U OVOM POGLAVLJU

- **Biranje alatki**
- **Skeniranje mrežnih hostova**
- **Procenjivanje bezbednosti pomoću analizatora mreže**
- **Sprečavanje uskraćivanja usluga i ranjivosti infrastrukture**

# Poglavlje 9
# Sistemi mrežne infrastrukture

Da bi operativni sistemi i aplikacije bili bezbedni, mora biti bezbedna mreža. Zbog toga u okviru testiranja bezbednosti morate da procenite uređaje kao što su ruteri, mrežne barijere, pa čak i generički mrežni hostovi (uključujući servere i radne stanice).

Postoji na hiljade mogućih ranjivosti mreže, kao i podjednako mnogo alatki i još više tehnika za testiranje. Verovatno nemate dovoljno vremena i sredstava da biste testirali sve moguće ranjivosti svojih sistema mrežne infrastrukture i koristili svaku moguću alatku ili metodu. Zato treba da se usmerite na one testove kojima se dobija dobra opšta procena mreže. Upravo takve testove opisujem u ovom poglavlju.

Mnoge poznate ranjivosti karakteristične za mrežu možete ukloniti tako što ćete svoje mrežne hostove ažurirati najnovijim softverom i firmverom proizvođača. Budući da mnogi sistemi mrežne infrastrukture nisu javno dostupni, velika je verovatnoća da vaši mrežni hostovi neće biti napadnuti spolja. Brojne druge slabe tačke možete ukloniti tako što ćete na svojoj mreži poštovati neke dobre bezbednosne prakse, koje opisujem u ovom poglavlju. Među testovima, alatkama i tehnikama iz ovog poglavlja pronaći ćete gotovo sve što vam je potrebno za procenu bezbednosti.

SAVET

Što bolje razumete mrežne protokole, biće vam lakše da testirate ranjivosti mreže, jer mrežni protokoli predstavljaju osnovu za većinu bezbednosnih koncepata. Ako vam nije do kraja jasno kako mreža radi, preporučujem da pročitate

knjigu *TCP/IP For Dummies*, 6. izdanje, autora Candace Leiden i Marshall Wilensky (John Wiley & Sons, Inc.), koja je i meni pomogla da savladam koncepte umrežavanja. Kao dobra referenca može da posluži i lista zahteva za komentare (engl. *Request for Comments*, RFC) na stranici Official Internet Protocol Standards (`www.rfc-editor.org/standards`).

# Šta su ranjivosti mrežne infrastrukture

Ranjivosti mrežne infrastrukture uzrok su većine tehničkih problema u informacionim sistemima. Ove ranjivosti niskog nivoa utiču na gotovo sve što se izvršava na mreži, zbog čega morate da testirate sistem i proveravate da li postoje, i da ih uklanjate kad god je to moguće.

Testovi bezbednosti u mrežnoj strukturi moraju se usmeriti na to da se pronađu slabosti koje i drugi vide na mreži, kako bi mogao da se proceni i obradi nivo izloženosti mreže.

UPAMTITE

Mnogi problemi su povezani sa bezbednošću mrežne infrastrukture. Neki su tehničke prirode i za njihovu ispravnu procenu potrebne su različite alatke; ostale možete procenjivati samo pažljivim posmatranjem i donošenjem logičnih zaključaka. Neke probleme je lakše uočiti sa spoljašnje strane mreže, a druge sa unutrašnje.

Kada procenjujete bezbednost mrežne strukture svoje kompanije, morate da posmatrate sledeće:

- Gde se na mreži nalaze uređaji, kao što su mrežna barijera ili sistem za sprečavanje upada (IPS), i kako su konfigurisani.
- Šta vide spoljni napadači dok pretražuju priključke i kako mogu da iskoriste ranjivosti na vašim mrežnim hostovima.
- Projektovanje mreže, kao što su veze sa internetom, mogućnosti za daljinski pristup, slojevita odbrana i razmeštaj hostova na mreži.
- Interakcija instaliranih bezbednosnih uređaja, kao što su mrežne barijere, sistemi za sprečavanje upada i antivirusni programi.
- Koji se protokoli koriste, uključujući one za koje se zna da su ranjivi – na primer, Secure Sockets Layer (SSL).
- Priključci koji se najčešće napadaju i koji su nezaštićeni.
- Konfiguracije mrežnih hostova.
- Nadzor i održavanje mreže.

Ako neko iskoristi ranjivosti sa prethodnog spiska, ili ranjivost bilo kog drugog dela bezbednosti mreže, posledice mogu biti sledeće:

- Napadač može da izvede napad uskraćivanjem usluga (DoS), što može da prekine vezu sa internetom ili obori celu mrežu.
- Zlonamerno zaposleno lice koje koristi analizator mreže može da ukrade poverljive informacije iz e-poruka i datoteka i pošalje ih preko mreže.
- Haker može da konfiguriše pristup mreži na tajna vrata.
- Privremeni saradnik može da napadne posebne hostove iskorišćavanjem lokalnih ranjivosti na mreži.

