreža i da otkrije i iskoristi različite propuste.

Ova knjiga je sveobuhvatan vodič za nove korisnike Kali Linuxa za penetraciono testiranje, koji će vas u najkraćem mogućem roku osposobiti za rad. Naučićete da postavite laboratoriju i istražite osnovne koncepte penetracionog testiranja. Fokus ove knjige je prikupljanje informacija i razni alati za procenu ranjivosti koje zatičemo u Kali Linux paketu. Naučićete da otkrijete ciljne sisteme na mreži, da identifikujete bezbednosne propuste na uređajima, da iskoristite bezbednosne slabosti i dobijete pristup mrežama, da podesite operacije Command i Control (C2) i da izvršite penetraciono testiranje veb aplikacija. Uz ovo ažurirano drugo izdanje, naučićete da kompromitujete Active Directory i da koristite mreže preduzeća. Na kraju knjige je predstavljena najbolja praksa za izvršavanje kompleksnih tehnika penetracionog testiranja veba u okruženju visoke bezbednosti.

Uz ovaj udžbenik ćete ovladati veštinama neophodnim za napredno penetraciono testiranje mreža pomoću Kali Linuxa.

Naučite:

- Osnove etičkog hakovanja
- Instalaciju i konfiguraciju Kali Linuxa
- Tehnike otkrivanja elemenata postavke i mreže
- Da koristite poverenje u servise domena Active Directory
- Da vršite procenu ranjivosti
- Da vršite naprednu eksploataciju tehnikama Command and Control (C2).
- Primenu naprednih tehnika bežičnog hakovanja
- Korišćenje ranjivih veb aplikacija

ISBN: 978-86-7310-585-7

Kali Linux

prevod II izdanja

NAPREDNO PENETRACIONO TESTIRANJE ALATIMA NMAP, METASPLOIT, AIRCRACK-NG I EMPIRE

Glen D. Singh

kompjuter biblioteka

Packt›

Izdavač:

kompjuter biblioteka

Obalskih radnika 4a, Beograd

Tel: 011/2520272

e-mail: kombib@gmail.com

internet: www.kombib.rs

Urednik: Mihailo J. Šolajić

Za izdavača, direktor:
Mihailo J. Šolajić

Autor: Glen D. Singh

Prevod: Slavica Prudkov

Lektura: Nemanja Lukić

Slog: Zvonko Aleksić

Znak Kompjuter biblioteke:
Miloš Milosavljević

Štampa: „Pekograf“, Zemun

Tiraž: 500

Godina izdanja: 2023.

Broj knjige: 562

Izdanje: Prvo

ISBN: 978-86-7310-585-7

The Ultimate Kali Linux Book
Second Edition

Glen D. Singh

ISBN 978-1-80181-893-3

CIP - Каталогизација у публикацији
Народна библиотека Србије, Београд

004.7.056.5

СИНГ, Глен Д.
Kali linux: Napredno penetraciono testiranje alatima Nmap, Metasploit, Aircrack-NG I Empire / Glen D. Singh; prevod 2. izd. [Slavica Prudkov]. - Izd. 1. - Beograd: Kompjuter biblioteka, 2023 (Zemun : Pekograf). - XXII, 711 str. : ilustr. ; 25 cm. - (Kompjuter biblioteka ; br. knj. 562)

Prevod dela: The Ultimate Kali Linux Book. - Tiraž 500. -
O autorima: str. III. -
Registar.

ISBN 978-86-7310-585-7
a) Рачунарске мреже -- Заштита

COBISS.SR-ID 108376585

O AUTORU

Glen D. Singh je instruktor za sajber bezbednost i autor InfoSec-a. Njegove oblasti stručnosti su operacije sajber bezbednosti, ofanzivne bezbednosne taktike i umrežavanje preduzeća. Ima mnogo sertifikata, uključujući CEH, CHFI, PAWSP i 3xCCNA (CyberOps, bezbednost i rutiranje i svičing).

Glen voli da podučava druge i da deli svoje bogato znanje i iskustvo. Napisao je mnoge knjige koje se fokusiraju na otkrivanje ranjivosti i iskorišćavanje, otkrivanje pretnji, analizu upada, reagovanje na incidente, implementaciju bezbednosnih rešenja i umrežavanje preduzeća. Veoma je ambiciozan i strastven je u širenju svesti o sajber bezbednosti u svojoj domovini, Trinidadu i Tobagou.

Želim da zahvalim Bogu, čuvaru univerzuma, za sve Njegove božanske blagodati i vođstvo. Takođe bih želeo da zahvalim Rahulu Nairu, Sayali Pingale, Rahulu D'souzi, Neilu D'mellou i divnom timu u Packt Publishing-u, koji mi je pružio neverovatnu podršku tokom ovog putovanja. Tehničkom recenzentu Rishalinu Pillayu, hvala vam na izvanrednom doprinosu da ovo bude neverovatna knjiga.

O RECENZENTU

Rishalin Pillay ima preko 12 godina iskustva u sajber bezbednosti i stekao je veštine kao konsultant za kompanije Fortune 500 tokom učešća u projektima, izvršavanja zadataka u projektovanju, implementaciji i analizi ranjivosti mreže. Poseduje mnoge sertifikate koji dokazuju njegovo znanje i stručnost u oblasti sajber bezbednosti, od proizvođača kao što su ISC2, Cisco, Juniper, Check Point, Microsoft i CompTIA. Rishalin trenutno radi u velikoj softverskoj kompaniji kao inženjer sajber bezbednosti.

Želeo bih da zahvalim Glenu što mi je dozvolio da pregledam ovu knjigu. Za izdavački tim i Packt tim – hvala vam što ste mi dali priliku da recenziram ovu knjigu. Uvek je zadovoljstvo raditi sa vama.

Mojoj supruzi Rubleen i mom sinu Kaiju, hvala vam za svu podršku. Bez vas bi život bio zaista dosadan - volim vas.

Kratak sadržaj

Sadržaj

POGLAVLJE 3

DEO 2
Izviđanje i penetraciono testiranje mreže 109

POGLAVLJE 4

POGLAVLJE 10

POGLAVLJE 11

POGLAVLJE 12

POGLAVLJE 16

POGLAVLJE 17

Predgovor

Kada kročite u oblast etičkog hakovanja i penetracionog testiranja u industriji sajber bezbednosti, često ćete čuti za čuvenu Linux distribuciju poznatu kao Kali Linux. Kali Linux je Linux distribucija za penetraciono testiranje koja je izgrađena da podrži potrebe profesionalaca za sajber bezbednošću tokom svake faze pen testa. Kao autor informacione bezbednosti, trener za sajber bezbednost i predavač, čuo sam od mnogih ljudi u industriji, pa čak i od studenata, o važnosti pronalaženja knjige koja vodi čitaoca ka temeljnom razumevanju izvršenja penetracionog testiranja, pristupom korak po korak, korišćenjem Kali Linuxa. To mi je bila motivacija i inspiracija da kreiram ultimativnu knjigu koju će svi lako razumeti i koja će pomoći čitaocima da nakon učenja uz nju postanu stručnjaci u upotrebi najnovijih alata i tehnika.

Tokom godina, istraživao sam i kreirao mnogo sadržaja u vezi sa sajber bezbednošću, a ono što je najvažnije, kada ste etički haker i pen tester, je da uvek budete u toku i da znate kako da otkrijete najnovije bezbednosne propuste. Kao rezultat toga, etički hakeri i pen testeri moraju da budu opremljeni najnovijim znanjem, veštinama i alatima da efikasno otkriju i iskoriste skrivene bezbednosne propuste na ciljnim sistemima i mrežama. Tokom procesa pisanja ove knjige, koristio sam pristup koji je usredsređen na učenike i prilagođen učenicima, što olakšava da razumete najsloženije teme, terminologije i zašto postoji potreba da se testiraju bezbednosni propusti na sistemu i mreži.

Na početku ove knjige uvodimo vas u razumevanje načina razmišljanja aktera pretnji kao što je haker i upoređujemo način razmišljanja hakera sa načinom razmišljanja penetracionih testera. Važno je razumeti kako akter pretnje razmišlja i šta mu je najvrednije. Iako pen testeri mogu da imaju sličan način razmišljanja, njihov cilj je da otkriju i pomognu u rešavanju bezbednosnih propusta pre nego što dođe do pravog sajber napada na organizaciju. Štaviše, naučićete kako da kreirate laboratorijsko okruženje korišćenjem tehnologije virtuelizacije da biste smanjili troškove kupovine opreme. Laboratorijsko okruženje će oponašati

mrežu sa ranjivim sistemima i serverima veb aplikacija. Pored toga, kreirana je potpuno zakrpljena laboratorija Windows Active Directory kako bismo demonstrirali bezbednosne propuste pronađene u okviru Windows domena.

Uskoro ćete naučiti da izvršite prikupljanje obaveštajnih podataka o organizacijama u stvarnom svetu, korišćenjem popularnih alata i strategija za izviđanje i prikupljanje informacija. Učenje o etičkom hakovanju i penetracionom testiranju ne bi bilo potpuno bez učenja kako da izvršite procenu ranjivosti korišćenjem standardnih alata u industriji. Štaviše, provešćete neko vreme učeći kako da iskoristite uobičajene bezbednosne propuste. Nakon faze iskorišćavanja, bićete izloženi post-eksploatacionim tehnikama i naučićete da podesite Command and Control (C2) operacije za održavanje pristupa na ugroženoj mreži.

U ovo izdanje su uključene nove teme, kao što su nabrajanje i iskorišćavanje Active Directory-a, jer mnoge organizacije imaju Windows okruženje sa pokrenutim servisom Active Directory. Naučićete da zloupotrebite poverenje servisa Active Directory i preuzmete Windows domen. Uključeni su novi bežični napadi kako bismo pomogli potencijalnim pen testerima da steknu veštine za testiranje bezbednosnih propusta na bežičnim mrežama, kao što je iskorišćavanje bežičnog bezbednosnog standarda WPA3. Konačno, u poslednjem odeljku, uključili smo tehnike za otkrivanje i iskorišćavanje veb aplikacija i izvođenje tehnika društvenog inženjeringa i napada.

Do kraja ove knjige, vodićemo vas kroz neverovatno putovanje, od početnika do stručnjaka u smislu učenja, razumevanja i razvoja veština u etičkom hakovanju i penetracionom testiranju, kao ambicioznog profesionalca za sajber bezbednost.

Kome je ova knjiga namenjena

Ova knjiga je dizajnirana za studente, trenere, predavače, IT stručnjake i one koji jednostavno imaju interes da nauče etičko hakovanje, penetraciono testiranje i sajber bezbednost. Ova knjiga može da se koristiti kao vodič za samostalno učenje i u okviru obuke u učionici o temama koje obuhvataju otkrivanje i iskorišćavanje ranjivosti, tehnike etičkog hakovanja i strategije penetracionog testiranja.

Bilo da ste novi u oblasti sajber bezbednosti ili ste iskusan profesionalac u industriji, ova knjiga ima da ponudi svakome ponešto i sadrži mnogo toga za učenje da biste stekli praktično iskustvo i započeli posao kao etički haker i penetracioni tester.

