1.2 Maliciozni softveri

Maliciozni softveri

- **Maliciozni softver** (*malware – malicious software*) je program koji se tajno ubaci u neki drugi program, sa namerom da se unište podaci, izvrše razorni ili nametljivi programi, ili se na drugi način ugrozi poverljivost, integritet, raspoloživost podataka žrtve, aplikacija ili operativnog sistema
- **Maliciozni softveri** su **programi koji rade nešto nedozvoljeno na računaru**.
- Šteta koju pričinjavaju se najčešće ogleda u krađi naših privatnih informacija, brisanju fajlova ili preuzimanju kontrole nad našim računarom.
- Veliki broj virusa, reklamnog i špijunskog softvera će usporiti računar, rušiti aplikacije, ometati saobraćaj na Internetu.
- Zbog toga što imaju **štetno delovanje**, maliciozni programi moraju da ostanu **sakriveni od korisnika** i da se na drugim računarima **instaliraju samostalno ili putem prevare korisnika**.

Maliciozni softveri

- Osnovna karaktveristika zlonamernog softvera je njihova sposobnost da **zaraze računar bez znanja korisnika** i da ih je kasnije **teško pronaći i odstraniti**.
- Osnovne dve strategije su:

  sakrivanje, kada se koristi tehnička veština da se program učini "nevidljivim" i

  prevara, kada se program predstavlja kao nešto sasvim drugo.
- Maliciozni program se obično kreira da bude robustan - korisnik obično ne može da prekine njegovo izvršavanje ako je program aktivan u memoriji, niti da obriše fajl.

Maliciozni softveri

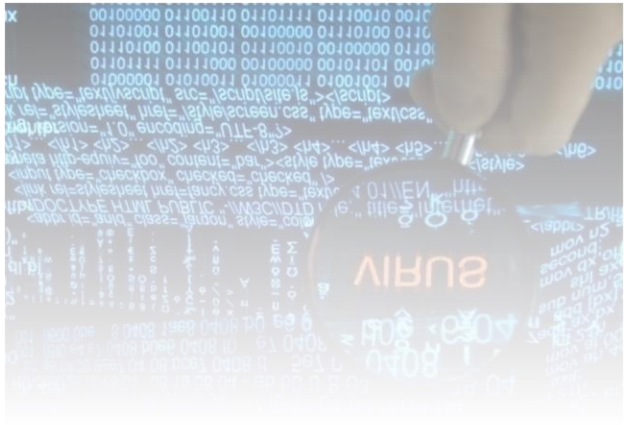
- Postoji širok spektar pretnji malicioznim softverom i mera protiv njih
- Klasifikacija zlonamernog softvera može biti zasnovana:
  - Na sredstvima koje zlonamerni softver koristi za svoje prostirenje ili širenje;
  - Na akcijama ili glavnim teretima (payloads) koji se koriste kada zlonamerni softver stigne na svoj cilj.
- Mehanizmi širenja su oni koje koriste virusi, crvi i trojanci
- Glavni “tereti” (payloads) uključuju kvar sistema (system corruption), botove (bots), phishing, spyware, lažne administratorske pakete, rootkits.

Računarski virus

- **Računarski virus** je zlonamerni softver koji izvršava neku zasebnu neželjnu funkciju u operativnom sistemu računara korisnika
  - Virus može oštetiti softver, hardver ili fajl.
  - Virus je po pravilu povezan sa drugim executable programom, tako da kada se program aktivira, aktivira se i virus (aktivira ga korisnik pokretanjem programa za koji je virus povezan).
  - Neophodan je korisnik kako bi se virus proširio na druge računare (deljenje inficiranih fajlova između korisnika ili slanje email-ova sa virusom u *attachment*-u)
- Računarski virus je softver koji "inficira" druge programe, tako što ih **promeni** u određenoj meri.
  - Modifikacija se može ogledati u tome da se u originalni kod ubaci rutina koja pravi kopije virusnog koda, a on zatim može da nastavi sa inficiranjem drugog sadržaja.

Računarski virus

- U svom instrukcijskom kodu računarski virus nosi recept po kojem pravi savršene kopije sebe samog
- Tipičan virus ostaje ugrađen u programu, ili nosiocu izvršnog sadržaja u računaru
- Kad god zaraženi računar stupi u dodir sa nezaraženim delom koda, sveža kopija virusa prelazi na novu lokaciju
  - Na taj način infekcija može da se širi sa računara na računar, uz pomoć korisnika koji ništa ne sumnjaju i razmenjuju te programe ili fajlove na disku ili USB stiku, ili ih šalju jedni drugima preko mreže
- Virus je neaktivan sve dok se *executable* program ne pokrene od strane korisnika



Računarski virus

- Računarski virus, a generalno i mnoge druge savremene vrste zlonamernog softvera, sadrže jednu ili više varijanti svake od ovih komponenti:
  - **Mehanizam infekcije** (infection mechanism) – sredstvo pomoću kojeg se virus širi, što mu omogućava da se replicira. Mehanizam se takođe naziva vektor infekcije
  - **Okidač (trigger)** – događaj ili stanje koje određuje kada će glavni teret virusa da se aktivira ili isporučuje. (logic bomb)
  - **Glavni teret korisnih informacija (payload)** – to što virus radi osim što se kopira i širi. Glavni teret može sa sobom da povlači štetne ili bezazlene, ali primetne aktivnosti

Računarski crv

- **Worm – „**Računarski crv“ je maliciozni program koji aktivno traži uređaje koje bi mogao da zarazi, a zatim svaki inficirani uređaj služi kao automatizovana odskočna daska za napade na druge uređaje.
- Zloupotrebljava se ranjivost klijentskog ili serverskog softvera u težnji za nedozvoljenim pristupu svakom novom sistemu
- Računarski crv je računarski program sličan virusu, neki ga smatraju podgrupom virusa.
- Računarski crv ima sposobnost da umnožava samog sebe (korisnik nije potreban). Pri tome koristi računarsku mrežu da bi se kopirao na druge računare, često bez uticaja čoveka.

Računarski crv

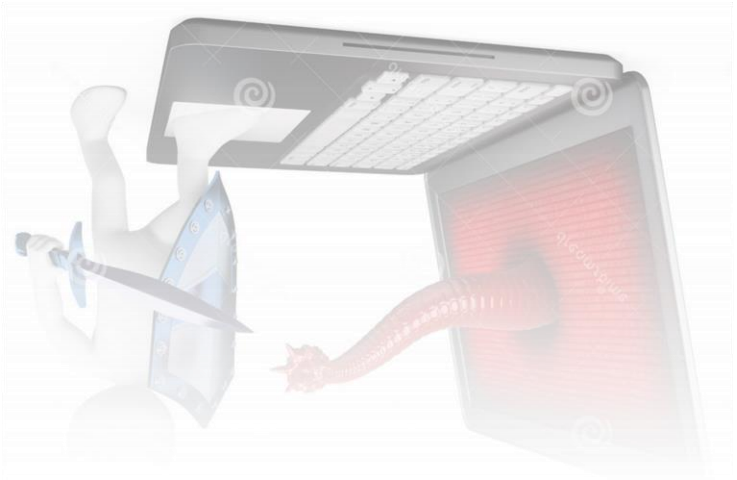
- Najčešće se širi kao fajl u mejlu te mu pristup računaru omogućuju propusti u operativnim sistemima i aplikacijama.
- „Crvi“ otežavaju rad mreže, a mogu oštetiti podatke i smanjiti sigurnost računara.
- Zaraženi računar šalje na hiljade kopija „crva“ drugim računarima u mreži i time i njih inficira.

Računarski crv

- Primer, crv se šalje svim korisnicima iz e-mail address book-a, kada se svi ti korisnici zaraze, onda se kopije crva dalje šalju svim korisnicima iz e-mail address book-ova prethodno zaraženih korisnika, i tako redom
- Zbog prirode samokopiranja crva i njegove mogućnosti prenosa kroz računarsku mrežu, posledice mogu biti:
  - preveliko zauzimanje sistemske memorije
  - Preveliko zauzimanje propusnog opsega u mreži
  - Zagušenje rada Web servera
  - Zagušenje rada mrežnih servera
  - Zagušenje rada krajnjih korisnika

Računarski crv

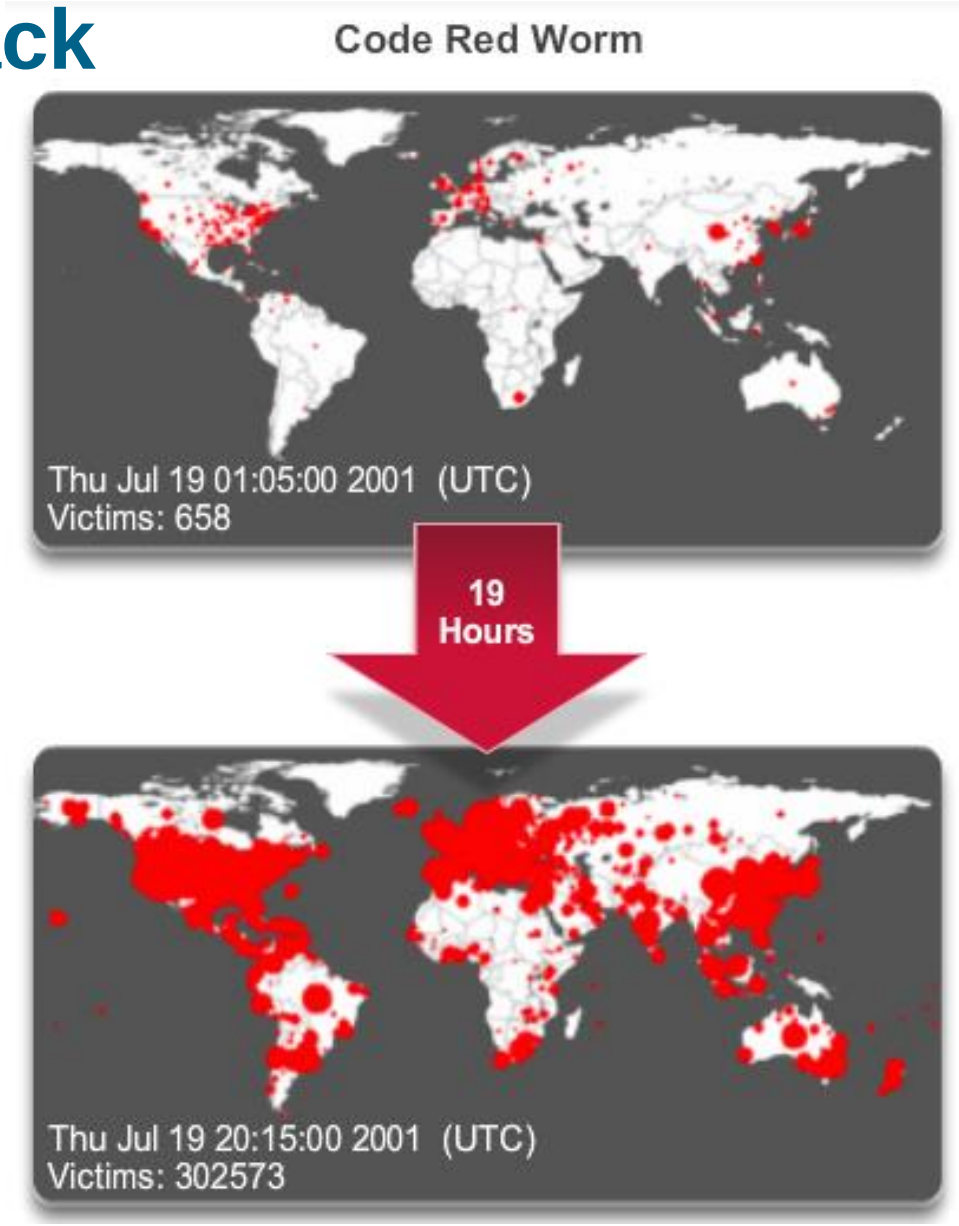
- Kad se crv aktivira, on može da se replicira i ponovo dalje širi.
- Pored širenja, crv obično nosi sa sobom neki vid aktivnog sadržaja, payload.
- Crv obično prolazi kroz iste faze kao i virus: spavanje, širenje, okidanje i izvršavanje



Code Red Worm Attack

Šta predstavlja“Code Red”?