SAVET

Pre procene bezbednosti mrežne infrastrukture, ne zaboravite da uradite sledeće:

- Testirajte sisteme spolja i iznutra (to jest, u internim mrežnim segmentima i demilitarizovanim zonama [DMZ], kao i između njih).
- Pribavite dozvolu od partnerskih mreža da proverite postojanje ranjivosti na njihovim sistemima (kao što su otvoreni priključci, nedostatak mrežnih barijera ili pogrešno konfigurisani ruter), koje mogu da utiču na bezbednost *vaše* mreže.

# Biranje alatki

Kao i kod svih procena bezbednosti, za testiranje bezbednosti mreže potrebne su prave alatke: programi za skeniranje priključaka, analizatori protokola i alatke za procenu ranjivosti. Postoje odlične komercijalne, javne i besplatne alatke, a u narednim odeljcima ću opisati neke koje su mi omiljene. Imajte na umu da ćete morati da koristite više alatki, jer nijedna od njih ne radi sve što vam je potrebno.

SAVET

Ako tražite bezbednosne alatke koje se lako koriste i imaju sve neophodne funkcije, uglavnom ćete dobijati ono što ste platili, naročito na Windows platformi. Veliki broj stručnjaka za bezbednost veliča kvalitete raznih besplatnih alatki, pogotovo onih koje se izvršavaju u Linuxu i drugim operativnim sistemima srodnim Unixu. Mnoge od tih alatki su veoma korisne ako imate dovoljno vremena, strpljenja i volje da se bavite njihovim prednostima i nedostacima. Ako se uporede rezultati besplatnih i komercijalnih alatki za ovu namenu, mislim da će se izvesna prednost pokazati na strani korišćenja komercijalnih alatki.

## Programi za skeniranje i analizatori

Ovi programi obavljaju gotovo sva skeniranja priključaka i testiranja mreže koja su vam potrebna:

- **Cain & Abel** (`www.oxid.it/cain.html`) za analizu mreže i trovanje ARP protokola.
- **Essential NetTools** (`https://www.tamos.com/products/nettools`) sa velikim brojem funkcija za skeniranje mreže.

- **NetScanTools Pro** (`https://www.netscantools.com`) sa velikim brojem funkcija za procenu bezbednosti mreže, uključujući skeniranje signalom ping, skeniranje priključaka i testiranje SMTP releja.
- **Getif** (`www.wtcs.org/snmp4tpc/getif.htm`), stara dobra alatka za pretraživanje SNMP protokola.
- **Nmap** (`https://nmap.org`) ili **NMapWin** (`https://sourceforge.net/projects/nmapwin`), čeoni grafički korisnički interfejs (GUI) sa programom Nmap u pozadini, za testiranje hostova i priključaka, kao i za identifikovanje (engl. *fingerprint*) operativnih sistema (OS).
- **Savvius Omnipeek** (`https://www.savvius.com`) za analizu mreže.
- **TamoSoft CommView** (`https://www.tamos.com/products/commview`) za analizu mreže.
- **Wireshark** (`http://wireshark.org`) za analizu mreže.

## Procenjivanje ranjivosti

Ove alatke za procenu ranjivosti omogućavaju da, između ostalog, testirate da li mrežni hostovi sadrže različite poznate ranjivosti, kao i potencijalne probleme konfiguracije koji mogu dovesti do zloupotrebe:

- **GFI LanGuard** (`https://www.gfi.com/products-and-solutions/network-security-solutions/gfi-languard3`) za skeniranje priključaka i testiranje ranjivosti.
- **Nexpose** (`https://www.rapid7.com/products/nexpose`), sveobuhvatna alatka za detaljno testiranje ranjivosti.

# Skeniranje i provociranje mreže

Testiranje bezbednosti mrežne infrastrukture, koje se opisuje u sledećim odeljcima, obuhvata sledeće korake hakovanja:

1. **Prikupljanje informacija i mapiranje mreže.**
2. **Skeniranje sistema da bi se proverilo koji je dostupan.**
3. **Utvrđivanje šta se izvršava na sistemima koje ste otkrili.**
4. **Pokušaj proboja u sisteme koje ste otkrili (ako se za to opredelite).**

SAVET

Svaki upravljački program mrežne kartice i svaka implementacija TCP/IP protokola u većini operativnih sistema – uključujući Windows, Linux, pa čak i mrežne barijere i rutere – imaju osobenosti koje dovode do različitog ponašanja tokom skeniranja i provociranja sistema. Zbog tih razlika u ponašanju može doći

do različitih odgovora sistema, od lažnih uzbuna do DoS uslova. U svojim vodičima za administratore ili na veb lokacijama proizvođača potražite detalje o svim poznatim problemima i zakrpama za njihovo rešavanje. Ako ste zakrpili sve svoje sisteme, ne bi trebalo da imate probleme, ali imajte na umu da je sve moguće.