Šta je obuhvaćeno ovom knjigom

Poglavlje 1, Uvod u etičko hakovanje - upoznajemo vas sa konceptima etičkog hakovanja i tehnikama i strategijama penetracionog testiranja.

Poglavlje 2, Izgradnja laboratorije za penetraciono testiranje - fokusiramo se na to kako da koristite tehnologije virtuelizacije za kreiranje personalizovanog virtuelnog laboratorijskog okruženja, da biste vežbali svoje veštine u bezbednom okruženju.

Poglavlje 3, Podešavanje za napredne tehnike hakovanja - fokusiramo se na to kako da podesite Windows Active Directory laboratoriju i bežično okruženje preduzeća za obavljanje naprednih tehnika penetracionog testiranja.

Poglavlje 4, Izviđanje i snimanje sistema - upoznajemo vas sa značajem izviđanja i tehnikama koje se koriste tokom penetracionog testiranja.

Poglavlje 5, Istraživanje aktivnog prikupljanja informacija - fokusiramo se na obavljanje aktivnog prikupljanja informacija o ciljevima i uređajima za profilisanje.

Poglavlje 6, Izvršenje procene ranjivosti - fokusiramo se na to kako da otkrijete ranjivosti korišćenjem popularnih automatizovanih alata za procenu ranjivosti.

Poglavlje 7, Razumevanje penetracionog testiranja - fokusiramo se na istraživanje osnova penetracionog testiranja mreže, tehnika izbegavanja malvera i rada sa bežičnim mrežnim adapterima.

Poglavlje 8, Izvršenje penetracionog testiranja mreže - fokusiramo se na otkrivanje i iskorišćavanje bezbednosnih ranjivosti koje se obično nalaze u stvarnom svetu.

Poglavlje 9, Napredno penetraciono testiranje mreže – posle eksploatacije - upoznajemo vas sa tehnikama i strategijama nakon eksploatacije.

Poglavlje 10, Active Directory napadi - fokusiramo se na iskorišćavanje poverenja Windows Active Directory Domain Servisa na mreži.

Poglavlje 11, Napredni Active Directory napadi - fokusiramo se na izvršenje napredne eksploatacije Active Directory-a, vršeći i bočno i vertikalno pomeranje i preuzimanje domena.

Poglavlje 12, Command and Control taktike - upoznajemo vas sa značajem i tehnikama za uspostavljanje C2 tokom penetracionog testiranja.

Poglavlje 13, Napredno bežično penetraciono testiranje - fokusiramo se na razumevanje bežične komunikacije, ranjivosti i tehnika iskorišćavanja.

Poglavlje 14, Izvršenje napada na strani klijenta – društveni inženjering - upoznajemo vas sa načinom korišćenja tehnika društvenog inženjeringa za kompromitovanje ljudskog uma tokom sajber napada.

Poglavlje 15, Razumevanje bezbednosti aplikacija na veb sajtu - fokusiramo se na otkrivanje bezbednosnih rizika veb aplikacija, koji su opisani na OWASP Top 10 2021 listi bezbednosnih propusta.

Poglavlje 16, Napredno penetraciono testiranje veb sajtova - fokusiramo se na izvršenje bezbednosnog testiranja veb aplikacija za otkrivanje i iskorišćavanje bezbednosnih propusta.

Poglavlje 17, Najbolja praksa za stvarni svet - pružamo smernice za ambiciozne etičke hakere i pen testere kako bismo osigurali da, nakon što završite ovu knjigu, imate bogato znanje i da možete da se prilagodite dobroj praksi u industriji.

Da biste izvukli maksimum iz ove knjige

Da biste izvukli maksimum iz ove knjige, preporučujemo da imate čvrstu osnovu o umrežavanju, kao što su razumevanje uobičajenih mrežnih i aplikativnih protokola TCP/IP, IP adresiranje, koncepti rutiranja i svičinga, kao i uloge i funkcije mrežnih uređaja i sigurnosnih uređaja. Poznavanje tehnologija virtuelizacije, kao što su hipervizori i njihove komponente biće od koristi, jer je većina laboratorija izgrađena u virtuelizovanom okruženju kako bi se smanjila potreba za kupovinom dodatnih sistema.

Softver/hardver obuhvaćen u knjizi	Zahtevi za OS
Oracle VM VirtualBox 6.1.24	Windows 10 Enterprise
Oracle VM VirtualBox Extension Pack	Windows Server 2019
OWASP Juice Shop	Kali Linux 2021.2
FreeRadius 3.0	Ubuntu Server 20.04.2
Osintgram	Metasploitable 2
Sherlock	Metasploitable 3
S3Scanner	OWASP Broken Web Applications
Nessus	
PacketWhisper	
Greenbone Vulnerability Manager	
Python 2.7.28	
Hashcat	
PowerView	
Bloodhound	
MITM6	
Mimikatz	
Empire 4	
Starkiller	
Airgeddon	
Alfa AWUS036NHA High Gain Wireless B/G/N USB Adapter	
Alfa AWUS036ACH Long-Range Dual-Band AC1200 Wireless USB 3.0 Wi-Fi Adapter	

Sve laboratorije i vežbe su izgrađene na sistemu sa pokrenutimWindows 10 Home operativnim sistemom, višejezgarnim procesorom sa omogućenom virtuelizacijom, 16 GB RAM-a i 300 GB slobodnog prostora za skladištenje za virtuelne mašine. Biće potreban namenski GPU da bi se izvršilo razbijanje lozinke pomoću

alatke zasnovane na GPU-u i dva bežična mrežna adaptera koji podržavaju injektiranje paketa i rade na 2,4 i 5 GHz.

Oracle VM VirtualBox je bio preferiran izbor hipervizora jer pruža bolje mogućnosti virtuelnog umrežavanja u poređenju sa drugim rešenjima. Međutim, ako više volite da koristite neki drugi hipervizorski proizvod, kao što je VMware, možete to učiniti, ali imajte na umu činjenicu da su sve laboratorije u ovoj knjizi završene i testirane pomoću Oracle VM VirtualBox-a.

> **Napomena**
>
> Dok su sadržaj i laboratorije, koji se nalaze u ovoj knjizi, zasnovani na Kali Linuxu 2021, koncepti i vežbe su primenljivi i na novije verzije Kali Linuxa koje će biti objavljene u budućnosti.

Nakon što završite čitanje ove knjige, opremljeni maštom i novootkrivenim veštinama, pokušajte da kreirate dodatne laboratorijske scenarije, pa čak i da proširite svoje laboratorijsko okruženje dodavanjem virtuelnih mašina kako biste poboljšali svoje veštine. To će vam pomoći da nastavite sa učenjem i dalje razvijate veštine kao ambiciozan etički haker i penetracioni tester.

Preuzmite slike u boji

Takođe pružamo PDF fajl koji sadrži slike u boji snimaka ekrana/dijagrama koji se nalaze u ovoj knjizi. Možete ga preuzeti ovde:https://static.packt-cdn.com/downloads/9781801818933_ColorImages.pdf.

Korišćene konvencije

Postoji veliki broj tekstualnih konvencija koje se koriste u ovoj knjizi.

Kod u tekstu: označava kodne reči u tekstu, nazive tabela baze podataka, nazive direktorijuma, nazive fajlova, ekstenzije fajlova, nazive putanja, lažne URL adrese, korisnički unos i Twitter postove. Na primer: „Da biste isključili OWASP BWA virtuelnu mašinu, koristite komandu sudo halt“.

Blok koda je postavljen na sledeći način:

```
C:\Users\Slayer> cd .vagrant.d\boxes
C:\Users\Slayer\.vagrant.d\boxes> vagrant init metasploitable3-
win2k8
C:\Users\Slayer\.vagrant.d\boxes> vagrant up
```

Podebljana slova: označavaju novi termin, važnu reč ili reči koje vidite na ekranu (na primer, reči u menijima ili okvirima za dijalog koje se pojavljuju u tekstu). Na primer: „Kliknite Exit da biste zatvorili prozor Microsoft Azure Active Directory Connect kada se konfiguracija završi."

Saveti ili važne napomene
Prikazani su ovako.

Odricanje od odgovornosti

Informacije u ovoj knjizi namenjene su da se koriste samo na etički način. Nemojte koristiti nikakve informacije iz knjige ako nemate pismenu dozvolu vlasnika opreme. Ako izvršite nezakonite radnje, verovatno ćete biti uhapšeni i krivično gonjeni. Ni Packt Publishing ni autor ove knjige ne preuzimaju nikakvu odgovornost ako zloupotrebite bilo koju informaciju sadržanu u knjizi. Ove informacije se mogu koristiti samo tokom testiranja okruženja uz odgovarajuće pismeno ovlašćenje odgovarajućih odgovornih osoba.

Postanite član Kompjuter biblioteke

Kupovinom jedne naše knjige stekli ste pravo da postanete član Kompjuter biblioteke. Kao član možete da kupujete knjige u pretplati sa 40% popusta i učestvujete u akcijama kada ostvarujete popuste na sva naša izdanja. Potrebno je samo da se prijavite preko formulara na našem sajtu. Link za prijavu: http://bit.ly/2TxekSa

Skenirajte QR kod
registrujte knjigu
i osvojite nagradu

DEO 1

Penetraciono testiranje

U ovom odeljku ćete učiti o važnosti razumevanja potrebe za penetracionim testiranjem u okviru sajber bezbednosti dok učite da izgradite efikasno laboratorijsko okruženje za penetraciono testiranje.

Ovaj deo knjige sastoji se od sledećih poglavlja:

- Poglavlje 1, Uvod u etičko hakovanje
- Poglavlje 2, Izgradnja laboratorije za penetraciono testiranje
- Poglavlje 3, Podešavanje za napredne tehnike hakovanja

1

Uvod u etičko hakovanje

Sajber bezbednost je jedna od oblasti koje se najbrže razvijaju u industriji **informacionih tehnologija** (**IT**). Svakog dana profesionalci za bezbednost velikom brzinom otkrivaju nove pretnje i pretnje u nastajanju, a napadači ugrožavaju resurse organizacija. Zbog ovih pretnji u digitalnom svetu, u mnogim organizacijama se stvaraju nove profesije za ljude koji mogu da pomognu u zaštiti resursa. Ova knjiga je osmišljena sa namerom da vam pruži znanje, mudrost i veštine koje su potrebne ambicioznom penetracionom testeru kako bi bio uspešan u industriji sajber bezbednosti. Penetracioni tester je profesionalac za sajber bezbednost koji ima veštine hakera; organizacija ih angažuje da izvode simulacije sajber-napada u stvarnom svetu na mrežnu infrastrukturu organizacije sa ciljem otkrivanja i iskorišćavanja bezbednosnih propusta. To omogućava organizaciji da otkrije bezbednosne propuste i implementira kontrolu bezbednosti za sprečavanje i ublažavanje stvarnih sajber napada.