- The Code Red worm napad je bio DoS napad koji se desio 19. jula 2001. godine.
- Tom prilikom je bio napadnut i inficiran veliki broj web servera na globalnom nivou i oko 350 000 hostova
- Milioni korisnika je bilo pogođeno ovim napadom



Trojan Horse Concept

- Trojanski konj je naizgled koristan program ili pomoćni program koji sadrži skriveni program koji kada se pozove izvodi neku neželjenu ili štetnu funkciju
- Trojanski programi mogu da se koriste za indirektno obavljanje funkcija koje napadač ne bi mogao da izvši direktno

Trojan Horse Concept

- Na primer, da bi dobio pristup osetljivim, ličnim informacijama koji se nalaze u fajlovima korisnika, napadač može da napravi program trojanac koji kada se izvrši, skenira korisničke fajlove u potrazi za željenim osetljivim informacijama i šalje njihovu kopiju napadaču preko web obrasca, ili e-poštom ili tekstualnom porukom.
- Napadač može da namami korisnika da pokrene program tako što program ugradi u igricu ili neki koristan pomoćni program i stavi ga na raspolaganju preko nekog poznatog sajta za distribuciju softvera
- **Trojanci se nalaze u slikovnim datotekama, audio datotekama ili igrama.**
- **Trojanac se vezuje za neizvršive datoteke za razlikuje od virusa koji se vezuje za exe. datoteke.**

Maliciozni softveri

Ime	opis
Logic bomb	Program koji je uljez ubacio u softver i koji leži neaktivan sve dok se ne ispuni unapred definisan uslov. Program onda aktivira neovlašćene postupke. Primeri uslova koji mogu da se koriste kao okidači su prisustvo ili odsustvo određenih fajlova ili uređaja na sistemu, određen dan u nedelji ili datum, određena verzija ili konfiguracija nekog softvera, ili određeni korisnik koji izvršava aplikaciju. Aktiviranjem programa, mogu da se menjaju ili brišu podaci ili celi fajlovi, izazove zaustavljanje mašine, ili napravi neka druga šteta.

Maliciozni softveri

Ime	opis
Backdoor	Svaki mehanizam kojim se zaobilazi normalna bezbednosna provera, a potom omogućava neovlašćen pristup funkcijama. Zadnja vrata se obično implementiraju kao mrežni servis koji osluškuje neki standardni port sa kojim napadač može da se poveže i kroz njega da izdaju komande koje će se izvršiti na kompromitovanom sistemu.

Maliciozni softveri

Ime	opis
Spammer programs	Programi koji se koriste za slanje velike količine neželjene e-pošte. Dok se neka neželjena pošta šalje sa legitimnih servera za poštu, većinu novijeg spama šalju botneti koji koriste prethodno zaražene korisničke sisteme. Značajan deo neželjene e-pošte čine reklame, pokušaji da se primalac ubedi da kupi neki proizvod on-line. Spam je takođe značajan prenosilac zlonamernog softvera. E-pošti može biti priložen dokument koji ako se otvori, može da zloupotrebi ranjivost softvera i instalira zlonamerni softver na korisnikov sistem. Pošti može biti priložen program trojanski konj ili skripta, koja ako se pokrene, takođe instalira zlonamerni softver

Maliciozni softveri

Ime	opis
Zombie, bot	Program koji se na inficiranoj mašini aktivira da bi pokrenuo napade na druge mašine. Zlonamerni softver podriva računarske i mrežne resurse zaraženog sistema da bi ga koristio napadač. Za takav zaražen sistem se kaže da je bot, koji potom tajno preuzima drugi računar povezan sa Internetom, a zatim koristi taj računar za pokretanje napada ili za upravljanje napadima. Bot se obično postavlja na stotine i hiljade računara u vlasništvu trećih lica koja ništa ne sumljanju. Kolekcija botova je često u stanju da se ponaša na koordinisan način – čineći *Botnet* Vrste napada koje izazivaju botovi: DDoS, slanje neželjene pošte, *sniffing traffic* Sposobnost daljinske kontrole je ono po čemu se bot razlikuje od crva

Maliciozni softveri

Ime	opis
Spyware	Softver koji prikuplja informacije iz računara i šalje ih drugom sistemu Omogućava praćenje širokog spektra aktivnosti na sistemu To može biti nadgledanje istorije i sadržaja pretraživačke aktivnosti, preusmeravanje nekih zahteva za web stranice na lažne sajtove koje kontroliše napadač... Sve to može da dovede do značajnog ugrožavanja korisnikovih ličnih informacija

Maliciozni softveri

Ime	opis
Keylogger	Krađa ovlašćenja, obično korisnici šalju svoja ovlašćenja za prijavljivanje (korisničko ime i lozinka) bankarskim sajtovima, sajtovima za igranje i srodnim sajtovima preko šifrovanih komunikacionih kanala (HTTPS, POP3S) koji ih štite od hvatanja nadgledanjem paketa na mreži. Napadač može da instalira program za hvatanje kucanja na tastaturi, koji hvata otkucaje na tastaturi inficirane mašine što omogućava napadaču na nadgleda osetljive informacije. Program poseduje mehanizam filtriranja koji vraća samo one informacije koje se nalaze u blizini ključnih reči (npr., „login“, „password“, „paypal.com“...)

Maliciozni softveri

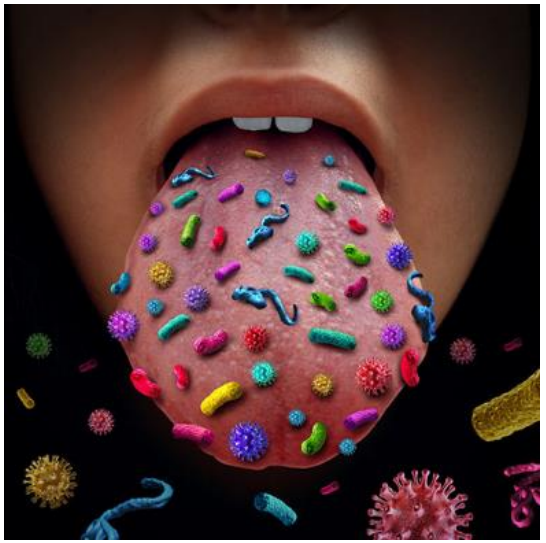
Ime	opis
Ransomware	Ovaj malware zaključava podatke na računaru kriptovanjem ključem koji je nepoznat korisniku. Motiv je materijalne prirode jer se potom obično od zaraženog korisnika traži novčana nadoknada za otključavanje podataka Malware je dizajniran da zadrži računarski sistem ili podatke zaključanim dok žrtva ne plati (plaćanje naravno nije nikakva garancija da će resursi biti oslobođeni). Ransomware obično radi enkripciju podataka ključem koji je sakriven na serveru koji kontroliše malware. Neke druge verzije ransomvare mogu iskoristiti određene sistemske ranjivosti da bi zaključali sistem. Ransomvare se širi pomoću preuzete datoteke ili neke softverske ranjivosti

Maliciozni softveri

Ime	opis
Rutkit „Rootkit“	Ovaj malware je dizajniran da modifikuje operativni sistem i kreira „a backdoor“ kako bi napadač mogao da pristupi udaljeno inficiranom računaru. Most rootkits take advantage of software vulnerabilities to perform privilege escalation and modify system files. Skup programa instaliranih na sistem da bi se držao tajni pristup tom sistemu sa administratorskim privilegijama, krijući dokaze o svom prisustvu u najvećoj mogućoj meri. Obezbeđen je pristup svim funkcijama i uslugama operativnog sistema. Rutkit može da napravi mnoge izmene sistema kako bi sakrio svoje postojanje, što korisniku otežavaju da utvrdi da je rutkit prisutan i da utvrdi koje izmene su izvršene. Rutkit se krije tako što podriva mehanizme koji nadgledaju procese, fajllove i registre na računaru i izveštavaju o njima.

Symptoms of Malware

- Povećano korišćenja CPU-a.
- Smanjenje brzine računara.
- Računar se često zamrzava ili cras-ira.
- Opada brzina Web pretraživanje.
- Postoje neobjašnjivi problemi sa mrežnom konekcijom.
- Datoteke su promenjene.
- Datoteke su izbrisane.
- Postoje nepoznati fajlovi, programi, ili desktop ikone.
- Postoje nepoznati procesi koji se uzvršavaju.
- Programi se isključuju ili rekonfigurišu sami od sebe.
- Email-ovi se šalju bez znanja i odobrenja korisnika.



Mitigating Viruses, Worms, and Trojan Horses

Antivirus Software

1.3 Attack Methodologies

Types of Attacks

- Definisane su 3 kategorije napada:
  - **A. Reconnaissance Attacks** – napad izviđanjem, podrazumeva neautorizovano otkrivanje i mapiranje slabosti sistema, servisa, uređaja
  - **B. Access Attacks** – napadi pristupom, eksploatiše se otkrivena slabost u servisima za autentifikaciju, FTP servisa i web servisa kako bi se pristupilo web nalozima, poverljivim bazama podataka i drugim osetljivim informacijama
  - **C. Denial of Service (DoS) Attacks** – ovim napadom se šalju ektremno veliki broj zahteva kroz mrežu ili Internet
    - Preterani broj zahteva ka uređaju koji se napada čini da uređaj funkcioniše otežano
    - Vrlo brzo napadnuti uređaj postaje nedostupan za legalan pristup i korišćenje

A) Reconnaissance attacks

- **Reconnaissance attacks** (napadi izviđanjem) su po pravilu napadi koji prethode kasnijim napadima sa ciljem da se obezbedi neautorizovan pristup mreži, ili remeti njeno funkcionisanje, zloupotrebe podaci...
- Administrator koji obezbeđuje sigurnost u mreži, može biti obavešten o izvršavanju ovog tipa napada zahvaljujući primanjem kratkih obaveštenja o pokušajima napada (neophodno je prethodno konfigurisati alarme)
- Na primer. broj primljenih icmp zahteva u sekundi

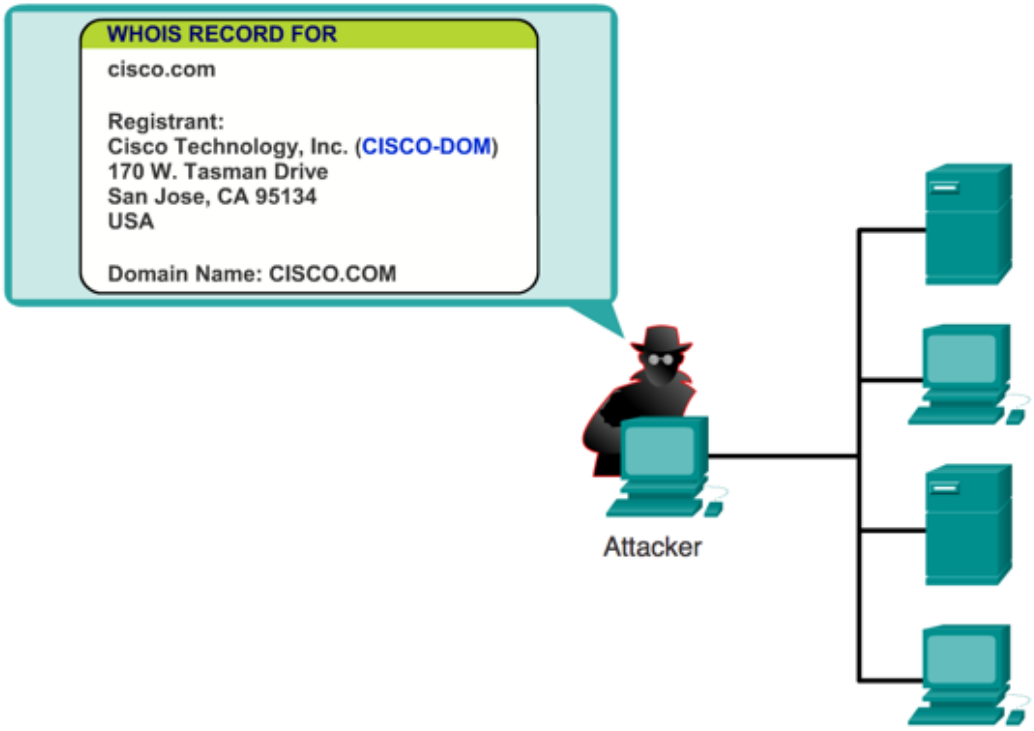
A) Reconnaissance attacks

- Izviđanje, ili drugim rečima prikupljanje informacija je neautorizovano, nelegalno otkrivanje i mapiranje sistema i njihovih slabosti.
- U većini slučajeva, ovaj tip napada prethodi access napadu ili DoS napadu
- Napadi izviđanjem može se mogu izvršiti na sledeće načine:
  1) **Internet information upiti (queries)**
  2) **Skeniranje mreže komandom ping**
  3) **Skeniranje porta**
  4) **Nadgledanje paketa (packet sniffing)**

1) Internet Information Queries

DNS upiti mogu odati informacije, npr. ko je vlasnik određenog domena i koje adrese su dodeljene tom domenu

Komande koje se tom prilikom koriste jesu: **whois**, **nslookup**, …



A) Reconnaissance attacks

1) Internet Information Queries

- **whois**

— Whois & Quick Stats

Dates	Created on 2008-05-15 - Expires on 2015-05-15 - Updated on 2014-04-04
IP Address	147.91.216.2 is hosted on a dedicated server
IP Location	- Central Serbia - Belgrade - Akademska Mreza Republike Srbije - Amres
ASN	AS13092 UB-AS Akademska mreza Republike Srbije - AMRES (registered Mar 16, 2000)
Whois History	30 records have been archived since 2010-08-22
Whois Server	whois.rnids.rs

