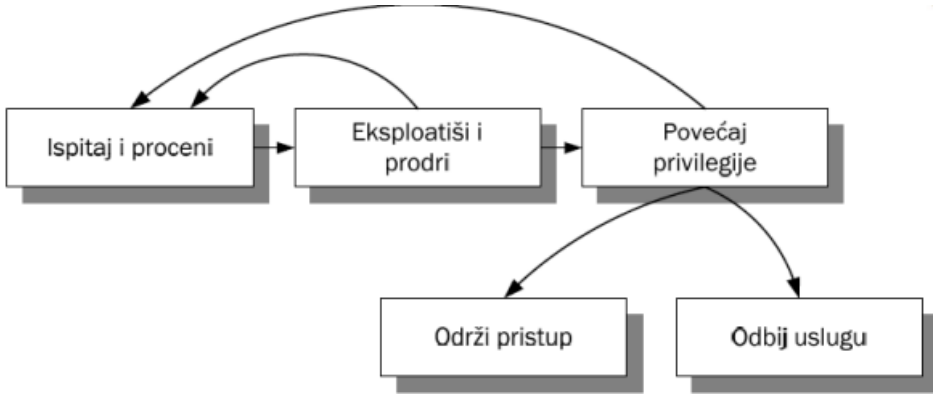
PRETNJE, NAPADI, SIGURNOST I METODE ZAŠTITE

Predmet: Zaštita podataka u komunikacionim mrežama

Predavač: dr Dušan Stefanović

PRIPREMA ZA NAPAD I NAPAD

1. **Ispitaj i proceni (survey and assess) -** istražne radnje radi ispitivanja potencijalne mete i indentifikovanje i procena njenih karakteristika.
2. **Eksploatiši i prodri** (exploit and penetrate) - pokušava da eksploatiše ranjivost i da prodre u mrežu ili sistem.
3. **Povećaj privilegije** (escalate privileges) - Nakon ubacivanja (injecting) koda u aplikaciju, pokušava da poveća svoja prava
4. **Održi pristup** (maintain access) - preduzima korake da olakša buduće napade i da prikrije tragove (back-door programi, brisanje log fajlova)
5. **Odbij uslugu** (deny service) - ako ne može da pristupi sistemu, preduzima napad koji prouzrukuje odbijanje usluge (DoS napad)



Ranjivost sistema

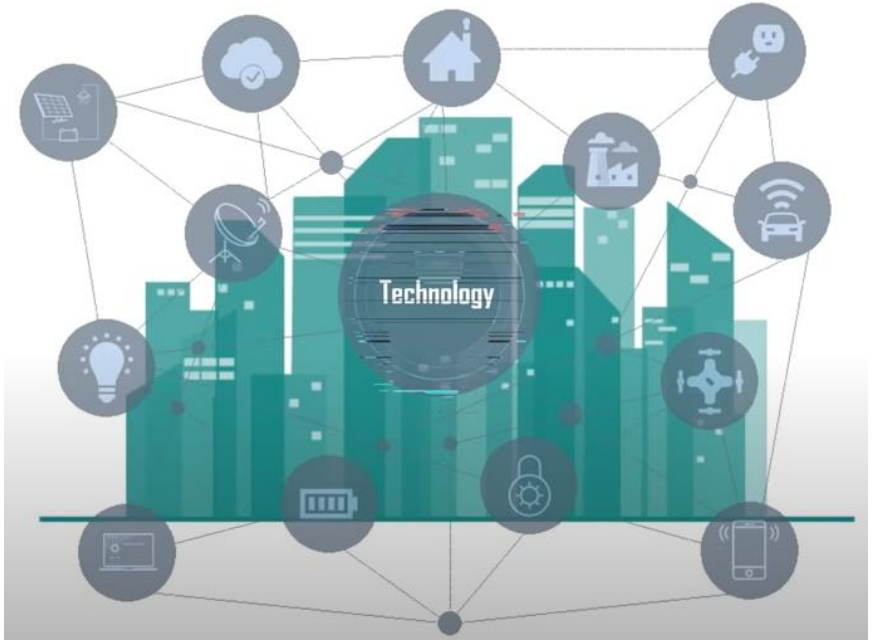
Dizajn sistema

Loša konfiguracija sistema

Nebezbedna mreža

Složenost sistema (sistem se oslanja na raznovrsne tehnologije)

Ljudske greške (deljenje lozinke)



TESTIRANJE PROBOJNOSTI SISTEMA (PEN TEST)

Pen test je simulirani cyber security napad radi provere i procene bezbednosti IT sistema

Proaktivni načini testiranja informacionog sistema izvršavanjem napada koji su slični stvarnim napadima

Način da se otkriju slabosti sistema na serveru, mreži ili aplikaciji da bi se odredio nivo neautorizovanog pristupa ili druga maliciozna aktivnost (dubina kompromitovanja mete)