Tokom čitavog kursa u ovoj knjizi, u vežbama penetracionog testiranja, učićete kako da koristite jednu od najpopularnijih distribucija Linuxa u industriji sajber bezbednosti, za simulaciju sajber-napada u stvarnom svetu da biste otkrili i iskoristili bezbednosne slabosti na sistemima i mrežama. Kali Linux operativni sistem ima mnogo unapred instaliranih Linux paketa/aplikacija koje su u redovnoj upotrebi u industriji sajber bezbednosti, pa je to arsenal ispunjen svime što će vam biti potrebno. Koristićemo pristup usredsređen na studente, ispunjen sa mnogo praktičnih vežbi, od početničkog do srednjeg nivoa, pa do naprednih tema i tehnika, uključujući angažovanje crvenog tima.

U ovom poglavlju ćete steći opširno razumevanje različitih karakteristika različitih napadača, njihovih namera i motiva koji stoje iza sajber-napada na njihove mete. Zatim ćete učiti o ključnim faktorima koji su važni za napadače i koji određuju nivo složenosti kompromitovanja sistema u poređenju sa profesionalcima za sajber bezbednost, kao što su etički hakeri i penetracioni testeri, koji su angažovani da otkriju i iskoriste skrivene bezbednosne slabosti unutar ciljne organizacije. Takođe ćete otkriti potrebu za penetracionim testiranjem, njegovim fazama i pristupima koje koriste iskusni profesionalci u industriji. Na kraju, istražićete **Cyber Kill Chain** radni okvir, kako ga stručnjaci za sajber bezbednost koriste da spreče sajber napade i kako se svaka faza može uskladiti sa penetracionim testiranjem.

Ovim poglavljem obuhvaćene su sledeće teme:

- Identifikovanje napadača i njihove namere
- Razumevanje šta je važno napadačima
- Otkrivanje terminologije sajber bezbednosti
- Istraživanje potrebe za penetracionim testiranjem i njegove faze
- Razumevanje pristupa penetracionom testiranju
- Istraživanje faza hakovanja
- Razumevanje Cyber Kill Chain radnog okvira

Nadam se da ste uzbuđeni, kao i ja, što ćete započeti ovo putovanje. Počnimo!

Identifikovanje napadača i njihove namere

Širom sveta postoji ogromna potražnja za profesionalcima za sajber bezbednost, jer mnoge organizacije počinju da shvataju potrebu za kvalifikovanim profesionalcima koji bi im pomogli da obezbede i zaštite svoju imovinu. Jedan od najvrednijih resursa za svaku organizaciju su podaci. **Napadači,** kao što su hakeri, poboljšavaju svoj plan igre i hakovanje je postalo posao na dark vebu. Napadači koriste napredne i sofisticirane napade i pretnje da bi kompromitovali ciljne sisteme i mreže, ukrali njihove podatke primenom različitih tehnika eksfiltracije, da bi zaobišli detekciju pretnji i prodali ukradene podatke na dark vebu.

Pre mnogo godina, hakeri su ručno obavljali ove zadatke; međutim, u današnje vreme oni su kreirali napredne pretnje kao što je **ucenjivački napad (eng. ransomware)**, koji je kripto-malver dizajniran da kompromituje ranjive sisteme. Kada je sistem zaražen ransomverom, on će šifrovati sve podatke na lokalnim diskovima osim operativnog sistema. Pored toga, ransomver ima mogućnost da kompromituje bilo koje cloud skladište koje je povezano sa zaraženim sistemom. Na primer, zamislite da sistem korisnika ima Google Drive, Microsoft OneDrive ili čak Dropbox i da se podaci stalno sinhronizuju. Ako je sistem zaražen, infekcija bi takođe mogla da utiče na podatke u cloud skladištu. Međutim, neki cloud provajderi imaju ugrađenu zaštitu od ovih vrsta pretnji.

Ransomver šifruje podatke i drži ih kao taoce dok na radnoj površini žrtve prikazuje prozor za plaćanje u kom se zahteva plaćanje za vraćanje podataka. Za to vreme, odgovorni napadač takođe eksfiltrira podatke i prodaje ih na dark vebu.

Važna napomena

Ne preporučuje se plaćanje otkupnine, jer nema garancije da će napadači objaviti podatke. Ako napadači daju ključ za dešifrovanje, on možda nije pravi. Štaviše, bivši član Microsoft **Detection and Response Team-a** (**DART**), Rishalin Pillay, pomenuo je da je tokom svog rada u Microsoftu video kako napadači „mogu" da daju ključ za dešifrovanje žrtvama, međutim, oni 110% implantiraju dodatni malver da bi se kasnije vratili radi veće zarade. U suštini, ciljna organizacija postaje „krava muzara" za napadača (grupu napadača).

Do sada smo našli samo na jednu vrstu napadača, hakera. Međutim, postoje i druge vrste napadača koji učestvuju u sajber napadima. Bićete iznenađeni raznovrsnošću ljudi koji su uključeni u hakovanje. Pogledajmo listu najpopularnijih napadača u industriji:

- **Haker amater (eng. script kiddie) –** Haker amater je uobičajen tip napadača koji nije obavezno mlada odrasla osoba ili dete. Umesto toga, to je neko ko ne razume tehničke detalje sajber bezbednosti da bi samostalno izvršio sajber napad. Međutim, haker amater obično prati uputstva ili tutorijale pravih hakera kako bi izvršio sopstvene napade na sistem ili mrežu. Iako možda mislite da je haker amater bezopasan, jer osoba nema potrebno znanje i veštine, on može da napravi jednaku količinu štete kao pravi haker prateći uputstva zlonamernih hakera na internetu. Ova vrsta *hakera* može da koristi alate za koje ne zna kako funkcionišu, čime nanosi veću štetu.
- **Haktivist (eng. hacktivist) –** Širom sveta postoji mnogo društvenih i političkih planova u mnogim nacijama i ima mnogo osoba i grupa koje podržavaju ili ne podržavaju njihove planove. Obično ćete naći demonstrante koji će organizovati skupove, marševe ili čak obavljati nezakonite aktivnosti kao što je uništavanje javne imovine. Postoji vrsta napadača koji koriste svoje veštine hakovanja da bi izvršili zlonamerne aktivnosti kao podršku političkoj ili društvenoj agendi. Tu osobu obično nazivamo haktivistom. Dok neki haktivisti koriste svoje veštine hakovanja za *dobra* dela, imajte na umu da je hakovanje i dalje nezakonit čin i da se napadač može suočiti sa pravnim postupkom.
- **Insajder (eng. insider) –** Mnogi napadači su shvatili da je izazovnije provaliti u organizaciju preko interneta i da je to lakše uraditi iznutra, na internoj mreži cilja. Neki napadači će kreirati lažni identitet i biografiju sa namerom da se prijave za posao u ciljnoj organizaciji i postanu zaposleni. Kada ova vrsta napadača postane zaposleni, osoba će imati pristup internoj mreži i steći bolji uvid u arhitekturu mreže i bezbednosne propuste. Stoga, ovaj tip napadača može da implementira mrežne implante na mreži i da kreira tajna vrata (eng. backdoor) za daljinski pristup kritičnim sistemima. Ovaj tip napadača je poznat kao insajder.

- **Pod pokroviteljstvom države (eng. state-sponsored) –** Dok će mnoge nacije poslati svoju vojsku u rat, mnoge bitke se sada vode unutar sajber prostora. To je poznato kao sajber rat. Mnoge nacije su shvatile potrebu da izgrade odbranu kako bi zaštitile svoje građane i nacionalnu imovinu od hakera i drugih nacija sa zlonamernim namerama. Stoga će vlada jedne nacije angažovati hakere koji su odgovorni za zaštitu svoje zemlje od sajber napada i pretnji. Neke nacije koriste ovu vrstu napadača da bi prikupile obaveštajne podatke o drugim zemljama, pa čak i da kompromituju sisteme koji kontrolišu infrastrukturu javnih preduzeća ili druge važne resurse potrebne zemlji.
- **Organizovani kriminal (eng. organized crime) –** Širom sveta često čitamo i slušamo o mnogim kriminalnim sindikatima i organizovanim kriminalnim grupama. I unutar industrije sajber bezbednosti postoje kriminalne organizacije sastavljene od grupe ljudi sa istim ciljevima na umu. Svaka osoba u grupi je obično stručnjak ili ima nekoliko posebnih veština, na primer, jedna osoba može biti odgovorna za izvršenje opsežnog izviđanja cilja, dok je druga odgovorna za razvoj **Advanced Persistent Threat-a** (**APT**). Unutar ove organizovane kriminalne grupe, obično postoji osoba koja je odgovorna za finansiranje grupe kako bi se obezbedili najbolji dostupni resursi, kako bi se osiguralo da napad bude uspešan. Namera ovog tipa napadača je obično velika, kao što je krađa podataka cilja i njihova prodaja radi finansijske dobiti.
- **Black hat (crni šešir) –** Black hat haker je akter pretnje koji koristi svoje veštine iz zlonamernih razloga. Ovaj haker može biti bilo ko i njegov razlog za hakovanje sistema ili mreže može biti nasumičan. Ponekad mogu da hakuju da unište reputaciju svoje mete, da ukradu podatke ili čak kao lični izazov, da dokažu poentu, iz zabave.
- **White hat (beli šešir) –** White hat hakeri su dobri momci i devojke u industriji. Ova vrsta hakera koristi svoje veštine da pomogne organizacijama i ljudima da obezbede svoje mreže i zaštite svoju imovinu od zlonamernih hakera. Etički hakeri i penetracioni testeri su primeri white hat hakera, jer oni koriste svoje veštine da pomognu drugima na pozitivan i etički način.
- **Gray hat (sivi šešir) –** Gray hat haker je osoba koja metaforički sedi između belog i crnog šešira. To znači da gray hat haker ima veštinu hakovanja i može biti dobar momak/devojka tokom dana, kao profesionalac za sajber bezbednost, a loš momak/devojka noću koristeći svoje veštine za zlonamerne radnje.

Uz kontinuirani razvoj novih tehnologija, radoznali umovi mnogih će uvek naći način da steknu dublje razumevanje osnovnih tehnologija sistema. To često dovodi do otkrivanja bezbednosnih nedostataka u dizajnu i na kraju omogućava osobi da iskoristi ranjivost. Na kraju ovog odeljka, otkrili ste karakteristike različitih napadača i njihove namere za izvršenje sajber-napada. U sledećem odeljku ćemo detaljnije zaroniti u razumevanje onoga što je važno napadaču.

Razumevanje šta je važno napadačima

Koncept hakovanja u drugi sistem ili mrežu će mnogima uvek izgledati veoma fascinantno, dok je za druge prilično zabrinjavajuće da znaju da nivo bezbednosti nije prihvatljiv ako sistem može biti kompromitovan od strane napadača. Napadači, etički hakeri ili čak penetracioni testeri moraju da planiraju i procene vreme, resurse, složenost i vrednost hakovanja pre nego što izvrše sajber napad na sisteme ili mreže cilja.