— Website

Website Title	Висока ICT школа | Висока школа струковних студија за информационе и комуникационе технологије
Server Type	Apache
Response Code	200
SEO Score	86%
Terms	1795 (Unique: 691, Linked: 717)
Images	34 (Alt tags missing: 23)
Links	239 (Internal: 225, Outbound: 9)

Whois Record (last updated on 2015-01-20)

```
Domain name: ict.edu.rs.
Domain status: Active
Registration date: 15.05.2008 13:51:47
Modification date: 04.04.2014 09:55:58
Expiration date: 15.05.2015 13:51:47
Registrar: Eunet d.o.o.

Registrant: Visoka ICT
Address: Zdravka Čelara 16, Beograd, Serbia
ID Number: 17459023
Tax ID: 102693219

DNS: wns.ict.edu.rs. - 147.91.216.2
DNS: ns.rcub.bg.ac.rs. - 147.91.1.5

Administrative contact: Irini Reljin, Visoka ICT
Address: Zdravka Čelara 16, Beograd, Serbia

Technical contact: EUnet Hostmaster, EUnet D.O.O
Address: Milentija Popovica 9, Beograd, Serbia
```

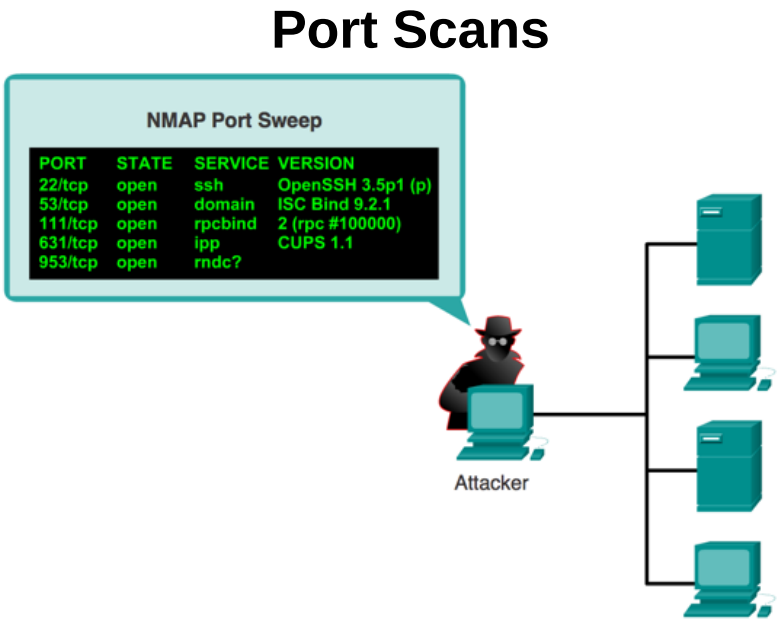
A) Reconnaissance attacks

2) 3) Ping Sweeps and Port Scans

- A ***ping sweep*** (ping skeniranje), ili *ICMP sweep* (icmp skeniranje), je skeniranje opsega IP adresa koje pripadaju aktivnim hostovima. Aktivni hostovi svojim icmp echo replay paketima daju do znanja da su njegove IP adrese aktivne. Ovo je jedna od osnovnih tehnika za skeniranje mreže

- A ***port scan*** (skeniranje porta) podrazumeva ispitivanje servera (ili bilo kog hosta) koji su im portovi otvoreni i na osnovu čega se može dalje zaključiti koji servisi na posmatranom serveru odnosno hostu su aktivni (vezuje se servis, aplikacija za well-known“ portove) i koje su njihove slabosti

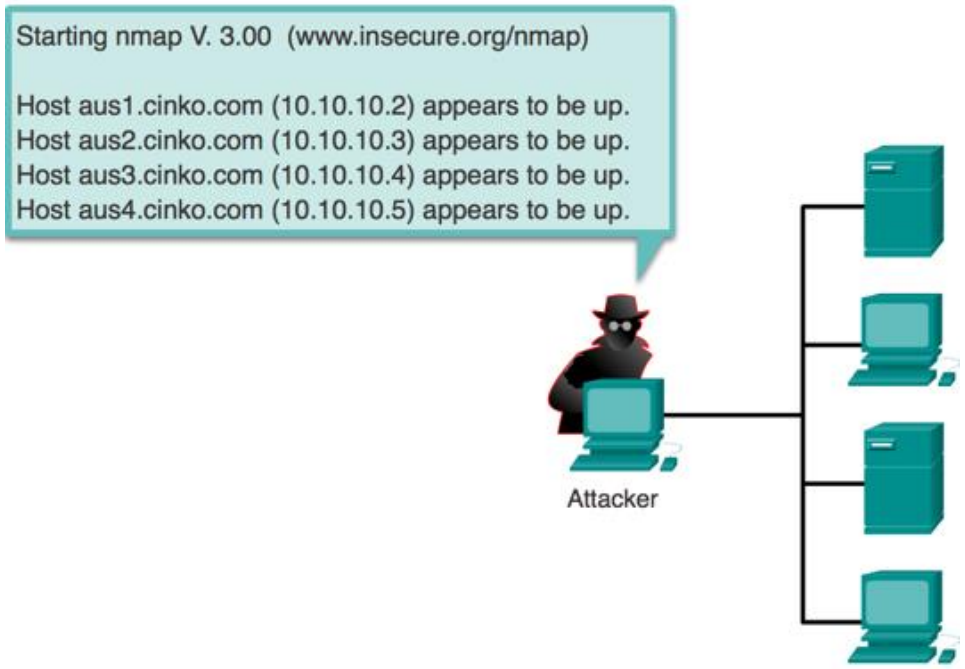
- Port scan podrazumeva slanje poruke na svaki port u različitim vremenskim trenucima. Odgovor koji se dobija nazad ukazuje na to koji port je aktivan, a potom je moguće istražiti njegovu slabost



2) 3) Ping Sweeps and Port Scans

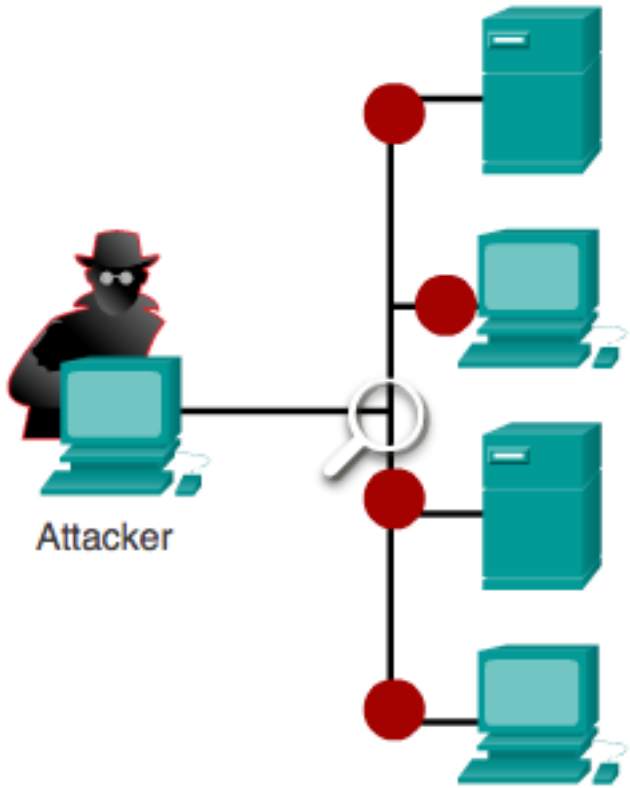
- Kao legitimni alati, *ping sweep* i *port scan* aplikacije vrše različita testiranja hostova kako bi otkrile slabosti servisa
- Informacije se prikupljaju ispitivanjem IP adresa i podataka sa TCP i UDP portova

Ping Sweep



4) Packet Sniffer

- A **packet sniffing** je softver aplikacija koja koristi mrežnu karticu uređaja u slobodnom modu za “hvatanje” svih paketa koji su poslati kroz LAN mrežu
- Ovaj softver može da se koristi samo unutar istog kolizionog domena u kome je i mreža koja se napada.
- ***Promiscuous* mode** (slobodan mod) je mod u kome mrežna kartica šalje sve pakete koji su primljeni ka aplikaciji za obradu sadžaja paketa.
- Primer aplikacije za *packet sniffing* je *Wireshark*



B) Access Attacks

- Access attacks je tip napada gde se iskorišćavaju slabosti i nedostaci rada servisa za autentifikaciju, FTP servisa i web servisa
- Usled pomenutih slabosti, pruža se mogućnost da napadač pristupi web nalozima (accounts) poverljivim bazama podataka i drugim osetljivim informacijama.

B) Access Attacks

Access attacks može biti izveden na razne načine:

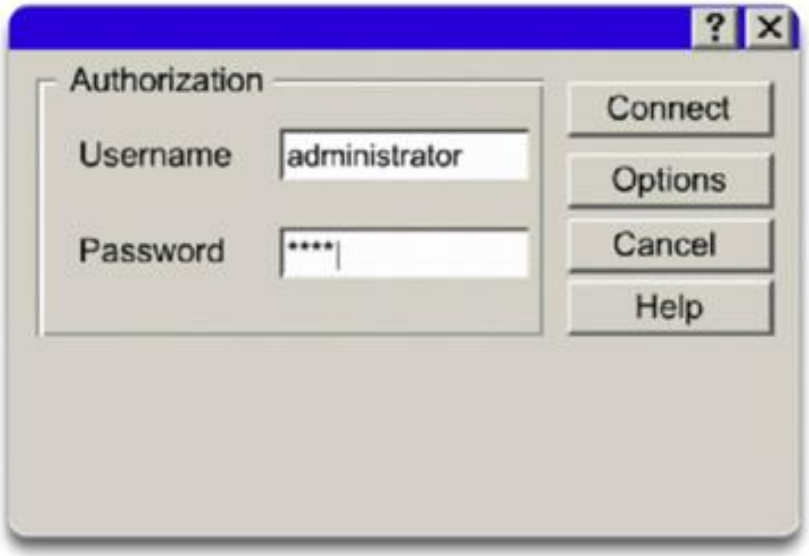
- **Password attacks**
- **IP spoofing**
- **Trust exploitation**
- **Port redirection**
- **Man-in-the-middle attacks**
- **Buffer overflow**

B) Access Attacks

Password Attacks

Hackers implement password attacks using the following:

- **Brute-force attacks** – *access attack* koja podrazumeva korišćenje posebnog softverskog programa koji generiše na hiljade potencijalnih passworda pokušavajući da otkrije sistemske lozinke za pristup sistemu korišćenjem elektronskih rečnika
- Jedan od načina zaštite od ovakvog tipa napada jeste definisanje max broja neuspelih pokušaja u određenom vremenskom periodu, nakon čega se pristup zatvara

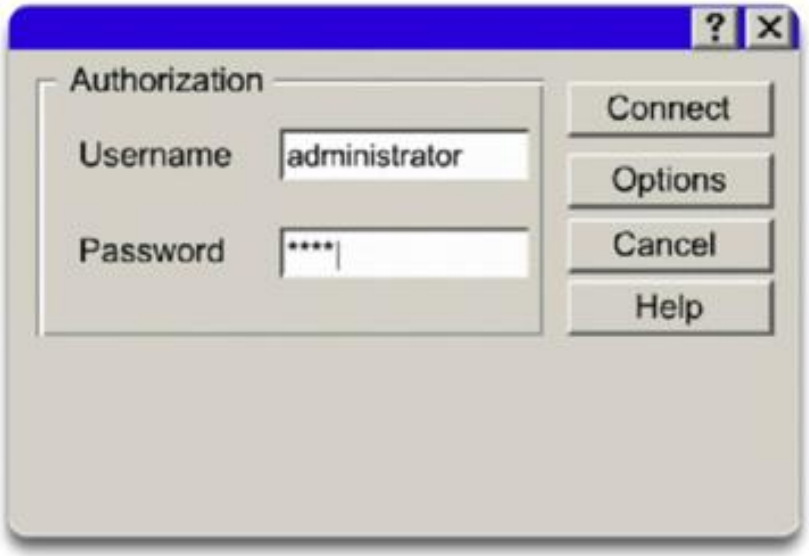


B) Access Attacks

Password Attacks

Hakeri izvršavaju password attacks koristeći sledeće:

- IP spoofing
  - Tehnika za neautorizovani pristup računaru koja se sastoji u slanju paketa sa validnom IP adresom koja ukazuje da paket stiže od legalnog hosta, iako taj paket zapravo šalje sam napadač. Napadač mora prvo da otkrije IP adresu nekog legalnog hosta i da potom modifikuje zaglavlje svog paketa kojim želi da prevari nekog drugog hosta, tako da paket izgleda kao da dolazi od legalne strane kojoj se može verovati