Svrha Testiranja Proboja sistema

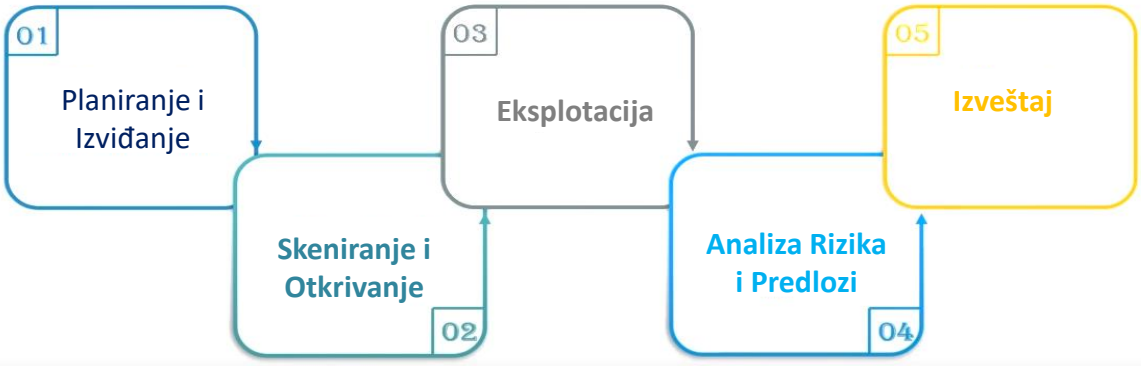
Otkrivanje ranjivosti sistema

Testiranje osoblja na primeni bezbedonosnih procedura

Proveri svest osoblja na bezbedonosne pretnje

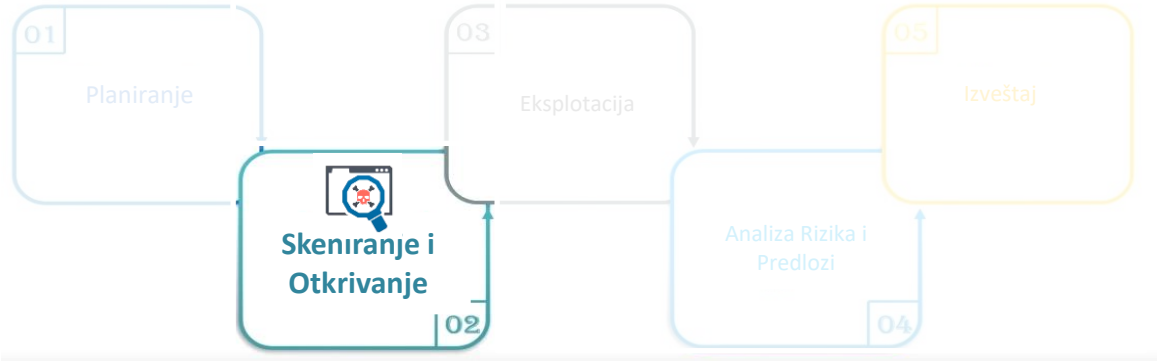
FAZE U SPROVOĐENJU PEN TESTA

- Faza 1
  - Sakupljanje što više informacija o meti napada
- Faza 2
  - Identifikovanje ranjivosti u sistemu skeniranjem sistema
- Faza 3
  - Eksplotacija – sprovođenje napada na uočene ranjivosti u sistemu
- Faza 4
  - Analiza svake ranjivosti i njen uticaj na bezbednost sistema
- Faza 5
  - Detaljan izveštaj koji sumarizuje rezultate testiranja



Faza 1 - Planiranje

- Definisanje ciljeva i opseg testiranja
- Sakupljanje što više informacija o meti
  - IP adrese
  - Detalji vezani za domen
  - Email servis
  - Opis mrežne topologije
  - Vrsta sistema koja je izabrana za metu
- Izbor metode testiranja



Faza 2 - Skeniranje

Napadač interaguje sa metom da bi identifikaovao ranjivosti (slabe tačke) u konfiguraciji servera, mrežne infrastrukture i aplikacije.

Skeniranje mreže i servisa primenom raznovrsnih alata za detekciju

- Deljenih foldera (shared drives)
- Otvorenih portova (FTP, HTTP, ...)
- Servisa koji se izvršavaju

Skeniranje aplikacija

- Statičko

  Otkrivanje ranjivih biblioteka, funkcija i implementacione logike

- Dinamičko

  Inspekcija koda u toku rada aplikacije (real time app inspection) prosleđivanjem aplikaciji različite ulazne parametre i praćenje ponašanja aplikacije

Faza 3 – Eksplotacija (Izvršenje)

- Izvršava se napad na ciljani sistem na isti način an koji bi napad izvršio pravi napadač
- Cilj je pristupiti podacima tj. kompromitovati računarski sistem, mrežu ili aplikaciju.
- Zahteva se visoki nivo ekpertize testera