Vreme

Važno je shvatiti koliko će vremena biti potrebno od početka prikupljanja informacija o meti do ispunjavanja ciljeva napada. Ponekad, napadaču može da bude potrebno od nekoliko dana do nekoliko meseci pažljivog planiranja sajber-napada kako bi osigurao da svaka faza bude uspešna, kada su izvršene odgovarajućim redosledom. Napadači takođe moraju da uzmu u obzir mogućnost da napad ili eksploatacija možda neće uspeti na meti i to stvara prepreku tokom procesa, što povećava vreme potrebno za postizanje ciljeva hakovanja. Ovaj koncept može da bude primenjen i na penetracione testere, jer je potrebno da odrede koliko će vremena biti potrebno da završe penetracioni test za klijenta i da prilože izveštaj sa nalazima i bezbednosnim preporukama.

Resursi

Bez pravog skupa resursa, završavanje zadatka će biti veliki izazov. Potrebno je da napadači imaju pravi skup resursa, koji mogu biti softverski i hardverski zasnovani alati. Dok vešti i iskusni hakeri mogu ručno da otkriju i iskoriste bezbednosne slabosti na sistemu, to može biti dugotrajan proces. Međutim, korišćenje pravog skupa alata može pomoći u automatizaciji ovih zadataka i skratiti vreme potrebno za pronalaženje bezbednosnih propusta i njihovu eksploataciju. Pored toga, bez odgovarajućeg skupa veština, napadač može da se suoči sa nekim izazovima u izvođenju sajber-napada. To može dovesti do dobijanja podrške dodatnih osoba sa veštinama potrebnim da pomognu i doprinesu postizanju ciljeva sajber-napada. Ponovo, ovaj koncept možemo da primenimo na profesionalce u oblasti bezbednosti, kao što su penetracioni testeri. Nemaju svi iste veštine i klijent će možda morati da angažuje tim za penetraciono testiranje.

Finansijski faktori

Drugi važan resurs su finansijski faktori. Ponekad napadaču nisu potrebni dodatni resursi i može da izvrši uspešan sajber napad i ugrozi svoje mete. Međutim, može biti trenutaka kada je potrebna dodatna softverska ili hardverska alatka da bi se osiguralo da napad bude uspešan. Posedovanje budžeta omogućava napadačima da kupe potrebna dodatna sredstva. Slično tome, poslodavci dobro finansiraju penetracione testere kako bi osigurali da imaju pristup najboljim alatima u industriji, da bi se istakli u svom poslu.

Vrednost hakovanja

Na kraju, **vrednost hakovanja (eng. hack value)** je jednostavno motivacija ili razlog za izvođenje sajber-napada na sisteme i mrežu mete. Za napadača, to je vrednost ostvarivanja ciljeva i ciljevi kompromitovanja sistema. Napadači možda neće ciljati organizaciju ako misle da nije vredno vremena, truda ili resursa da kompromituju njene sisteme. Drugi napadači mogu ciljati istu organizaciju sa drugim motivom.

Nakon što ste završili ovaj odeljak, naučili ste neke od važnih faktora za napadače, pre nego što izvedu sajber napad na organizaciju. U sledećem odeljku ćete otkriti različite ključne terminologije koje se obično koriste u industriji sajber bezbednosti.

Otkrivanje terminologije sajber bezbednosti

Tokom svog putovanja u uzbudljivoj oblasti sajber bezbednosti bićete izloženi različitim žargonima i terminologijom koja se obično nalazi u različitoj literaturi, diskusijama i resursima za učenje. Kao ambiciozan penetracioni tester, važno je da razumete i da budete svesni različitih ključnih terminologija i kako su one povezane sa penetracionim testiranjem.

Sledi lista najčešće korišćene terminologije u industriji sajber bezbednosti:

- **Resurs (eng. asset) –** U oblasti sajber bezbednosti, mi definišemo resurs kao sve što ima vrednost za organizaciju ili osobu. Resursi su sistemi unutar mreže sa kojima se može stupiti u interakciju i potencijalno izlažu mrežu ili organizaciju slabostima koje bi mogle da budu iskorišćene i daju hakerima način da eskaliraju svoje privilegije sa standardnog korisničkog pristupa na pristup na administratorskom/korenskom nivou ili da dobiju daljinski pristup mreži. Važno je napomenuti da resursi nisu, i ne bi trebalo da budu, ograničeni na tehničke sisteme. Drugi oblici resursa uključuju ljude, fizičke bezbednosne kontrole, pa čak i podatke koji se nalaze u mrežama koje želimo da zaštitimo.

Resurse možemo podeliti u tri kategorije:

i **Opipljivi**: To su fizičke stvari kao što su mrežni uređaji, računarski sistemi i uređaji.

ii **Nematerijalni**: To su stvari koje nisu u fizičkom obliku, kao što su intelektualna svojina, poslovni planovi, podaci i zapisi.

iii **Ljudi**: To su zaposleni koji vode posao ili organizaciju. Ljudi su jedno od najranjivijih resursa u oblasti sajber bezbednosti. Pored toga, organizacije bi trebalo da zaštite podatke svojih klijenata od krađe.

Kao profesionalci za sajber bezbednost, važno je da budete u stanju da identifikujete resurse i potencijalne pretnje koje im mogu naneti štetu.

- **Pretnja (eng. threat) –** U kontekstu sajber bezbednosti, pretnja je sve što ima potencijal da nanese štetu sistemu, mreži ili osobi. Bez obzira da li ste na ofanzivnoj ili defanzivnoj strani u sajber bezbednosti, važno je da budete u stanju da identifikujete pretnje. Mnoge organizacije širom sveta svakodnevno se suočavaju sa različitim vrstama pretnji i njihov tim za sajber bezbednost radi danonoćno kako bi osigurao da resursi organizacije budu zaštićeni od napadača i pretnji. Jedan od najuzbudljivijih, ali i ogromnih aspekata sajber bezbednosti je da profesionalci u industriji uvek moraju da budu korak ispred napadača kako bi brzo pronašli bezbednosne slabosti u sistemima, mrežama i aplikacijama i primenili protivmere za ublažavanje potencijalnih pretnji protiv tih resursa.

  Sve organizacije imaju resurse koje treba čuvati; sistemi, mreže i resursi organizacije uvek sadrže neku vrstu bezbednosne slabosti koju haker može da iskoristi. Pojasnimo sada šta je ranjivost.

- **Ranjivost (eng. vulnerability) –** Ranjivost je slabost ili bezbednosna greška koja postoji u tehničkim, fizičkim ili ljudskim sistemima, a koju hakeri mogu da iskoriste kako bi dobili neovlašćen pristup ili kontrolu nad sistemima unutar mreže. Uobičajene ranjivosti koje postoje u organizacijama uključuju ljudsku grešku (najveća ranjivost na globalnom nivou), pogrešnu konfiguraciju uređaja, korišćenje slabih korisničkih identifikatora, lošu programsku praksu, nezakrpljene operativne sisteme i zastarele aplikacije na host sistemima, korišćenje podrazumevanih konfiguracija na sistemima, itd.

Napadač će tražiti *najslabiju kariku*, kao što su ranjivosti koje je najlakše iskoristiti. Isti koncept važi i za penetraciono testiranje. Tokom angažmana, penetracioni tester će koristiti različite tehnike i alate za otkrivanje ranjivosti i pokušaće da iskoristi one lake, pre nego što pređe na složenije bezbednosne propuste na ciljnom sistemu.

- **Zloupotreba (eksploatacija, iskorišćavanje) (eng. exploit) –** Zloupotreba je stvar, alat ili kod koji služi za iskorišćavanje ranjivosti na sistemu. Na primer, uzmite čekić, komad drveta i ekser. Ranjivost je meka, propusna priroda drveta, a zloupotreba je čin zabijanja eksera u drvo. Kada pronađe ranjivost na sistemu, napadač ili penetracioni tester će ili razviti ili potražiti eksploataciju koja može da iskoristi bezbednosne slabosti. Važno je razumeti da bi zloupotreba trebalo da bude testirana na sistemu da bi se osiguralo da ima potencijal da bude uspešna kada je pokrene napadač. Ponekad zloupotreba može da funkcioniše na jednom sistemu, a možda neće raditi na drugom. Stoga će iskusni penetracioni testeri osigurati da se njihova zloupotreba testira i ocenjuje na osnovu njihove stope uspeha po ranjivosti.
- **Rizik (eng. risk) –** Iako može izgledati kao da su penetracioni testeri angažovani da simuliraju sajber-napade u stvarnom svetu na ciljnu organizaciju, cilj takvih angažmana je mnogo dublji nego što se čini. Na kraju penetracionog testa, stručnjak za sajber bezbednost će predstaviti sve ranjivosti i moguća rešenja da bi pomogao organizaciji da ublaži rizik od potencijalnog sajber-napada.

  Šta je rizik? Rizik je potencijalni uticaj koji ranjivost, pretnja ili resurs predstavlja na organizaciju, izračunat u odnosu na sve druge ranjivosti, pretnje i resurse. Procena rizika pomaže da se utvrdi verovatnoća da će određeni problem izazvati otkrivanje podataka koje će naneti štetu finansijama, reputaciji ili usklađenosti sa propisima. Smanjenje rizika je ključno za mnoge organizacije. Postoji mnogo sertifikata, regulatornih standarda i radnih okvira koji su dizajnirani da pomognu kompanijama da razumeju, identifikuju i smanje rizike.
- **Nulti dan (eng. zero-day) –** Napad nultog dana je eksploatacija koja je nepoznata svetu, uključujući prodavca proizvoda, što znači da ga prodavac nije zakrpio. Ti napadi se obično koriste u napadima na naciju-državu, kao i u velikim kriminalnim organizacijama. Otkriće napada nultog dana može biti veoma dragoceno za etičke hakere i penetracione testere i može im doneti nagradu za otkrivanje greške. Te nagrade su naknade koje dobavljači plaćaju istraživačima bezbednosti koji otkriju nepoznate propuste u aplikacijama.

Danas su mnoge organizacije uspostavile program za nagrađivanje koji omogućava zainteresovanim osobama koje otkriju ranjivost u sistemu dobavljača da je prijave. Osoba koja prijavi ranjivost, obično grešku nultog dana, dobija nagradu. Međutim, postoje hakeri koji namerno pokušavaju da iskoriste sistem ili mrežu za neku vrstu lične koristi; to je poznato kao vrednost hakovanja.

U ovom odeljku ste otkrili različite ključne termine koji se obično koriste u industriji sajber bezbednosti. U sledećem odeljku ćete istražiti različite faze penetracionog testiranja.

Istraživanje potrebe za penetracionim testiranjem i njegove faze

Svaki dan, profesionalci za sajber bezbednost su u trci sa vremenom, i napadačima, u otkrivanju ranjivosti sistema i mreža. Zamislite da napadač može da iskoristi ranjivost na sistemu pre nego što stručnjak za sajber bezbednost može da je pronađe i primeni bezbednosne kontrole kako bi ublažio pretnju. Napadač bi kompromitovao sistem. Tada profesionalac za sajber bezbednost treba da primeni strategije **odgovora na incident** (incident response **IR**) i planove za vraćanje kompromitovanog sistema u prihvatljivo radno stanje.