B) Access Attacks

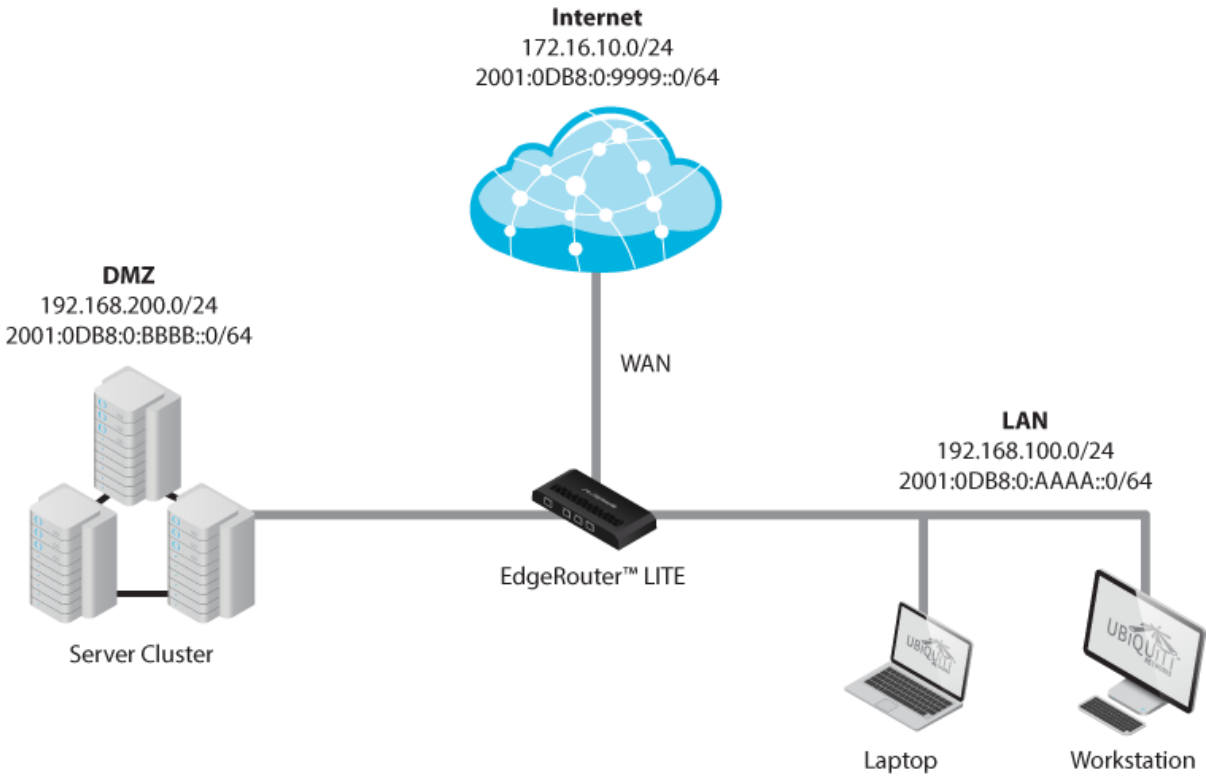
Trust Exploitation Cont.

- **Trust exploitation** je tip access attacks napada gde se iskorišćava prethodno dato poverenje u mreži nekom segmentu ili uređaju.

- **Primer:** firewall za koji je na jednom interfejsu povezana Demilitared Zone (DMZ) zona sa serverima, za drugi interfejs je povezana unutrašnja korpoorativna mreža, a treći interfejs na firewall-u je povezan sa spoljasnom mrežom, Internet-om.

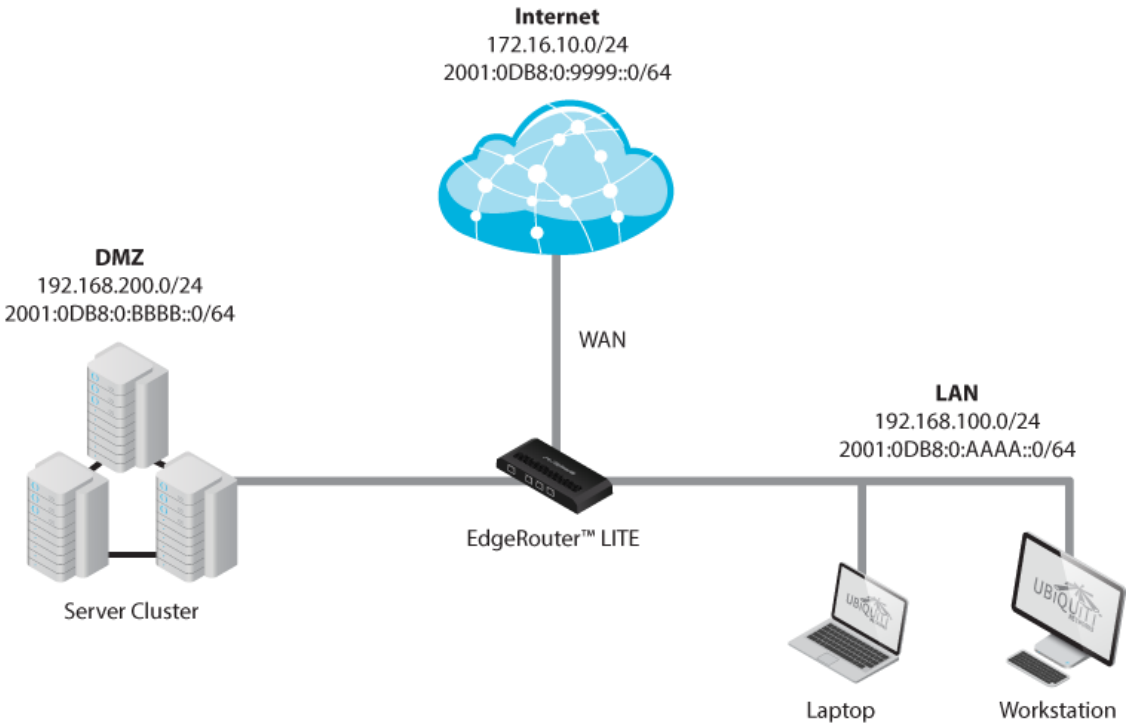
- Saobraćaj sa Interneta ka DMZ zoni je dozvoljen (postoji poverenje), ali ne i ka unutrašnjoj korporativnoj mreži.

- Saobraćaj iz DMZ zone je dozvoljen i ka unutrašnjoj zoni i ka Internetu. (host unutar mreže veruje DMZ hostu)



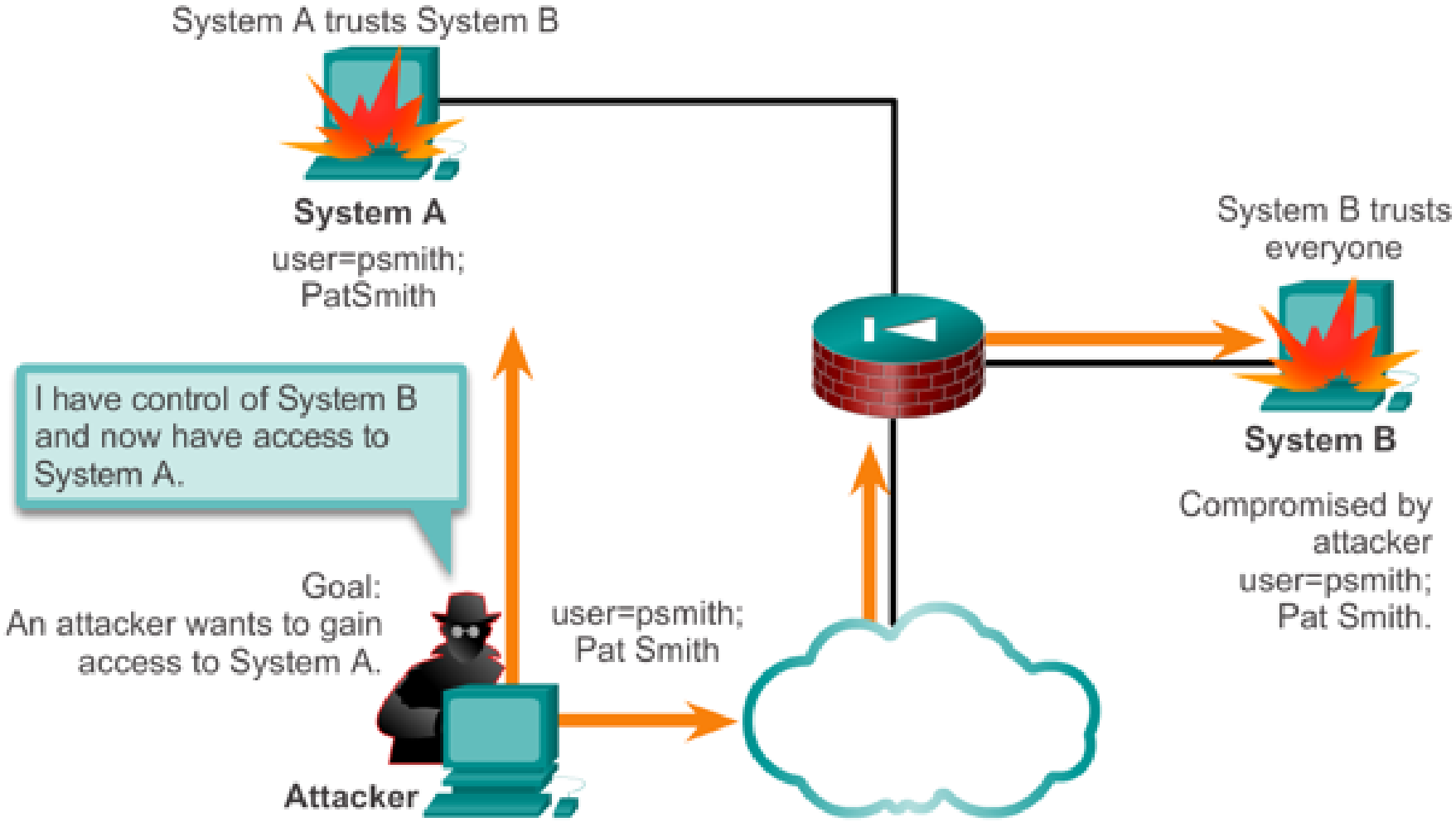
Trust Exploitation Cont.

- Ukoliko se DMZ host (neki server iz DMZ zone) napadne i kompromituje malicioznim softverom, napadač može da iskoristi poverenje između DMZ hosta i hostova unutar korporativne mreže, i da napadne hostove unutar korporativne mreže preko DMZ hosta.



B) Access Attacks

Trust Exploitation



B) Access Attacks

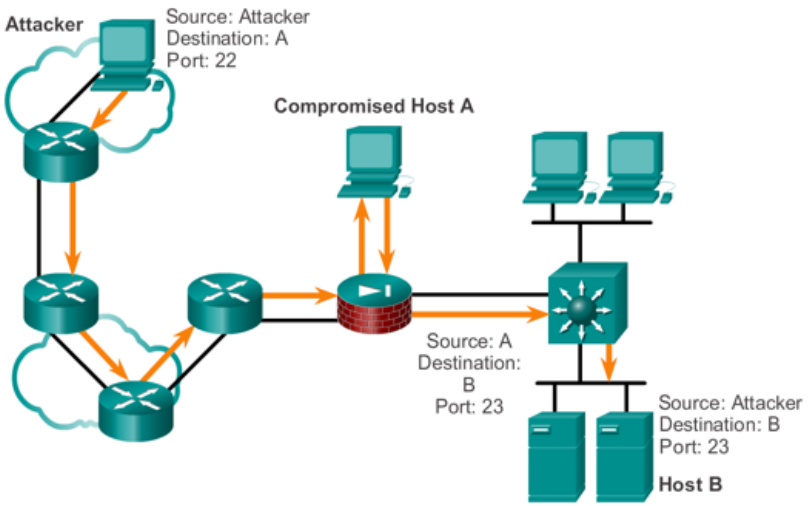
Port Redirection

- **Port redirection** je tip *trust exploitation* napada gde se host koji je prethodno inficiran i kompromitovan, šalje saobraćaj ka firewall-u koji taj saobraćaj propušta (u drugim uslovima bi ga odbio)
- Port redirection na neki način zaobilazi podešeno filtriranje saobraćaja na firewall-u, tako što menja izvorni port za određeni tip saobraćaja u mreži
- Moguće je sprečiti ovaj tip napada korišćenjem odgovarajućeg modela poverenje u mreži, njemu specifičan
- Ukoliko je sistem trenutno pod napadom, IPS može da pomogne u detektovanju napadača i spreči instalaciju malicioznog sofvera.

B) Access Attacks

Port Redirection Cont.