## Priključci za skeniranje

Program za skeniranje priključaka (engl. *port scanner*) pokazuje vam šta je šta na vašoj mreži, i to tako što je pretražuje da bi uočio šta je aktivno. Ovim programima se obezbeđuje osnovni prikaz rasporeda mreže, što vam može pomoći da identifikujete neovlašćene hostove ili aplikacije, kao i greške u konfiguraciji mrežnih hostova koje mogu da dovedu do ozbiljnih bezbednosnih ranjivosti.

Širom perspektivom programa za skeniranje priključaka često se otkrivaju bezbednosni problemi koji bi na neki drugi način ostali neprimećeni. Ovi programi se lako koriste i mogu da testiraju mrežne hostove bez obzira na operativne sisteme i aplikacije koji se izvršavaju. Testovi se izvršavaju relativno brzo i bez potrebe za obradom pojedinačnih mrežnih hostova (što može biti više nego zamorno).

Pri proceni opšte bezbednosti mreže važno je tumačenje rezultata koje dobijate iz skeniranja priključaka. Na primer, možete da dobijete lažne uzbune na otvorenim priključcima pa ćete morate da idete korak dalje. Skeniranja protokola za korisničke datagrame (engl. *User Datagram Protocol*, UDP), kao i sam protokol, manje su pouzdani od skeniranja protokola za upravljanje prenosom (engl. *Transmission Control Protocol*, TCP) i često dovode do lažnih uzbuna, jer mnoge aplikacije ne znaju kako da odgovore na nasumične dolazne UDP zahteve.

Program za skeniranje sa velikim brojem funkcija, kao što je Nexpose, može da identifikuje priključke i prikaže šta se izvršava u jednom koraku.

UPOZORENJE

Skeniranja priključaka mogu da oduzmu dosta vremena, zavisno od toga koliko hostova imate, koliko priključaka skenirate, koje alatke koristite, kakve su mogućnosti obrade sistema koji testirate i kolika je brzina mrežnih veza.

UPAMTITE

Po pravilu treba da skenirate više važnih hostova. Nemojte ništa izostaviti, jer sistemi koje zanemarite mogu kasnije da vam se osvete. Pored toga, izvršavajte iste testove različitim uslužnim programima, kako biste videli da li dobijate različite rezultate. Neće sve alatke pronaći iste otvorene priključke i ranjivosti – što nije dobro, ali je realna činjenica testiranja ranjivosti i neprobojnosti.

Ako testirate sistem pomoću više alatki i ne dobijete iste rezultate, možete dodatno da istražite problem. Ako nešto ne izgleda ispravno (na primer, pronašli ste čudan skup otvorenih priključaka), onda najverovatnije i nije. Pokrenite test ponovo, a ako ste sumnjičavi, upotrebite drugu alatku zbog drugačije perspektive.

SAVET

Ako je to moguće, treba da testirate svih 65.534 TCP priključaka na svakom mrežnom hostu koji pronađe vaš program za skeniranje. Ako pronađete sumnjive priključke, potražite u dokumentaciji da li je aplikacija poznata i odobrena. Ne bi bilo loše da pretražite svih 65.534 UDP priključaka. Imajte na umu da ovaj proces može znatno da produži vreme skeniranja.

Da bi sve bilo brže i jednostavnije, možete da pretražite najčešće hakovane priključke koji se navode u tabeli 9-1. Ne zaboravite da mnoge od tih priključaka koriste i zlonamerni programi..

**TABELA 9-1** **Najčešće hakovani priključci**

| Broj priključka | Usluga | Protokol(i) |
|---|---|---|
| 7 | Echo | TCP, UDP |
| 19 | Chargen | TCP, UDP |
| 20 | FTP data (File Transfer Protocol) | TCP |
| 21 | FTP control | TCP |
| 22 | SSH | TCP |
| 23 | Telnet | TCP |
| 25 | SMTP (Simple Mail Transfer Protocol) | TCP |
| 37 | Time | TCP, UDP |
| 53 | DNS (Domain Name System) | UDP |
| 69 | TFTP (Trivial File Transfer Protocol) | UDP |
| 79 | Finger | TCP, UDP |
| 80 | HTTP (Hypertext Transfer Protocol) | UDP |
| 110 | POP3 (Post Office Protocol version 3) | TCP |
| 111 | SUN.RPC (remote procedure calls) | TCP, UDP |
| 135 | RPC/DCE (endpoint mapper) for Microsoft networks | TCP, UDP |
| 137, 138, 139, 445 | NetBIOS over TCP/IP | TCP, UDP |
| 161 | SNMP (Simple Network Management Protocol) | TCP, UDP |
| 443 | HTTPS (HTTP over TLS) | TCP |
| 512, 513, 514 | Berkeley r-services and r-commands (such as `rsh`, `rexec`, and `rlogin`) | TCP |
| 1433 | Microsoft SQL Server (ms-sql-s) | TCP, UDP |
| 1434 | Microsoft SQL Monitor (ms-sql-m) | TCP, UDP |
| 1723 | Microsoft PPTP VPN | TCP |
| 3389 | Windows Terminal Server | TCP |
| 8080 | HTTP proxy | TCP |