Organizacije shvataju potrebu angažovanja white hat hakera, kao što su penetracioni testeri koji imaju veštine da simuliraju sajber-napade u stvarnom svetu na sisteme i mreže organizacije, sa namerom da otkriju i iskoriste skrivene ranjivosti. Te tehnike omogućavaju penetracionom testeru da izvrši iste vrste napada kao pravi haker; razlika je u tome što je organizacija unajmila penetracionog testera koji ima zakonsku dozvolu za sprovođenje takvog nametljivog bezbednosnog testiranja.

Važna napomena

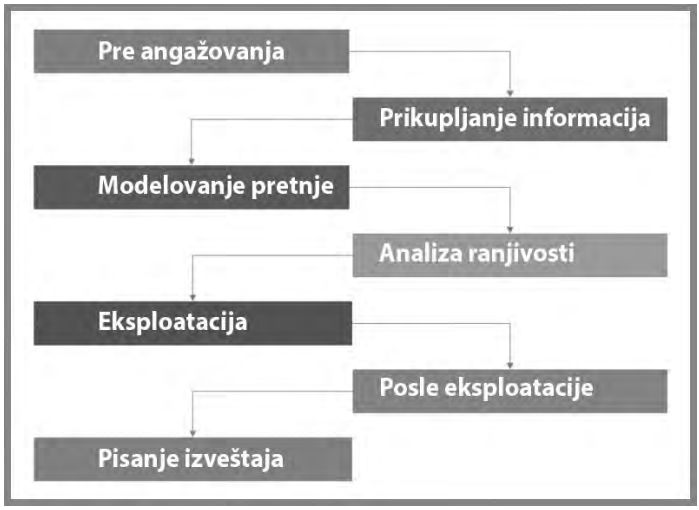
Penetracioni testeri obično dobro razumeju računare, operativne sisteme, umrežavanje i programiranje i kako to funkcioniše zajedno. Najvažnije je da vam je potrebna kreativnost. Kreativno razmišljanje omogućava osobi da razmišlja izvan okvira i prevaziđe predviđenu upotrebu tehnologija i da pronađe uzbudljive nove načine njihove primene.

Na kraju penetracionog testa, zainteresovanim stranama organizacije je predstavljen izveštaj sa detaljima o svim nalazima, kao što su ranjivosti, i kako svaka slabost može da bude zloupotrebljena. Izveštaj, takođe, sadrži preporuke o tome kako ublažiti i sprečiti mogući sajber napad na svaku pronađenu ranjivost. To omogućava organizaciji da razume šta će haker otkriti ukoliko su oni meta i kako da primeni kontramere za smanjenje rizika od sajber napada. Neke organizacije će čak izvršiti drugi penetracioni test nakon implementacije preporuka navedenih u izveštaju penetracionog testa, da bi utvrdile da li su sve ranjivosti ispravljene i da li je rizik smanjen.

Izrada plana za penetraciono testiranje

Iako je penetraciono testiranje zanimljivo, ne možemo napasti metu bez plana. Planiranje osigurava da penetraciono testiranje prati sekvencijalan redosled koraka za postizanje željenog ishoda, a to je identifikacija i iskorišćavanje ranjivosti. Svaka faza ističe i opisuje šta je potrebno, pre prelaska na sledeće korake. To osigurava efikasno prikupljanje svih detalja o radu i meti i da penetracioni tester ima jasno razumevanje zadatka koji je pred njim.

Slede različite faze penetracionog testiranja:



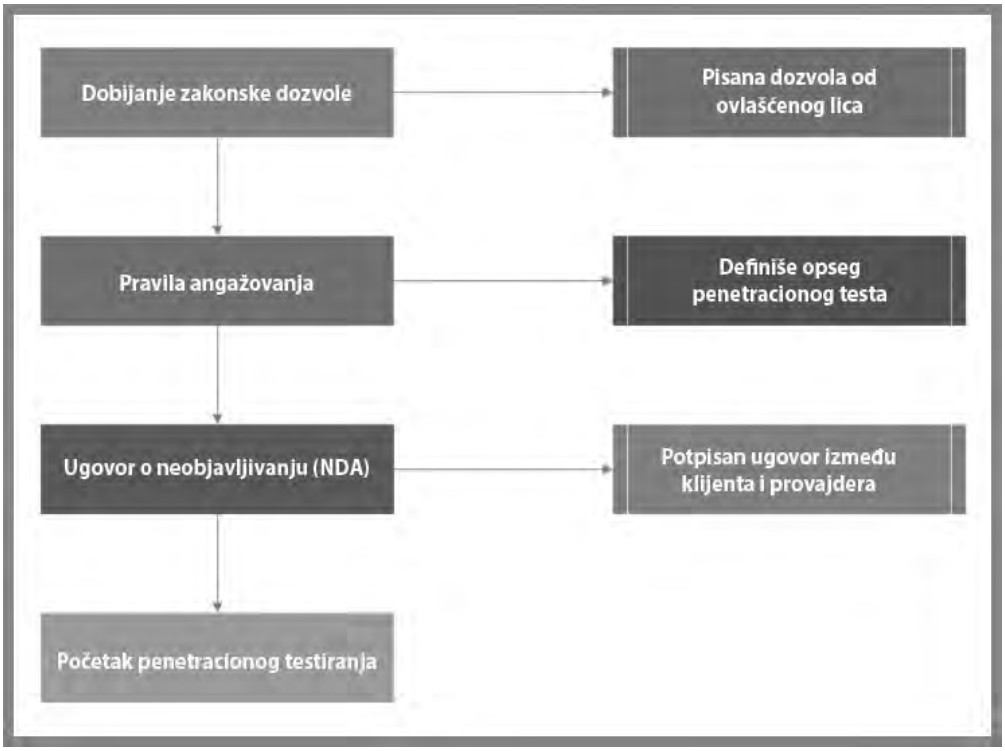
Slika 1.1 – Faze penetracionog testiranja

Kao što je prikazano prethodnim dijagramom, penetraciono testiranje se obično sastoji od faza pre angažovanja, prikupljanja informacija, modelovanja pretnji, analize ranjivosti, zloupotrebe, posle zloupotrebe i pisanja izveštaja. Svaka od ovih faza biće detaljnije obrađena u narednim odeljcima.

Pre angažovanja

Tokom ove faze bira se ključno osoblje. Ti pojedinci su ključni za obezbeđivanje informacija, koordinaciju resursa i pomoć penetracionim testerima da razumeju obim, širinu i pravila angažovanja u proceni.

Ova faza, takođe, obuhvata zakonske zahteve, koji obično uključuju **Ugovor o neobjavljivanju** (**Non-Disclosure Agreement - NDA**) i **Ugovor o konsultantskim uslugama** (**Consulting Services Agreement - CSA**). Sledi prikaz tipičnog procesa, onoga što je potrebno izvršiti pre izvršenja penetracionog testiranja:



Slika 1.2 – Pre angažovanja

NDA je pravni sporazum kojim je precizirano da penetracioni testeri i njihov poslodavac neće deliti ili zadržati bilo kakve poverljive ili vlasničke informacije na koje naiđu tokom procene. Kompanije obično potpisuju ove ugovore sa kompanijama za sajber bezbednost koje će ih, zauzvrat, potpisati sa zaposlenima koji rade na projektu. U nekim slučajevima, kompanije potpisuju ove ugovore direktno sa penetracionim testerima iz kompanije koja sprovodi projekat.

Obim penetracionog testa, takođe poznat kao **pravila angažovanja (eng. rules of engagement)**, definiše sisteme koje penetracioni tester može i ne može da hakuje. To osigurava da penetracioni tester ostane unutar zakonskih granica. To je zajednički dogovor između klijenta (organizacije) i penetracionog testera i njegovog poslodavca. Takođe, definiše osetljive sisteme i njihove IP adrese, kao i vreme testiranja i navedeno je koji sistemi zahtevaju posebne prozore za testiranje. Veoma je važno da penetracioni testeri obrate posebnu pažnju na obim penetracionog testa i gde testiraju, da bi uvek ostali u okviru ograničenja testiranja.

U nastavku su neki primeri pitanja pre angažovanja koja će vam pomoći da definišete obim penetracionog testa:

- Koja je veličina/klasa vaše eksterne mreže? (Penetraciono testiranje mreže)
- Koja je veličina/klasa vaše interne mreže? (Penetraciono testiranje mreže)
- Koja je svrha i cilj penetracionog testa? (Primenljivo na bilo koji oblik penetracionog testiranja)
- Koliko stranica ima veb aplikacija? (Penetraciono testiranje veb aplikacija)
- Koliko korisničkih unosa ili obrazaca ima veb aplikacija?

Ovo nije opširna lista pitanja pre angažmana i o svim angažmanima bi trebalo dobro da razmislite da biste bili sigurni da postavljate sva važna pitanja, da ne biste podcenili angažman.

Sada kada smo razumeli faze pravnog ograničenja penetracionog testiranja, pređimo na učenje o fazi prikupljanja informacija i njenom značaju.

Prikupljanje informacija

Penetraciono testiranje uključuje prikupljanje informacija, što je od vitalnog značaja da bi se osiguralo da penetracioni testeri imaju pristup ključnim informacijama koje će im pomoći u sprovođenju procene. Iskusni profesionalci obično provode jedan ili dva dana u vršenju detaljnog izviđanja svoje mete. Što više informacija o meti bude poznato, pomoći će penetracionom testeru da identifikuje površinu napada, kao što su tačke ulaska u sistem i mrežu mete. Pored toga, ova faza pomaže penetracionom testeru da identifikuje zaposlene, infrastrukturu, geolokaciju za fizički pristup, detalje o mreži, servere i druge vredne informacije o ciljnoj organizaciji.

Razumevanje mete je veoma važno pre bilo kakvog napada penetracionog testera, jer pomaže u kreiranju profila potencijalne mete. Na primer, oporavak korisničkih identifikatora/naloga za prijavu u ovoj fazi biće od vitalnog značaja za kasnije faze penetracionog testa, jer će nam pomoći da dobijemo pristup ranjivim sistemima i mrežama. Pogledajmo sada osnove modelovanja pretnji.

Modelovanje pretnji

Modelovanje pretnji je proces koji služi kao pomoć penetracionim testerima i zaštitnicima mrežne bezbednosti da bolje razumeju pretnje koje su inspirisale procenu ili pretnje kojima je aplikacija ili mreža najsklonija. Ti podaci zatim pomažu penetracionim testerima da simuliraju, procene i reše najčešće pretnje sa kojima se organizacija, mreža ili aplikacija suočavaju.

Slede radni okviri za modelovanje pretnji:

- **Spoofing, Tampering, Repudiation, Information disclosure, Denial of server and Elevation of privilege (STRIDE)**
- **Process for Attack Simulation and Threat Analysis (PASTA)**

Pošto se razumeju pretnje sa kojima se organizacija suočava, sledeći korak je izvršenje procene ranjivosti resursa da bi se dalje odredila ocena i ozbiljnost rizika.