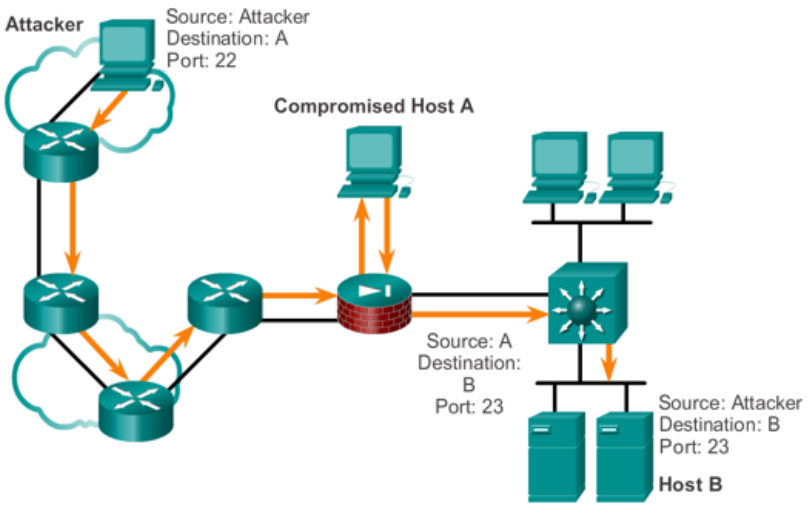
- Hostu iz spoljne mreže je dostupan host A u segmentu public services (Host A je najčešće web server ili email server koji opslužuje hostove spolja svojim servisima, drugim rečima DMZ zona servera)
- Hostu iz spoljne mreže nisu dostupni hostovi iz unutrašnje mreže (host B u ovom primeru)
- DMZ zoni mogu pristupiti i hostovi iz spoljne mreže i hostovi iz unutrašnje mreže



B) Access Attacks

Port Redirection Cont.

- Ukoliko napadač može da kompromituje rad hosta iz DMZ zone, ubacuje mu maliciozni softver koji čini da kompromitovani host vrši preusmeravanje saobraćaja od hosta iz spoljašnje mreže (napadač) ka hostu iz unutrašnje mreže (žrtva napada)
- Iako komunikacija ne narušava pravila koja su implementirana na firewall-u, host iz spoljne mreže može da pristupi hostu iz unutrašnje mreže, procesom port redirekcije na hostu iz DMZ zone



B) Access Attacks

Man-in-the-Middle Attacks (MITM)

- MITM napad je tip napada kada se napadač nađe na liniji komunikacije dva uređaja u mreži sa ciljem da utkrije slabosti njihovih sistema i pripremi se za kasniji pravi napad, ili da manipuliše podacima koji se razmenjuju između te dve posmatrane strane.
- Karakteristično za MITM napad:
  - krađa informacija
  - Krađa trenutne sesije radi pristupa internim mrežnim resursima
  - Analiza saobraćaja radi prikupljanja informacija o mreži i njenim korisnicima
  - DoS
  - Zloupotreba podataka uhvaćenih u prenosu kroz mrežu
  - Uvođenje novih informacije u postojeće sesije u mreži
- Primer MITM napada je kada neko koji ima pristup IPS sistemu je napadač i može da nadgleda sve pakete unutar saobraćaja između posmatrane mreže firme gde je IPS sistem implementiran i ostalih mreža

B) Access Attacks

Man-in-the-Middle Attacks (MITM)

- MITM napad može biti realizovan na L2 i L3 nivou.

1. MITM napad na L2 nivou:

- MITM napad na L2 nivou podrazumeva da napadač „man in the middle“ zloupotrebljava L2 MAC adrese (spoofs layer 2 mac address) i čini da ostali uređaji u LAN mreži veruju da je L2 MAC adresa napadača L2 MAC adresa *default-gateway*-a.
- Ovaj vid napada se naziva „ARP poisoning“.
- Frejmovi namenjeni default gateway-u se preko sviča usmeravaju ka napadaču koji je u istoj mreži.
- Napadač često u ovakvoj situaciji usmerava poslate frejmove ka ispravnim destinacijama kako izvorna strana ne bi posumnjala u napad, a za to vreme napadač ima prilike na nadgleda saobraćaj.
- Prevencija bi bila u korišćenju tehnike dynamic Address Resolution Protocol (ARP) inspection (DAI) na svičevima i sprečavanju „spoofing of the Layer 2 addresses“.
- Moguće je da napadač zauzme svič i da zloupotrebi Spanning Tree Protocol tako što sebe proglasi za root svič i onda ima mogućnost nadgledanja svog saobraćaj koji ide preko root sviča.

Man-in-the-Middle Attacks (MITM)

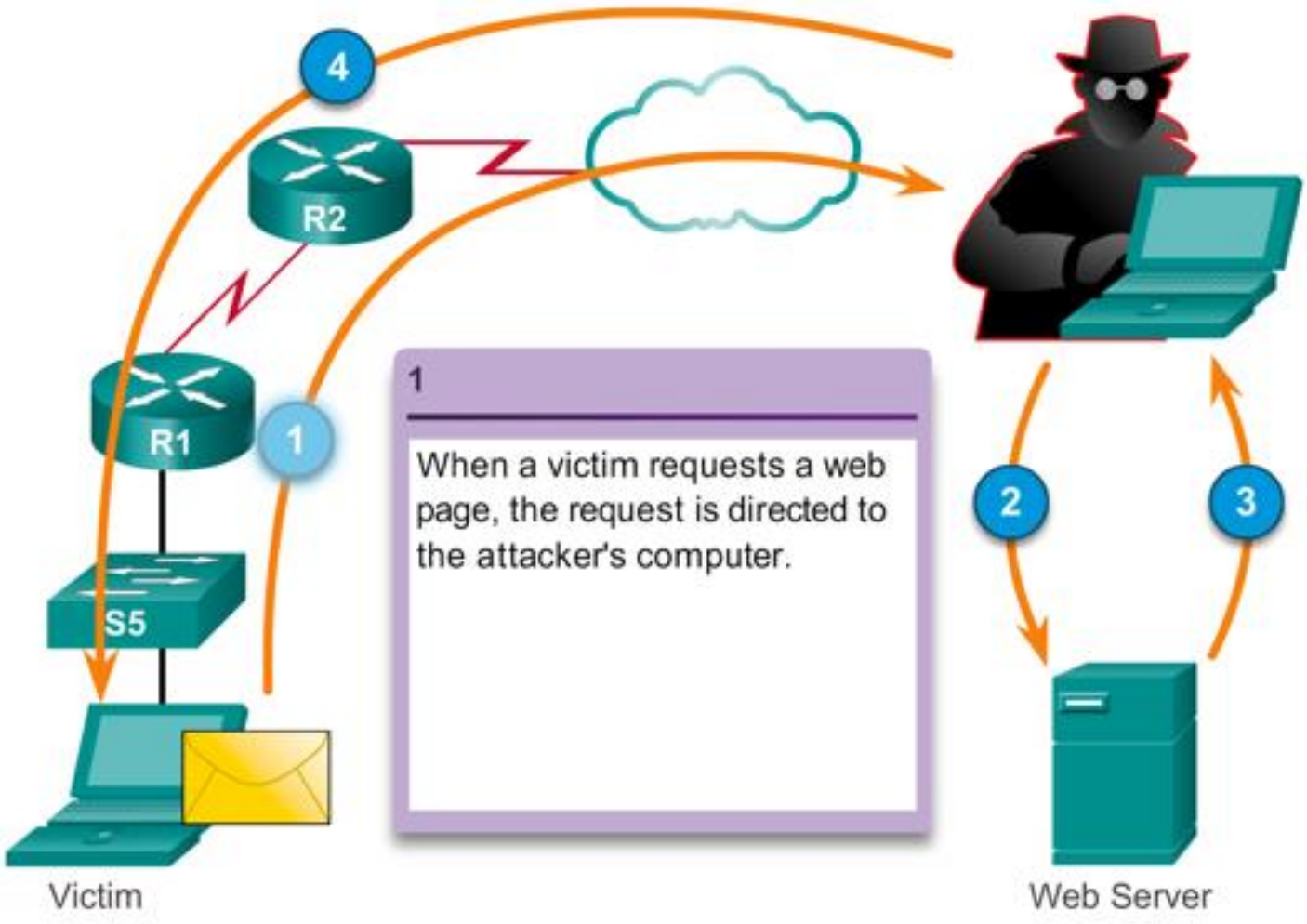
- MITM napad može biti realizovan na L2 i L3 nivou.

2. MITM napad na L3 nivou:

- MITM napad na L3 nivou podrazumeva ubacivanje lažnog rutera u mreži i navođenje ostalih rutera da veruju da lažni ruter sadrži najbolju rutu kako bi se upravo njemu prosleđivali paketi.
- Time se postiže da napadač može nesmetano da posmatra saobraćaj koji prolazi preko lažnog rutera
- Prevencija od ovog tipa napada bi bila u kriptovanju update poruka koje se razmenjuju u okviru protokola za rutiranje ili u filtriranju informacija koje se se oglašavaju ili uče na specifičnim interfejsima
- Takođe, prevencija bi bila i u korišćenju protokola i tehnike prenosa koje podrazumevaju kriptovanje poruka i saobraćaja koji se šalje kroz mrežu (SSH, HTTPS, VPN...)

B) Access Attacks

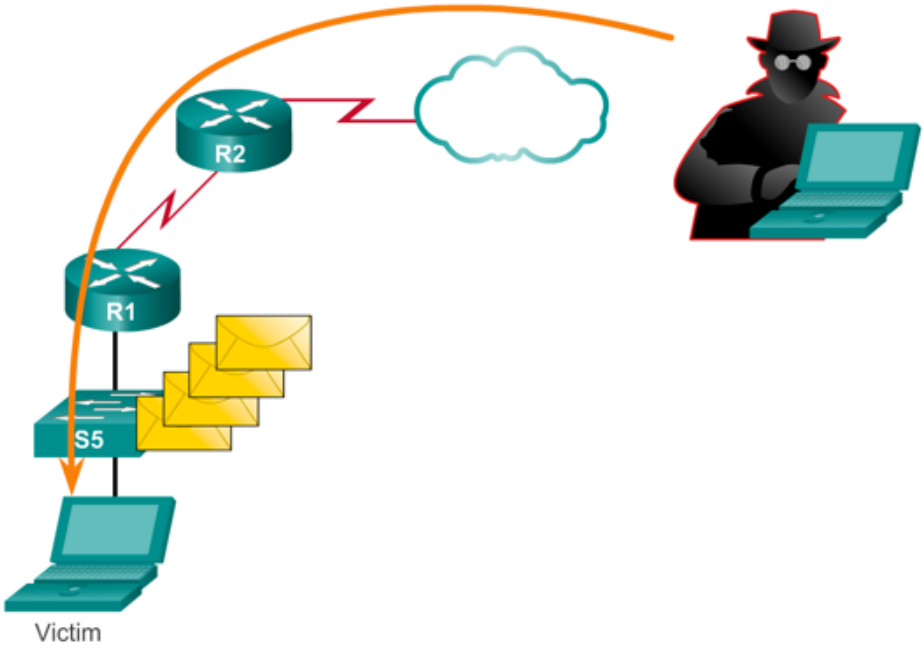
Man-in-the-Middle Attacks (MITM) Cont.