Analiza ranjivosti

Analiza ranjivosti obično uključuje procenjivače ili penetracione testere koji pokreću skeniranje ranjivosti ili mreže/portova da bi bolje razumeli koje usluge se nalaze na mreži ili koje aplikacije su pokrenute na sistemu i da li postoji ranjivost u bilo kom sistemu uključenom u opseg procene. Taj proces često uključuje ručno otkrivanje i testiranje ranjivosti, što je često najtačniji oblik analize ranjivosti ili procene ranjivosti.

Postoji mnogo alata, besplatnih i komercijalnih, koji nam pomažu da brzo identifikujemo ranjivosti na ciljnom sistemu ili mreži. Nakon otkrivanja bezbednosnih slabosti, sledeća faza je pokušaj iskorišćavanja.

Iskorišćavanje (eksploatacija)

Iskorišćavanje je najčešće zanemaren ili previđen deo penetracionog testiranja, a realnost je da klijenti i rukovodioci ne mare za ranjivosti osim ako razumeju zašto su im bitne. Iskorišćavanje je municija ili dokaz koji pomaže da izrazimo zašto je ranjivost važna i da ilustrujemo uticaj koji bi ranjivost mogla imati na organizaciju. Štaviše, bez eksploatacije, procena nije penetracioni test i nije ništa više od procene ranjivosti, koju većina kompanija može da sprovede u „svojoj kući" bolje nego što bi to mogao nezavisan konsultant.

Jednostavno rečeno, tokom faze prikupljanja informacija penetracioni tester će profilisati metu i identifikovati sve ranjivosti. Zatim, korišćenjem informacije o ranjivosti penetracioni tester će obaviti svoje istraživanje i kreirati specifične eksploatacije koje će iskoristiti ranjivosti mete - to je eksploatacija. Koristimo eksploatacije (zlonamerni kod) da bismo iskoristili ranjivost (slabost) u sistemu, što će nam omogućiti da izvršimo proizvoljni kod i komande na cilju.

Često, nakon uspešnog iskorišćavanja ciljnog sistema ili mreže, možemo misliti da je zadatak obavljen — ali još uvek nije. Postoje zadaci i ciljevi koje je potrebno da izvršimo nakon provale u sistem. To je faza penetracionog testiranja posle eksploatacije.

Posle eksploatacije

Eksploatacija je proces dobijanja pristupa sistemima koji mogu sadržati osetljive informacije. Proces posle eksploatacije je nastavak ovog koraka, gde stečeno uporište služi za pristup podacima ili širenje na druge sisteme pomoću tehnika lateralnog kretanja unutar ciljne mreže. Tokom faze posle eksploatacije, primarni cilj je obično demonstriranje uticaja koji ranjivost i dobijeni pristup mogu imati na organizaciju. Taj uticaj pomaže izvršnom rukovodstvu da bolje razume ranjivosti i štetu koju bi ona mogla da nanese organizaciji ako dođe do pravog sajber-napada.

Pisanje izveštaja

Pisanje izveštaja je jedan od najvažnijih elemenata svakog penetracionog testa. Penetraciono testiranje može da bude usluga, ali pisanje izveštaja je rezultat koji klijent vidi i jedini je opipljiv element koji se daje klijentu na kraju procene. Izveštajima bi trebalo posvetiti isto toliko pažnje kao i testiranju.

Pisanje izveštaja uključuje mnogo više od navođenja nekoliko ranjivosti otkrivenih tokom procene. To je medij kroz koji prenosite rizik i poslovni uticaj, rezimirate svoje nalaze i uključujete korake sanacije. Dobar penetracioni tester treba da bude dobar pisac izveštaja, inače će problemi koje pronađe biti izgubljeni, a klijent, koji ga je angažovao da sprovede procenu, ih možda nikada neće razumeti.

Nakon što ste završili ovaj odeljak, u mogućnosti ste da opišete svaku fazu penetracionog testa i stekli ste bolju predstavu o očekivanjima od penetracionih testera. Sada ćemo zaroniti u razumevanje različitih pristupa penetracionom testiranju.

Razumevanje pristupa penetracionom testiranju

Procena **bele kutije (eng. white box)** je tipična za testiranje veb aplikacija, ali može da bude proširena na bilo koji oblik penetracionog testiranja. Ključna razlika između testiranja bele, crne i sive kutije je količina informacija koja je dostavljena penetracionim testerima pre angažovanja. U proceni bele kutije, penetracioni tester će dobiti sve informacije o aplikaciji i njenim tehnologijama i obično će dobiti identifikatore sa različitim stepenom pristupa za brzo i temeljno identifikovanje ranjivosti u aplikacijama, sistemima ili mrežama. Ne izvršavamo sva bezbednosna testiranja korišćenjem pristupa bele kutije; ponekad se penetracionom testeru daje samo naziv ciljne kompanije.

Procena **crne kutije (eng. black box)** je najčešći oblik procene penetracije mreže i najtipičnija je među eksternim penetracionim testovima mreže i penetracionim testovima socijalnog inženjeringa. U proceni crne kutije, penetracionim testerima se daje vrlo malo ili nimalo informacija o ciljnim mrežama ili sistemima koje testiraju. Ovaj poseban oblik testiranja je efikasan kada pokušavate da utvrdite šta će pravi haker otkriti i njegove strategije da dobije neovlašćeni pristup mreži organizacije i da kompromituje njihove sisteme.

Procene **sive kutije (eng. gray box)** su hibrid testiranja bele i crne kutije i obično služe za obezbeđivanje realističnog scenaria testiranja, a istovremeno daju penetracionim testerima dovoljno informacija da smanje vreme potrebno za sprovođenje izviđanja i drugih aktivnosti testiranja crne kutije. Pored toga, važno je u svakoj proceni da se uverite da testirate sve sisteme u opsegu. U pravoj crnoj kutiji moguće je promašiti sisteme, a kao rezultat toga, oni su izostavljeni iz procene.

Svaki pristup penetracionom testu se razlikuje od drugih i od vitalnog je značaja da znate sve o njima. Zamislite potencijalnog klijenta koji zahteva test crne kutije na svojoj spoljnoj mreži; kao penetracioni tester, moramo biti upoznati sa uslovima i onim što se od nas očekuje.

Vrste penetracionog testiranja

Kao ambiciozan penetracioni tester, važno je razumeti razliku između procene ranjivosti i penetracionog testiranja. U proceni ranjivosti, stručnjak za sajber bezbednost koristi skener ranjivosti, koji služi kao pomoć u proceni bezbednosnog položaja sistema unutar organizacije. Ti skeneri ranjivosti koriste različite tehnike za automatizaciju procesa otkrivanja širokog spektra bezbednosnih slabosti na sistemima.

Nedostatak skeniranja ranjivosti je njegova nesposobnost da identifikuje probleme koje ručno testiranje može i to je razlog što organizacija angažuje penetracione testere za sprovođenje ove procene. Unutar industrije, organizacije mogu angažovati stručnjaka za sajber bezbednost da izvrši penetraciono testiranje na njihovoj infrastrukturi. Međutim, ako stručnjak za sajber bezbednost izvršava skeniranje umesto ručnog testiranja, to je oblik prevare i, po mom mišljenju, veoma je neetički. Ako ne možete da rešite problem penetracionog testiranja, onda vežbajte, vežbajte i vežbajte još više. Kasnije u ovoj knjizi naučićete legalne načine da poboljšate svoj zanat.

Penetraciono testiranje veb aplikacija

Penetraciono testiranje veb aplikacija, u daljem tekstu **WAPT (web application penetration testing)**, je najčešći oblik penetracionog testiranja i verovatno će biti prvi posao penetracionog testiranja koji će obaviti većina ljudi koji čitaju ovu knjigu. WAPT je čin sprovođenja ručnog hakovanja ili penetracionog testiranja na veb aplikaciji radi testiranja ranjivosti koje tipični skeneri ranjivosti neće pronaći. Previše često se dešava da penetracioni testeri šalju skenirane ranjivosti veb aplikacija umesto da ručno pronalaze i verifikuju probleme u veb aplikacijama.

Penetraciono testiranje mobilnih aplikacija

Penetraciono testiranje mobilnih aplikacija je slično WAPT-u, ali je specifično za mobilne aplikacije koje sadrže sopstvene vektore napada i pretnje. To je rastući oblik penetracionog testiranja sa velikim mogućnostima za one koji žele da se probiju u penetraciono testiranje i razumeju razvoj mobilnih aplikacija. Kao što ste možda primetili, svaki od različitih tipova penetracionog testiranja ima specifične ciljeve.

Penetraciono testiranje socijalnog inženjeringa

Penetraciono testiranje socijalnog inženjeringa, po mom mišljenju, je najuzbudljivija vrsta testiranja. Socijalni inženjering je umetnost manipulacije osnovnom ljudskom psihologijom da bismo pronašli ljudske ranjivosti i da bismo ljude naterali da rade nešto što inače ne bi radili. Tokom ovog oblika penetracijskog testiranja, od vas će se možda tražiti da izvršite aktivnosti kao što su slanje phishing e-poruka, upućivanje vishing telefonskih poziva ili razgovor o bezbednim objektima kako biste utvrdili šta napadač koji cilja osoblje može da postigne. Postoje mnoge vrste napada socijalnim inženjeringom o kojima će biti reči kasnije u ovoj knjizi.

Penetraciono testiranje mreže (eksterne i interne)

Penetraciono testiranje mreže fokusira se na identifikaciju bezbednosnih slabosti u ciljanom okruženju. Ciljevi penetracionog testa su da se identifikuju nedostaci u sistemima ciljne organizacije, njihovim mrežama (žičnim i bežičnim) i njihovim mrežnim uređajima, kao što su svičevi i ruteri.

Slede neki zadaci koje obavljamo pri penetracionom testiranju mreže:

- Zaobilaženje **Sistema za otkrivanje upada** (**Intrusion Detection System - IDS**)/**Sistema za sprečavanje upada** (**Intrusion Prevention System - IPS**)
- Zaobilaženje uređaja zaštitnih zidova (eng. firewalls)
- Probijanje lozinke
- Dobijanje pristupa krajnjim uređajima i serverima
- Iskorišćavanje pogrešnih konfiguracija na svičevima i ruterima

Sada kada imate bolju predstavu o ciljevima penetracionog testiranja mreže, pogledajmo svrhu penetracionog testiranja u cloudu.

Penetraciono testiranje u cloudu

Penetraciono testiranje u cloudu uključuje izvođenje bezbednosnih procena i penetracionog testiranja rizika za cloud platforme radi otkrivanja svih ranjivosti koje mogu izložiti poverljive informacije zlonamernim korisnicima. Pre nego što pokušate da direktno angažujete cloud platformu, uverite se da imate zakonsku dozvolu cloud provajdera. Na primer, ako ćete da izvršite penetraciono testiranje na platformi Microsoft Azure, biće vam potrebna zakonska dozvola od Microsofta jer vaše radnje mogu uticati na druge korisnike i servise koji dele centar podataka.