B) Access Attacks

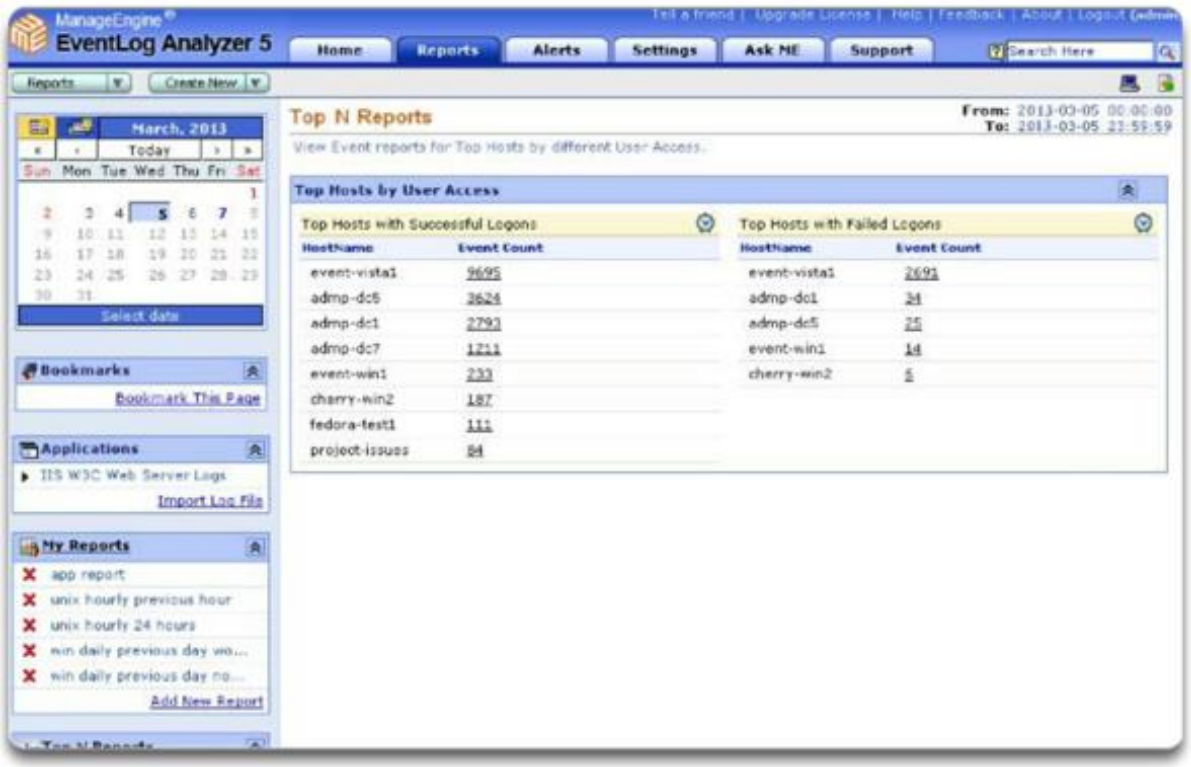
Buffer Overflow Attacks

- **Preopterećenje bafera pristizanjem velikog broja paketa**
- U jednom trenutku program počinje da upisuje podatke van memorije bafera
- Buffer overflows obično nastaje zbog baga u C ili C++ programu
- Rezultat ove vrste napada jeste da se validan podatak iz memorije briše upisivanjem drugog podatka na njegovom mestu u memoriji, što dalje omogućava delovanje malicioznog koda
- The overflow napad se može koristiti za menjanje promenljivi u kodu programa čime se menjaju validne instrukcije koje bi ispravan program inače zadao.



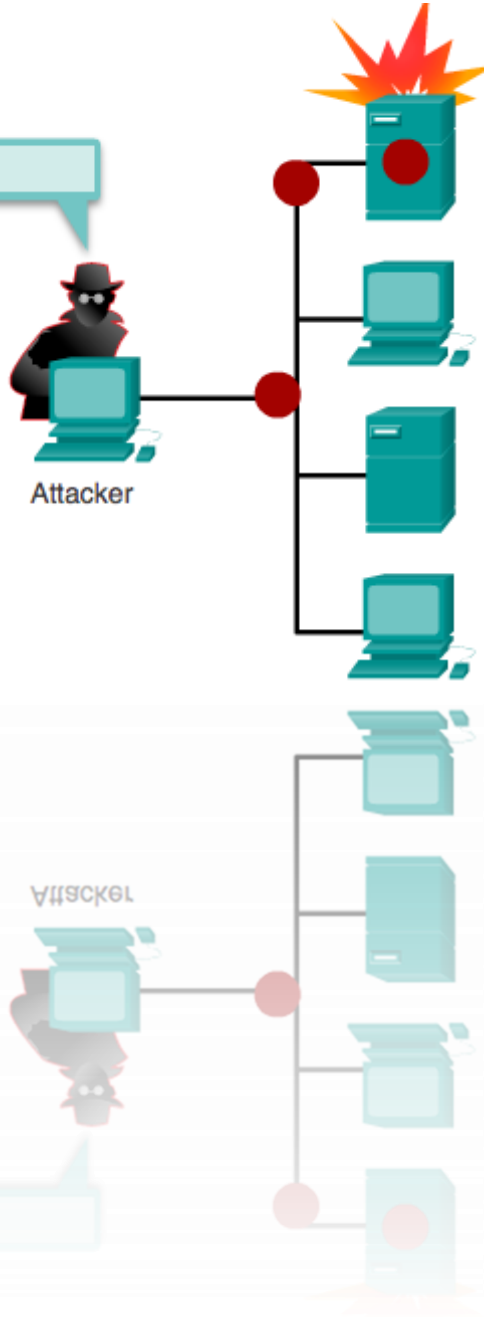
Mitigating Access Attacks

- **Kako sprečiti Access attacks napade?**
- Generalno se ovi tipovi napada mogu detektovati pregledom i analizom log informacija, iskorišćenja propusnog opsega, opterećenja procesa.
- Potrebno je specificirati polisama bezbednosti, *The network security policy,* da je neophodno nadgledati log poruke svih mrežnih uređaja i servera



C) DoS Attack

- **DoS** napad (napad uskraćivanjem usluge) je pokušaj da se legitimnim korisnicima uskrati korišćenje nekog servisa
- To je mrežni napad koji rezultira nekom vrstom prekida normalnog rada servisa korisnika, uređaja ili aplikacija
- DoS napad potiče od jednog uređaja u mreži
- DoS napad nastupa kad:
  - host ili aplikacija prekida sa radom zbog toga što nije u mogućnosti da adekvatno odgovori na neočikivano izmenjene uslove rade, kao što su:
    - Ulazni podatak je maliciozno promenjen
    - neočekivana interakcija sa drugim sistemskim komponentama
    - Iscrpljivanje resursa.
  - Mreža, host ili aplikacija nisu u stanju za opsluže ogroman broj podataka (npr. zahteva), što čini rad sistema oborenim ili jako usporenim

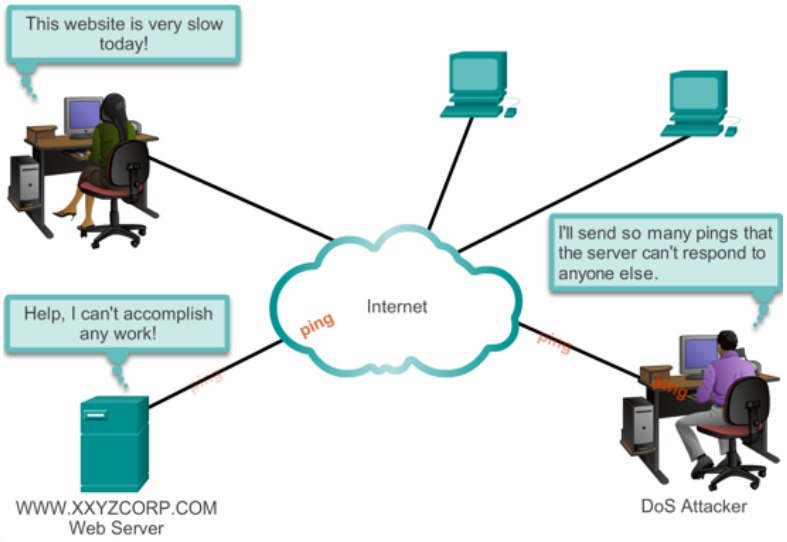


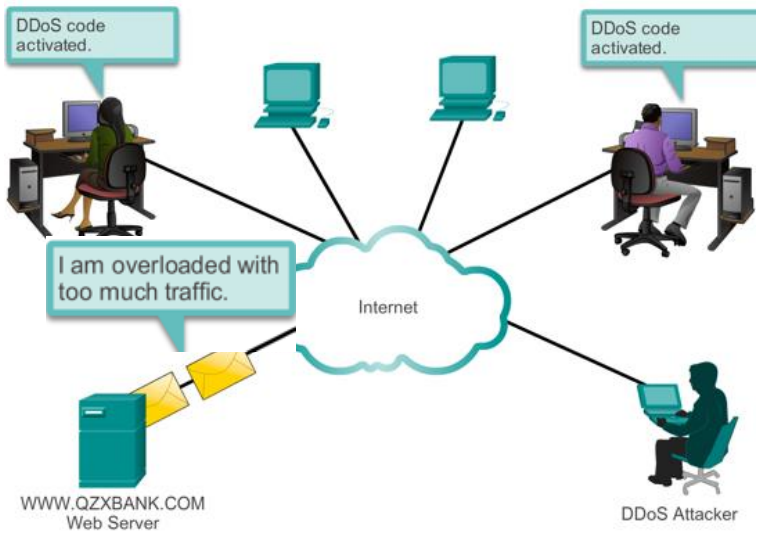
DoS i DDoS

Distributed DoS Attack – **DDoS** (Distribuirani napad uskraćivanjem usluge) je napad koji dovodi do toga da računarski sistemi (resursi) postanu nedostupni tako što se serveri, mreže, pa čak i sistemi krajnjih korisnika preplave beskorisnim informacijama, i legitimni korisnici više ne mogu da priđu tim resursima

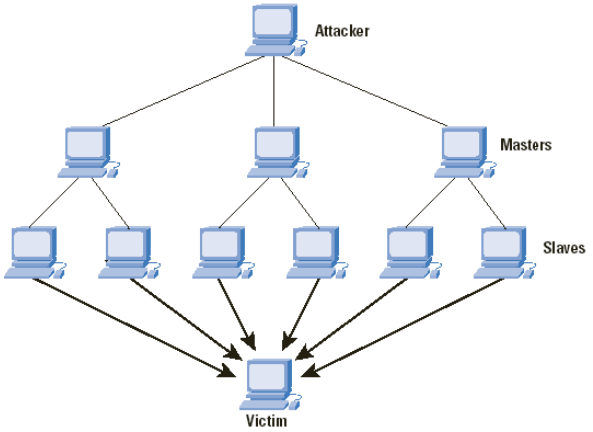
DDoS napad pokušava da potroši resurse cilja, tako da napadnuta strana ne može da pruža usluge.

DDoS napad se izvršava od strane velikog broja zaraženih računara (**botova**) čije je delovanje koordinisano - **Botnet**

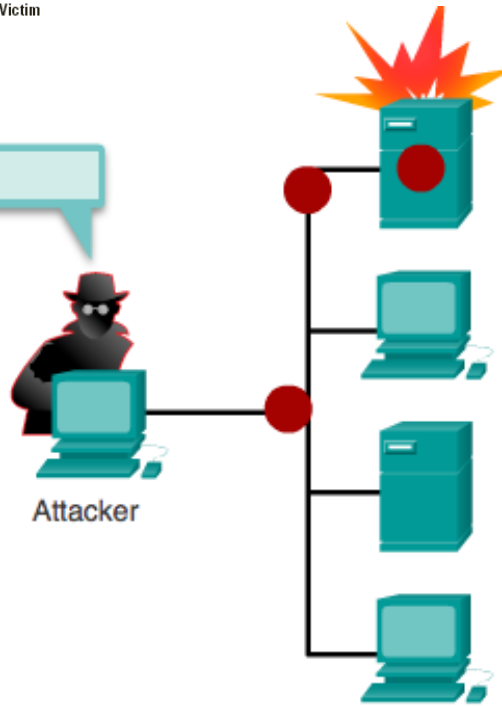




C) DDoS Attack



- **Klasifikacija DDoS napada:**
- **Direktni DDoS napad**
- Napad u kome izvor napada generiše i šalje veliki broj paketa (nevezano od protokola, aplikacije itd) direktno žrtvi napada
  - napadač preuzima kontrolu nad grupom računara preko Interneta, uspeva da ih zarazi i usadi u njima odgovarajući „zombi“ maliciozni softver (često DDoS napad uključuje dva nivoa „zombi“ mašina: glavne i podređene „zombi“ mašine).
  - Napadač koordinira i pokreće glavne „zombi“ mašine koje potom koordiniraju i pokreću podređene „zombi“ mašine. Zaraženi uređaji na zahtev napadača šalju veliki broj ICMP echo pakete koji preopterećuju cilj i čini njegovovo normalno funkcionisanje nemogućim

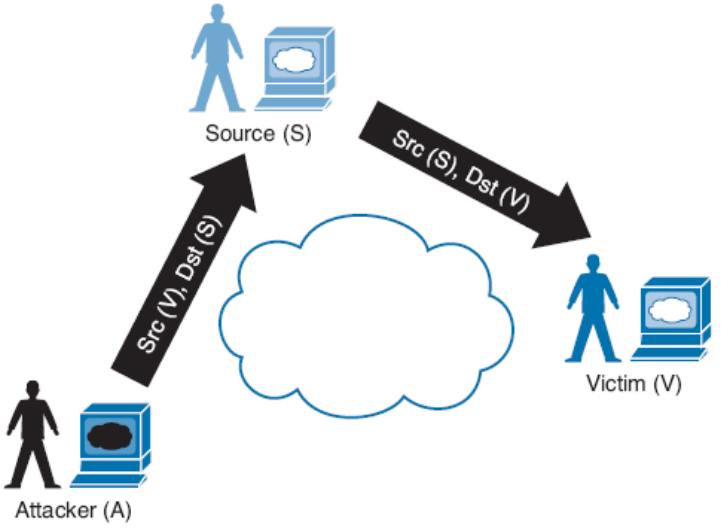


C) DDoS Attack

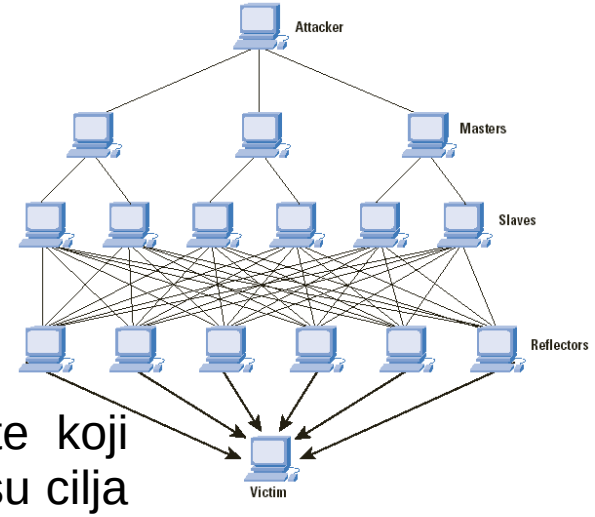
- **Klasifikacija DDoS napada:**
- **Reflektovani DDoS (RDDoS) napad**

- Izvor napada je nesvesni učesnik koji šalje *spoofed* paket (paket sa „ukradenom“ IP adresom žrtve) ka žrtvi kao odgovor na zahtev. Zahtev je prethodno nesvesni učesnik dobio od pravog izvora napada (napadača), a ne od žrtve. Napadač je u paketu zahteva uneo izvornu IP adresu žrtve koju je nekako ukrao (sniffing metoda) i nesvesni učesnik je zbog toga ubeđen da je paket stigao od žrtve kojoj treba onda i odgovoriti (ne od pravog napadača.

- **Reflected:** Reflektovani DDoS napadi se javljaju kada se izvorima napada pošalju lažni paketi koji kao da se pojavljuju od žrtve, a onda izvori postaju neviđeni učesnici u DDoS napadima tako što šalju odgovor žrtvi. UDP se često koristi kao mehanizam transporta jer je nesiguran. Na primer, ako napadač (A) odluči da napadne žrtvu (V), on će poslati pakete (na primjer, zahteve za mrežni protokol [NTP]) do izvora (S) koji smatraju da su ovi paketi legitimni. Izvori (S) odgovaraju zahtevima NTP slanjem odgovora žrtvi (V), koja nikada nije očekivala ove NTP pakete od izvora (S)



C) DDoS Attack



- **Klasifikacija DDoS napada:**
- **Reflektovani DDoS (RDDoS) napad**
  - U ovoj vrsti napada podređeni zombiji prave pakete koji zahtevaju odgovor, a zaglavlju paketa sadrže IP adresu cilja (žrtve) kao izvornu IP adresu
  - Ti paketi se šalju nezaraženim mašinama poznatijim kao reflektori
  - Nezaražene mašine (reflektori) odgovaraju paketima usmerenim na ciljanu metu
  - Reflektovani DDoS napad lako može da uključi više računara i više saobraćaja nego direktni DDoS napad i samim tim je mnogo štetniji.
  - Teže se ulazi u trag napadu i filtrirnje paketa napada je teže zato što napad stiže sa široko razuđenih nezaraženih mašina

C) DDoS Attack

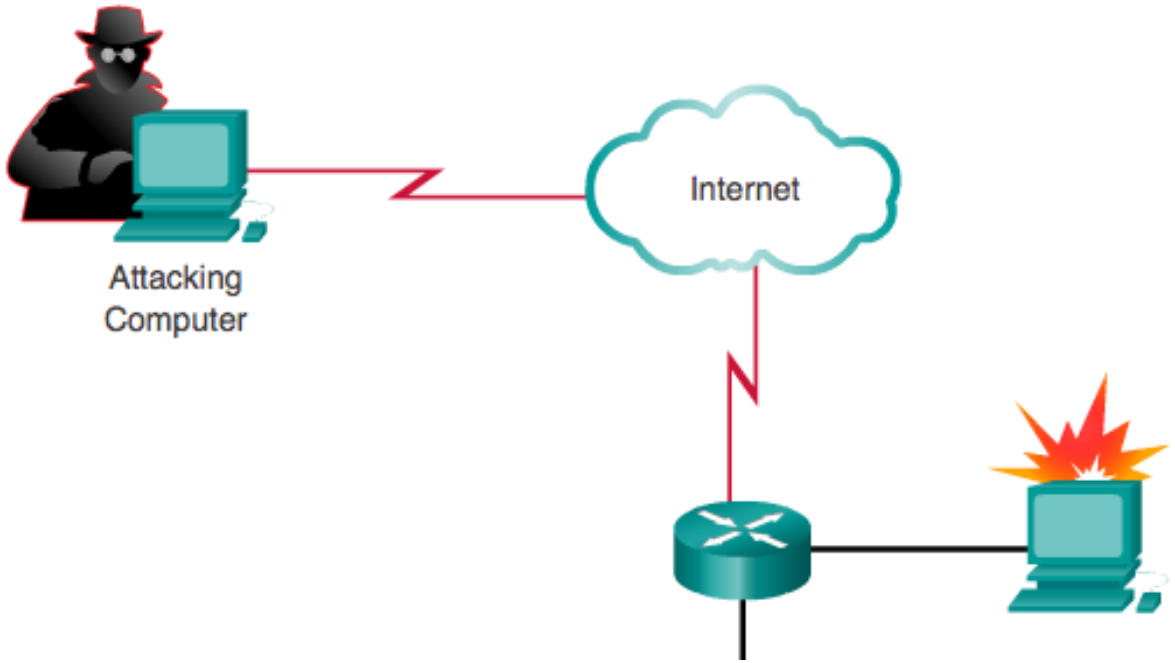
- **Klasifikacija DDoS napada:**
- **Amplification DDoS napad**
- „Amplification attacks“ pripada grupi reflektovanih DDoS napada gde nesvesni učesnici šalju odgovor žrtvi napada kao odgovor na zahtev koji su prethodno dobili od pravog napadača
- Odgovor je zapakovan u paketu znatno veće veličine nego što je to bio paket zahteva
- Primer ovoga je kada su DNS odgovori mnogo veći od inicijalnih paketa upita. Krajnji rezultat je da se žrtva poplavi velikim paketima za koje nikada nije izdao upite.

Tipovi DoS i DDoS napada

- Among the most difficult to completely eliminate because they require so little effort to execute. Spadaju među najteže da se u potpunosti eliminišu zato što zahtevaju premalo napora da se izvrše
- Tipovi DoS napada uključuju:
  - **Ping of death**
  - **Smurf Attack**
  - **TCP SYN flood attack**

Ping of Death

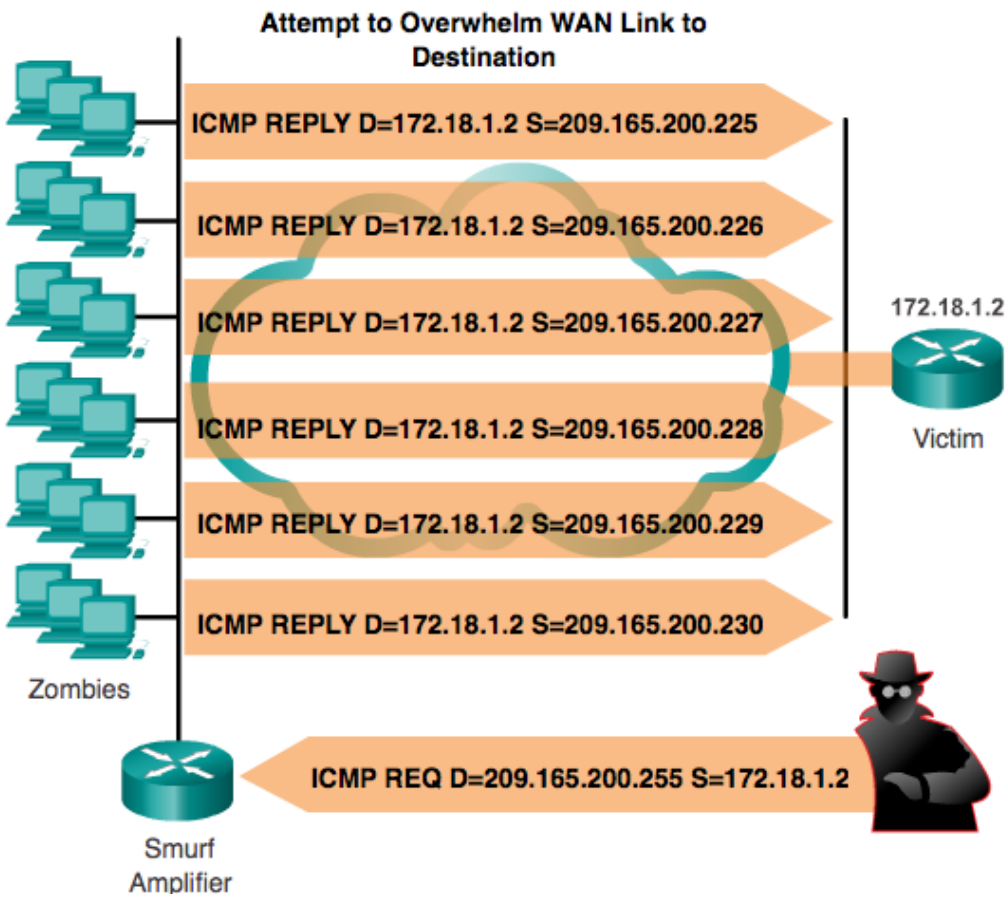
- Ovim tipom napada se šalju echo request zahtevi u IP paketima koji su duži od maksimalne dužine IP paketa (65,535 bytes).
- Slanje pinga ove dužine obara sistem napadnutog računara
- Posebna vrsta ovog napada je slanje ICMP fragmenata koji popunjavaju buffers napadnutog uređaja



C) DoS Attacks

Smurf Attack

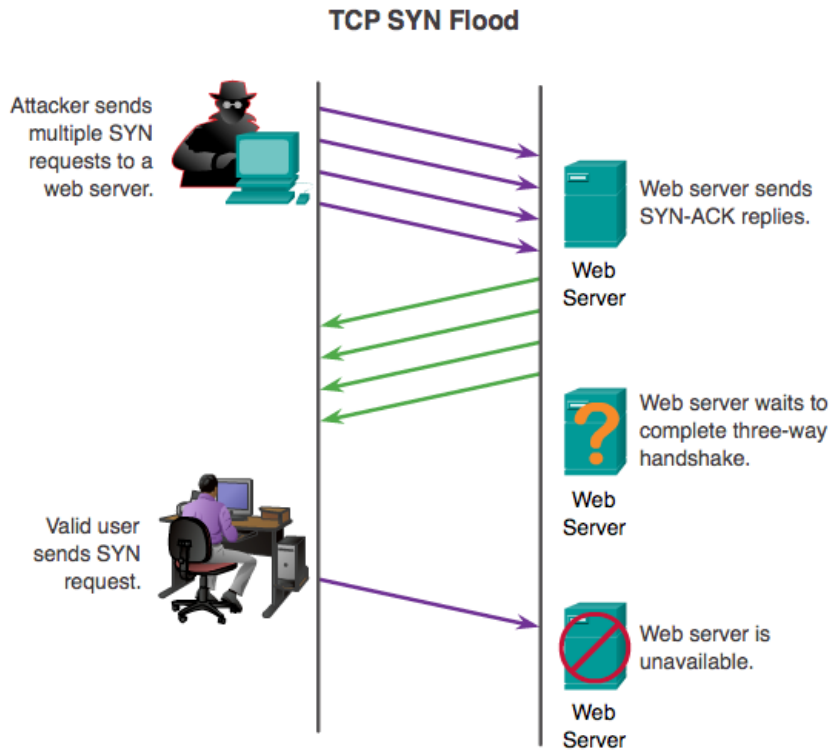
- Pripada grupi direktni i reflektovani DDoS napadi
- A Smurf Attack je tip DDoS napada gde se veliki broj ICMP paketa sa ukradenom izvornom IP adresom (victim's spoofed source IP) šalje broadcast u računarsku mrežu.
- Na stotine uređaja koji primaju icmp pakete odgovaraju na svaki paket, šaljući ih kao icmp odgovor na adresu ciljane žrtve, koja time biva preplavljena icmp replay paketima.