Fizičko penetraciono testiranje

Fizičko penetraciono testiranje se fokusira na testiranje fizičkih bezbednosnih sistema kontrole pristupa koji su postavljeni za zaštitu podataka organizacije. Bezbednosne kontrole postoje u kancelarijama i data centrima da bi se sprečio ulazak neovlašćenih lica u bezbedna područja kompanije.

Fizičke bezbednosne kontrole uključuju sledeće:

- **Sigurnosne kamere i senzore**: Sigurnosne kamere služe za praćenje fizičkih radnji u oblasti.
- **Biometrijske sisteme autentikacije**: Biometrija služi da bi se osiguralo da samo ovlašćene osobe imaju pristup nekoj oblasti.
- **Vrata i brave**: Sistemi zaključavanja služe da bi sprečili ulazak neovlašćene osobe u prostoriju ili oblast.
- **Obezbeđenje** (čuvari): Čuvari su ljudi zaduženi da štite nešto, nekoga ili područje.

Nakon što ste završili ovaj odeljak, sada ste u mogućnosti da opišete različite vrste penetracionog testiranja. Vaše putovanje neće biti završeno bez razumevanja faza hakovanja. Različite faze hakovanja će biti opisane u sledećem odeljku.

Istraživanje faza hakovanja

Pošto su penetracioni testeri beli šeširi, dobri momci i devojke u industriji, važno je razumeti faze hakovanja jer je to takođe povezano sa penetracionim testiranjem. Tokom bilo koje obuke za penetraciono testiranje naići ćete na pet faza hakovanja. Te faze su sledeće:

Slika 1.3 – Faze hakovanja

Kao što je prikazano prethodnim dijagramom, pre nego što napadač napadne metu, potrebno je prikupljanje informacija da bi bolje razumeo različite detalje o meti. Zahvaljujući sledećim odeljcima bolje ćete razumeti svaku fazu i kako se ona odnosi na penetraciono testiranje.

Izviđanje ili prikupljanje informacija

Faza izviđanja ili prikupljanja informacija je faza u kojoj se napadač fokusira na sticanje značajnih informacija o meti. Ovo je najvažnija faza u hakovanju: što je više detalja poznato o meti, lakše je kompromitovati slabost i iskoristiti je.

Slede tehnike koje primenjujemo u fazi izviđanja:

- Korišćenje pretraživača za prikupljanje informacija
- Korišćenje platformi za društvene mreže
- Izvođenje Google hakovanja/dorkinga
- Izvođenje ispitivanja **sistema imenovanja domena** (**Domain Name System - DNS**)
- Korišćenje socijalnog inženjeringa

U ovoj fazi cilj je prikupiti što više informacija o meti. Sada ćemo govoriti o primeni usmerenijeg pristupa i iskoristiti metu da bismo dobili konkretnije i detaljnije informacije.

Skeniranje i nabrajanje

Druga faza hakovanja je skeniranje. Skeniranje uključuje korišćenje direktnog pristupa u iskorišćavanju mete za dobijanje informacija koje nisu dostupne u fazi izviđanja. Ova faza uključuje profilisanje ciljne organizacije, njenih sistema i mrežne infrastrukture.

Slede tehnike koje primenjujemo u fazi skeniranja:

- Provera uključenih sistema
- Provera zaštitnih zidova i njihovih pravila
- Provera otvorenih mrežnih portova
- Provera aktivnih servisa
- Provera bezbednosnih propusta
- Kreiranje mrežne topologije ciljne mreže

Ova faza je veoma važna jer nam pomaže da poboljšamo profil mete. Informacije pronađene u ovoj fazi će nam pomoći da pređemo na eksploataciju ciljnog sistema ili mreže.

Dobijanje pristupa

Ova faza ponekad može biti najizazovnija faza od svih. U ovoj fazi, napadač koristi informacije dobijene iz prethodnih faza da bi iskoristio cilj. Nakon uspešnog iskorišćavanja ranjivosti, napadač može daljinski da izvrši zlonamerni kod na cilju i da dobije daljinski pristup ciljnom sistemu.

Kada napadač dobije pristup može da se desi sledeće:

- Probijanje lozinke
- Iskorišćavanje ranjivosti
- Proširivanje ovlašćenja
- Sakrivanje fajlova

Faza dobijanja pristupa (eksploatacije) ponekad može biti teška jer eksploatacije mogu funkcionisati na jednom sistemu, ali ne i na drugom. Kada je eksploatacija uspešna i dobijen je pristup sistemu, sledeća faza je da obezbedite stalnu vezu sa ciljem.

Održavanje pristupa

Nakon iskorišćavanja sistema napadač bi obično trebalo da obezbedi mogućnost pristupa sistemu žrtve u bilo kom trenutku sve dok je sistem onlajn. To postiže stvaranjem pristupa tajnim vratima (eng. backdoor) cilja i postavljanjem višestrukih veza između napadačevih mašina i sistema žrtve.

Ciljevi održavanja pristupa su sledeći:

- Lateralno kretanje
- Eksfiltracija podataka
- Kreiranje tajnih vrata i trajnih veza

Održavanje pristupa je važno da biste osigurali da vi, penetracioni tester, uvek imate pristup ciljnom sistemu ili mreži. Kada je tehnički aspekt penetracionog testa završen, vreme je da očistite mrežu.

Prikrivanje tragova

Poslednja faza je prikrivanje tragova. To osigurava da ne ostavljate nikakve tragove svog prisustva na kompromitovanom sistemu ili mreži. Kao penetracioni testeri, želeli bismo da budemo neotkriveni na mreži cilja, da ne pokrećemo nikakva upozorenja na bezbednosnim senzorima i uređajima dok uklanjamo sve preostale tragove radnji izvršenih tokom penetracionog testa. Prikrivanje tragova osigurava da ne ostavljate nikakav trag o svom prisustvu na mreži, jer je penetracioni test dizajniran da bude prikriven i da simulira napade u stvarnom svetu na organizaciju.

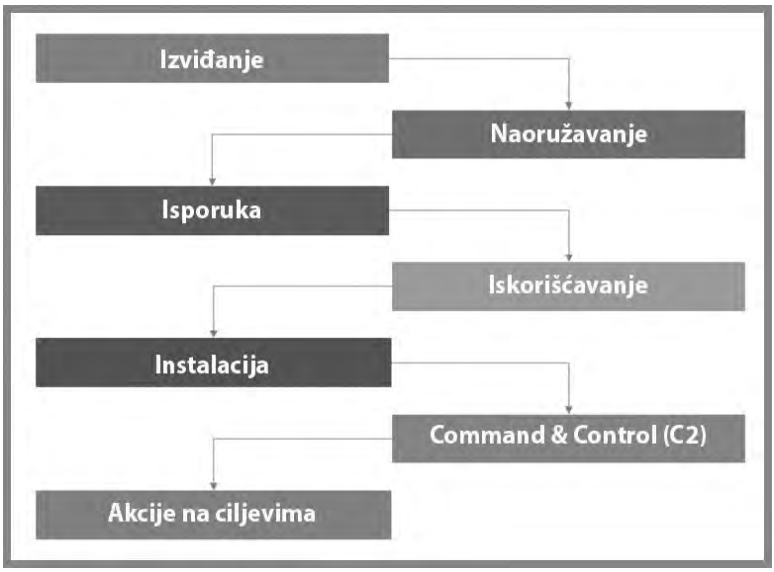
Nakon što ste završili ovaj odeljak, stekli ste znanje o fazama hakovanja koje obično koriste napadači. U sledećem odeljku ćete otkriti radni okvir Cyber Kill Chain, a kombinovaćemo ga u obuku i vežbe u ovoj knjizi.

Razumevanje radnog okvira Cyber Kill Chain

Kao ambiciozan penetracioni tester koji se probija u industriju sajber bezbednosti, od vitalnog je značaja da razumete način razmišljanja napadača. Da biste bili bolji u penetracionom testiranju morate da imate veoma kreativan i strateški način razmišljanja. Jednostavno rečeno, morate da razmišljate kao pravi haker ako želite da ugrozite sisteme i mreže kao profesionalac za sajber bezbednost.

Cyber Kill Chain je sedmostepeni radni okvir koji je razvio Lockheed Martin, američka aerokosmička korporacija. Ovaj radni okvir opisuje svaki važan korak koji će napadač morati da izvrši pre nego što uspešno ispuni ciljeve sajber-napada na svoje mete. Stručnjaci za sajber bezbednost će moći da smanje verovatnoću da napadač ispuni svoje ciljeve i da smanje količinu štete, ako uspeju da zaustave napadača tokom ranijih faza Cyber Kill Chain-a.

Sledećim dijagramom prikazano je sedam faza Cyber Kill Chain-a koje koriste napadači:



Slika 1.4 – Cyber Kill Chain

Kao što je prikazano na *slici 1.4*, možete videti kako se svaka faza preliva u drugu sve dok napadač ne dostigne poslednju fazu u kojoj je uspešan u svom sajber-napadu, a profesionalci za sajber bezbednost nisu bili u stanju da zaustave napad. Na strani plavog tima operacija sajber bezbednosti, inženjeri bezbednosti moraju da osiguraju da su sistemi i mreže veoma dobro zaštićeni i nadgledani u pogledu bilo kakvih potencijalnih pretnji. Ako je detektovana pretnja, plavi tim treba da ublaži pretnju što je pre moguće, otuda potreba za razumevanjem Cyber Kill Chain-a. Međutim, kao penetracioni tester, možemo da primenimo tehnike i strategije koje koriste napadači, koje odgovaraju svakoj fazi Cyber Kill Chain-a da bismo postigli svoje ciljeve tokom penetracionog testa za organizaciju.

U narednih nekoliko odeljaka učićete osnove svake faze Cyber Kill Chain-a, kako svaku od njih koriste napadači i kako penetracioni testeri primenjuju ove strategije u svojim angažmanima.

Izviđanje

Kao i u svakom planu bitke, važno je da znate mnogo o svom protivniku pre nego što započnete rat. Faza izviđanja je fokusirana na prikupljanje mnogo informacija i obaveštajnih podataka o meti, bilo da se radi o osobi ili organizaciji. Napadači i penetracioni testeri koriste ovu fazu da kreiraju profil svoje mete, koji sadrži IP adrese, operativne sisteme sistema, otvorene servisne portove, pokrenute aplikacije, ranjivosti i sve poverljive resurse koji mogu da budu nenamerno izloženi i mogu da povećaju površinu napada.

Važna napomena

Faza izviđanja uključuje i pasivne i aktivne tehnike prikupljanja informacija, koje ćemo opisati u kasnijim odeljcima ove knjige. Takođe ćete otkriti alate i tehnike za poboljšanje vaših informacionih veština prilikom obavljanja penetracionog testiranja.

Napadači će provesti dosta vremena istražujući svoju metu da bi utvrdili geolokaciju bilo koje fizičke kancelarije, onlajn servise, nazive domena, mrežnu infrastrukturu, onlajn servere i veb aplikacije, zaposlene, telefonske brojeve i adrese e-pošte, itd. Glavni cilj je saznati što više informacija o meti. Ponekad ova faza može potrajati dugo. U poređenju sa penetracionim testerom koji ima određeni vremenski period da izvrši ceo penetracioni test, može potrajati od 1 do 2 dana intenzivnog istraživanja pre nego što se pređe na sledeću fazu.