SYN Flood Attack

TCP SYN paketi se šalju u ogromnom broju sa pogrešnim informacijama izvorne IP adrese onoga ko šašlje zahtev

- Svaki paket nosi zahtev za uspostavljanjem TCP konekcije sa serverom
- Server na pristigli zahtev šalje TCP SYN-ACK paket hostu i čeka njegov odgovor (odgovor sa izvorne adrese)
- S obzirom da je izvorna adresa pogrešna, odgovora-potvrde neće nikad stići do servera
- Na ovaj način ostaju otvorene *half-open* konekcije na serveru čime se rad servera drastično usporava (server prima veliki broj ovakvih zahteva tokom napada)
- Legitimne konekcije se odbijaju dok server žrtva čeka da kompletira „half-open“ konekcije



Symptoms of a DoS Attack

Pet različitih posledica koje DoS napad može načiniti:

a) Zauzimanje resursa: bandwidth, disk space, ili processor time.

b) Narušavanje konfiguracionih informacija, npr. informacija o rutiranju

c) Narušavanje statusa poput neželjenog resetovanja TCP sesija

d) Narušavanje rada fizičkih mrežnih komponenti

e) Opstrukcija komunikacije između žrtve i ostalih uređaja u mreži

Protiv mere za DDoS napad

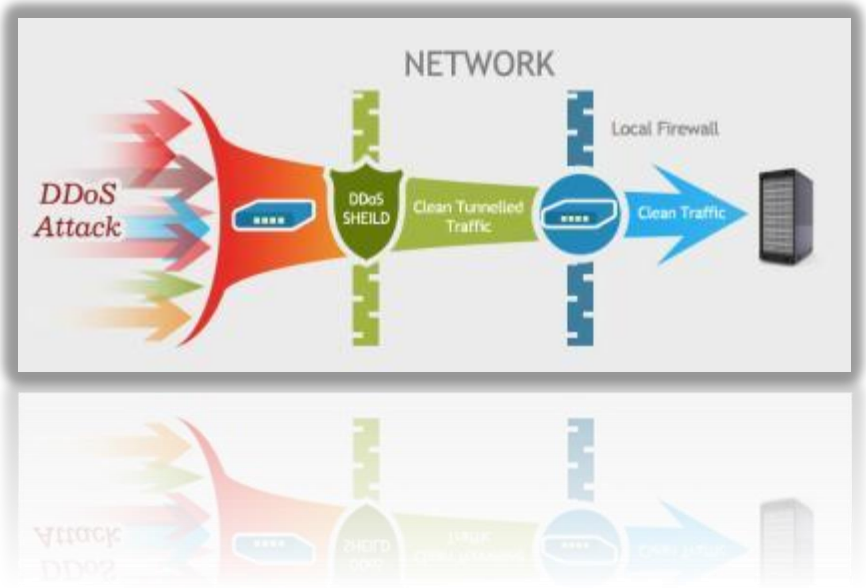
1) Sprečavanje i predupređivanje napada (pre napada)

- Ovi mehanizmi omogućavaju žrtvi da izdrži pokušaje napada, a da pri tom ne uskrati usluge legitimnim klijentima.
- Tehnike obuhvataju nametanje polisa za trošenje resursa i obezbeđivnje rezervnih resursa raspoloživih na zahtev.
- Pored toga, mehanizmi za sprečavanje menjaju sisteme i protokole na Internetu kako bi se smanjila mogućnost DDoS napada

Protiv mere za DDoS napad

2) Otkrivanje i filtriranje napada

- Ovi mehanizmi pokušavaju da uoče napad na samom početku i potom odmah reaguju
- Tako se uticaj napada na cilj svodi na minimum
- Otkrivanje podrazumeva potragu za sumnjivim obrascima ponašanja.
- Reagovanje podrazumeva filtriranje paketa koji mogu biti deo napada



Protiv mere za DDoS napad

3) Ulaženje u trag i identifikacija izvora napada (za vreme napada i posle njega)

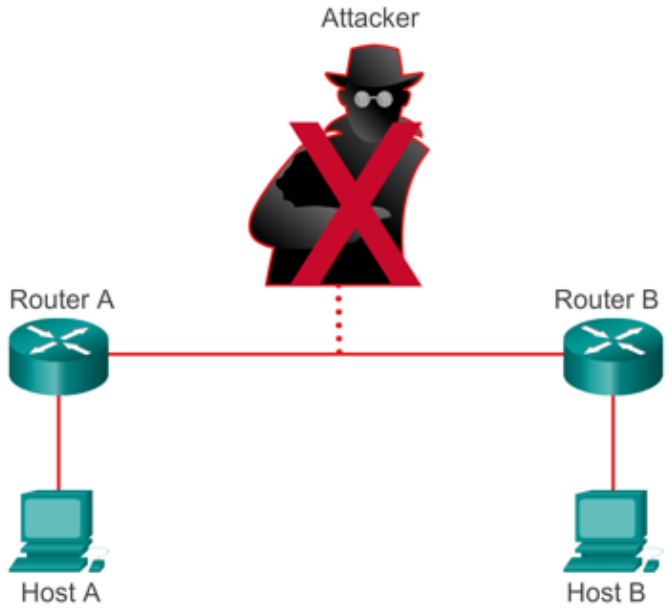
- Ovo predstavlja pokušaj da se identifikuje izvor napada kao prvi korak u sprečavanju budućih napada
- Ovaj metod obično ne daje rezultate dovoljno brzo, da bi se ublažio napad koji je već u toku

Prevencija napada u računarskoj mreži

Tipovi napada, označeni kategorizacijom poput izviđanja, pristupa ili DoS napada, određuju načine ublažavanja pretnje mreži

Prevencija od *Reconnaissance* napada

- Implementacija i dosledno sprovođenje polisa bezbednosti kojima se zabranjuje korišćenje protokola koji su osetljivi na prisluškivanje
- Korišćenje enkripcije podataka
- Korišćenje anti-sniffer alata za detekciju *sniffer attacks* napada.
- Korišćenje switched networks.
- Korišćenje firewall-a and IPS sistema.



Prevencija od Access napada

- Tehnike za ublažavanje Access napada uključuju:
  - Jake lozinke
  - Princip minimalnog poverenja
  - Kriptografija
  - Primena patch-eva za operativne sisteme i aplikacije

Prevencija od DoS napada

- IPS and firewalls (Cisco ASAs and ISRs)
- Antispoofing technologies
- Quality of Service-traffic policing

Prevencija od DoS napada

- **Anti-DoS features** on routers and firewalls:
  - Odgovarajuća konfiguracija anti-DoS features na routerima i firewall-ovima može pomoći u smanjenju efikasnog DoS napada
  - Anti-DoS features konfiguracija može da uključi **ograničenje broja half-open TCP konekcija** koju sistem može da dozvoli u nekom trenutku
- **Anti-spoof features** on routers and firewalls:
  - Takođe, odgovarajuća konfiguracija anti-spoof features na routerima i firewall-ovima može pomoći u smanjenju rizika od DoS napada
  - Anti-spoof features uključuju **adekvatno filtriranje sa pristupnim listama**, unicast reverse path forwarding that looks up the routing table to identify spoofed packets, disabling of source route options, and others.

Prevencija od Port Scan and Ping Sweep

- Port scanning i ping sweeping nije zločin i ne postoji način za zaustavljanje ovih scan-ova i sweep-ova kada je računar povezan na Internet.
- Ping sweeps može da se zaustavi ako se ICMP echo i echo-reply isključe na edge ruterima, međutim tada su i podaci o mrežnoj dijagnostici izgubljeni.

Prevencija od Packet Sniffer-a

- Authentication
  - Jaka autentifikacija (provera identiteta) predstavlja prvu liniju odbrane.
- Cryptography
  - Ukoliko je komunikacioni kanal zaštićen kriptovanjem podataka, jedine podatke koje „sniffer“ može da detektuje jeste kriptovan tekst.
- Anti-sniffer tools
  - „Anti-sniffer“ alati detektuju promene u dužini vremena potrebno hostu za odgovor na neki zahtev, čime se može zaključiti da posmatrani host procesira više saobraćaja nego što je to uobičajeno za njega i samim tim se može posumnjati da posmatrani host možda koristi neki od „sniffing“ alata za analizu saobraćaja
- Switched infrastructure
  - Mreža u čijoj se infrakstrukturi koriste svičevi može u značajnoj meri da redukuje efikasnost „sniffer“ aktivnosti. Odgovorajuća konfiguracija svičeva je neophodna.

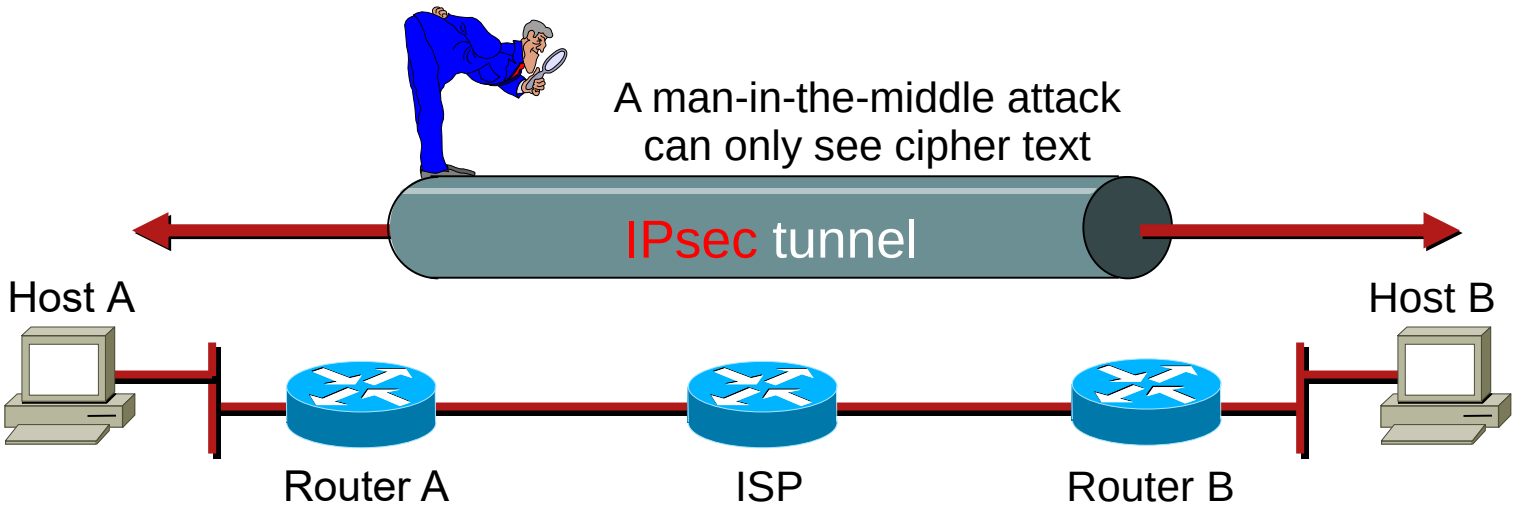
Prevencija od Password Attacks

Tehnike ublažavanja Password attack-a uključuju:

- Ne dozvoliti korisnicima da koriste istu lozinku na više sistema.
- Onemogućiti naloge nakon određenog broja neuspešnih prijava. Ova praksa pomaže u sprečavanju kontinuiranih napada na lozinku
- Preporučuje se korišćenje OTP (One-Time Password - password validan samo za jednu sesiju logovanja) ili kriptovanih lozinki.
- Ne koristiti čisti tekst za lozinke.
- Koristiti jake lozinke. Jaka lozinka ima najmanje osam karaktera i sadrži velika i mala slova, brojeve i posebne znakove.

Man-in-the-Middle Mitigation

Man-in-the-middle napad se može uspešno ublažiti jedino korišćenjem šifrovanja (encryption).



10 najboljih praksi

1. Postavljati patch-eve redovno (nedeljno ili dnevno), kako bi se sprečilo preopterećenje bafera i eskalacija napada.
2. Isključiti nepotrebne servise i portove.
3. Koristiti jaku lozinku i često je menjati.
4. Kontrolisati fizički pristup sistemu.
5. Izbegavajte nepotrebne unose na web stranici:
   - Neki web sajtovi dozvoljavaju korisnicima da unesu korisničko ime i lozinku.
   - Hacker može uneti više od običnog korisničkog imena.
   - Na primer, unošenje **jdoe; rm -rf /** može dozvoliti napadaču da izbriše root file system sa UNIX servera.
   - Programer bi trebalo da obezbedi da se limitiraju ulazni karakteri i da se ne prihvataju neodgovarajući karaktere, poput | ; < >

10 najboljih praksi

6. Praviti rezervne kopije i testirati ih.
7. Obučiti zaposlene o rizicima socijalnog inženjeringa i razvijati strategije za potvrđivanje identiteta preko telefona, putem e-pošte ili lično.
   - http://www.networkworld.com/news/2010/091610-social-networks.html?source=NWWNLE_nlt_daily_pm_2010-09-16
   - http://searchsecurity.techtarget.com/news/1519804/Phishing-attacks-target-users-of-Facebook-other-social-networks?asrc=EM_NLN_12420860&track=NL-102&ad=784799&
8. Šifrovati i zaštititi lozinkom osetljive podatke.
9. Implementirati bezbednosni hardware i software poput firewalls, Intrusion Prevention Systems (IPSs), Virtual Private Network (VPN) uređaja, antivirus software, and content filtering.
10. Razviti pisanu bezbednosnu politiku za kompaniju.