Naoružavanje

Korišćenjem informacija prikupljenih u fazi izviđanja, napadač i penetracioni tester mogu da ih koriste da bolje izgrade oružje (koje nazivamo eksploatacijom), koje može da iskoristi bezbednosnu ranjivost na meti. Oružje (eksploatacija) mora da bude posebno izrađeno i testirano da bi se osigurao njegov uspeh kada ga pokrene napadač ili penetracioni tester. Cilj eksploatacije je da utiče na poverljivost, integritet i/ili dostupnost sistema ili mreža cilja.

Eksploatacija iskorišćava ranjivosti. Nakon što se to dogodi, šta je sledeće? Radi bolje strategije, napadači i penetracioni testeri će upariti svoje oružje sa korisnim opterećenjem. Korisni teret je oslobađen nakon što eksploatacija ugrozi sistem. Kao jednostavan primer, korisni teret može da služi za kreiranje trajnih tajnih vrata na ciljnom sistemu koja omogućavaju napadaču ili penetracionom testeru daljinski pristup sistemu u bilo kom trenutku kada je kompromitovani sistem na mreži.

Isporuka

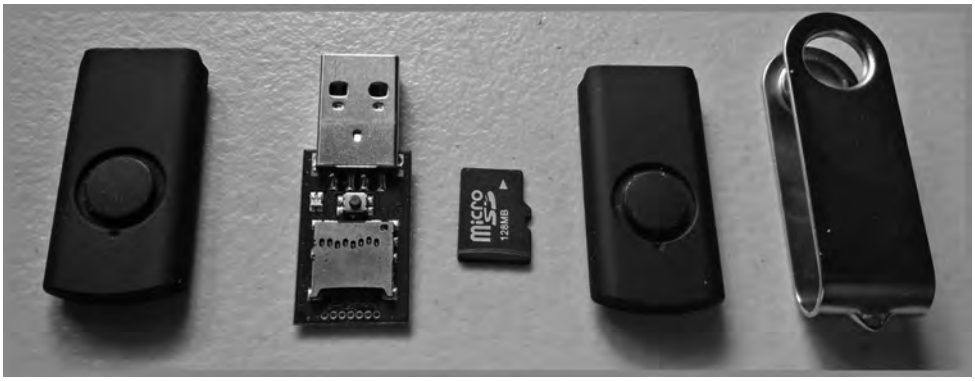
Nakon kreiranja oružja, napadač ili penetracioni tester mora da isporuči oružje na ciljni sistem. Isporuku može da izvrši korišćenjem kreativnog načina razmišljanja napadača, razmenom poruka e-pošte, korišćenjem servisa za poruke, ili čak kreiranjem preuzimanja na kompromitovanim veb servisima. Druga tehnika može da bude kopiranje zlonamernog koda na više USB diskova i njihovo postavljanje u krug ciljne organizacije, sa nadom da će ga zaposleni pronaći i povezati sa internim sistemom zbog ljudske radoznalosti.

Čini se da je na sledećoj slici prikazan običan kabl za prenos podataka za mobilni telefon, međutim, to je posebna vrsta USB ninja kabla, koji napadač može unapred da programira sa zlonamernim skriptovima koji će biti izvršeni kada je kabl povezan sa računarom:

Slika 1.5 – USB ninja kabl

USB ninja kabl mogu da koriste i napadači i penetracioni testeri kao metod za isporuku zlonamernog tereta na sistem mete.

Na sledećoj slici prikazan je USB rubber ducky, koji može da služi za isporuku korisnih podataka:



Slika 1.6 – USB rubber ducky

Kada su USB ninja kabl i USB rubber ducky umetnuti u računar, oni funkcionišu kao emulator tastature i izvršavaju korisne podatke. Ova tehnika omogućava i napadačima i penetracionim testerima da jednostavno zaobiđu zaštitne zidove i anti malverski softver.

Kao penetracioni tester, uverite se da imate više metoda za isporuku oružja do mete, tako da u slučaju da jedan metod ne funkcioniše, imate drugi itd.

Eksploatacija

Nakon što je oružje (eksploatacija) isporučeno na metu, napadač treba da se uveri da, kada je eksploatacija izvršena, uspešno iskoristi bezbednosnu ranjivost na ciljnom sistemu, kako je i predviđeno. Ako eksploatacija nije uspešna, plavi tim organizacije može da otkrije napadača ili penetracionog testera i doći će do zastoja u Cyber Kill Chain-u. Napadač treba da se uveri da je eksploatacija ispravno testirana pre nego što je izvrši na ciljnom sistemu.

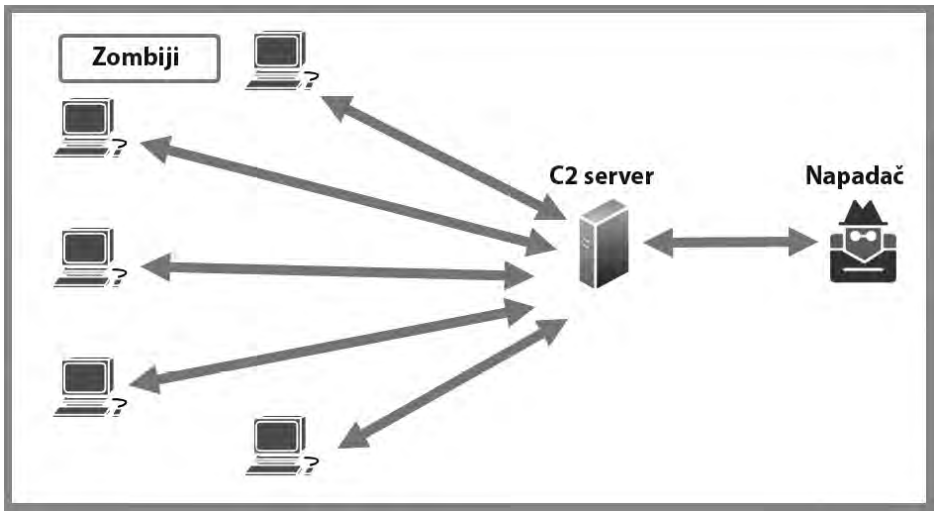
Instalacija

Nakon što napadač iskoristi ciljni sistem, pokušaće da kreira višestruke trajne pristupe, tajnim vratima, kompromitovanom sistemu. To omogućava napadaču ili penetracionom testeru da ima više kanala za ulazak u sistem i mrežu. Tokom ove faze, obično mogu da budu instalirane dodatne aplikacije dok napadač preduzima mnogo mera predostrožnosti da bi izbegao da ga otkriju bilo kakvi sistemi za otkrivanje pretnji.

Command and Control (C2)

Važna faza u sajber-napadu je kreiranje **Command and Control** (**C2**) veze između kompromitovanih sistema i C2 servera na internetu. To omogućava napadaču da centralno kontroliše grupu zaraženih sistema (botnet) korišćenjem C2 servera kojim upravlja napadač. To omogućava napadaču da stvori vojsku zombija, koje kontroliše i kojima upravlja jedan napadač.

U sledećem dijagramu prikazan je primer C2:



Slika 1.7 – C2 operacije

Napadač koristi šifrovanje podataka, enkapsulaciju i različite tehnike tuneliranja da bi izbegao sisteme za otkrivanje pretnji unutar ciljnih organizacija. Slično tome, postoji napredna faza penetracionog testiranja poznata kao crveno timovanje gde ne postoje ograničenja (pravila angažovanja) u pogledu metoda i tehnika koje su primenjene za kompromitovanje ciljne organizacije, sa ciljem simulacije onoga što je najbliže stvarnom naprednom sajber napadu zlonamerne sajber vojske. Međutim, imajte na umu da je zakonska dozvola i dalje potrebna za bilo koju vrstu angažmana crvenog tima.

Akcije na ciljeve

Ako napadač ili penetracioni tester uspe da dostigne ovu fazu Cyber Kill Chain-a, plavi tim organizacije nije uspeo da zaustavi napadača i spreči sajber napad. U ovoj fazi, napadač je ispunio svoje ciljeve i postigao ciljeve napada. U ovoj fazi, napadač može da dovrši glavni cilj napada, bilo da se radi o eksfiltraciji podataka iz organizacije i prodaji tih podataka na dark vebu ili čak da proširi svoj botnet za veći sajber napad na drugu ciljnu organizaciju.

Zaustavljanje napadača ili penetracionog testera u ovoj fazi smatra se izuzetno teškim jer bi napadač već uspostavio višestruke trajne backdoor pristupe sa šifrovanim C2 vezama na više kompromitovanih sistema unutar ciljne organizacije. Štaviše, napadač će takođe očistiti tragove svih dokaza ili artefakata koji bi mogli pomoći profesionalcima za sajber bezbednost da uđu u trag napadaču.

Nakon što ste završili ovaj odeljak, naučili ste sve o različitim fazama Cyber Kill Chain-a i kako on pomaže profesionalcima za sajber bezbednost da razumeju namere napadača. Pored toga, naučili ste kako penetracioni testeri mogu da primenete strategije u okviru svojih angažmana penetracionog testiranja.

Rezime

U ovom poglavlju otkrili ste različite vrste napadača i njihovu motivaciju za izvođenje zlonamernih sajber-napada na osobe i organizacije. Štaviše, stekli ste razumevanje nekih faktora koji se uzimaju u obzir među napadačima i penetracionim testerima, jer utiču na pokretanje sajber-napada ili izvođenje procene penetracionog testiranja na ciljne organizacije. Takođe ste stekli znanje da identifikujete različite ključne termine u industriji sajber bezbednosti i istražili ste faze penetracionog testiranja i kako se ono povezuje sa fazama hakovanja. Na kraju, otkrili ste različite vrste penetracionih testova koji se sprovode unutar organizacija i istražili ste radni okvir Cyber Kill Chain u vezi sa penetracionim testiranjem.

Nadam se da vam je ovo poglavlje bilo informativno i od pomoći na vašem putovanju ka tome da postanete super sjajan penetracioni tester i profesionalac za sajber bezbednost u industriji. U sledećem poglavlju, poglavlju 2, *Izgradnja laboratorije za penetraciono testiranje*, učićete da izgradite sopstvenu laboratoriju za penetraciono testiranje da biste usavršili svoje nove veštine u bezbednom prostoru.

Dodatna literatura

Da biste saznali više o ovoj temi, pogledajte sledeće linkove:

- *Razumevanje brojeva mrežnih portova*: https://hub.packtpub.com/understanding-network-port-numbers-tcp-udp-and-icmp-on-anoperating-system/
- *Ranjivosti u aplikacijskom i transportnom sloju* TCP/IP steka: https://hub.packtpub.com/vulnerabilities-in-theapplication-and-transport-layer-of-the-tcp-ip-stack/
- Razumevanje prostora IP adresa: https://hub.packtpub.com/understanding-address-spaces-and-subnetting-in-ipv4-tutorial/
- Cyber Kill Chain: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html