Faza 4 – Analiza

- Prilog sa dokazima o izvršenoj eksplotaciji tj. kompromitovanju sistema
- Kategorizacija rizika
  - Critical
  - High
  - Medium
  - Low
- Izveštavanje klijenta o sprovedenim rezultatima testiranja i definisanje korektivnih mera za unapređenje bezbednosti sistema

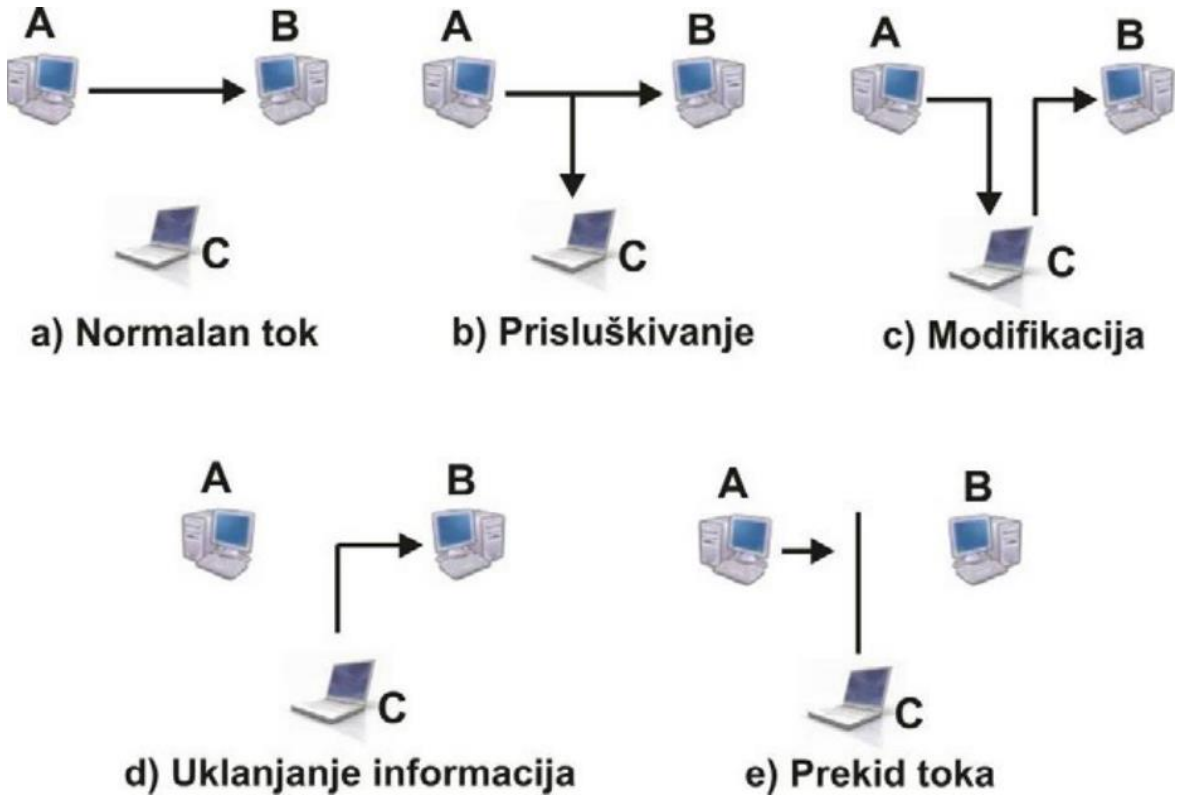
Faza 5 – Finalni izveštaj

- Uključuje sve sprovedene aktivnosti od otkrivenih ranjivosti u sistemu do predloga za njihovo uklanjanje

VRSTE NAPADA

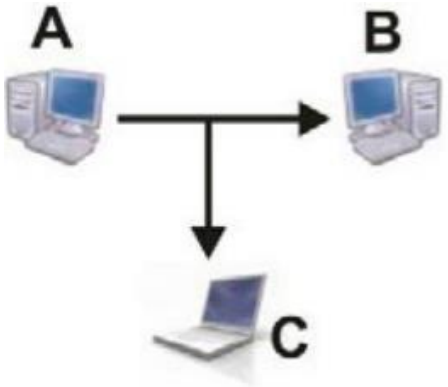
Napadi predstavljaju akcije koje su usmerene na ugrožavanje sigurnosti informacija, računarskih sistema i mreža.

Postoje različite vrste napada koji se mogu svrstati u više kategorija

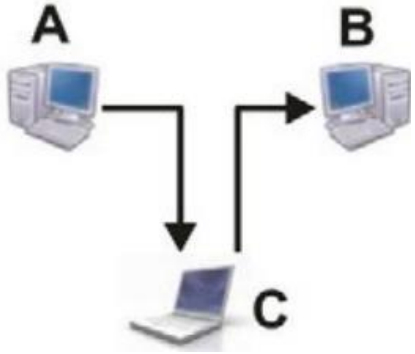


VRSTE NAPADA

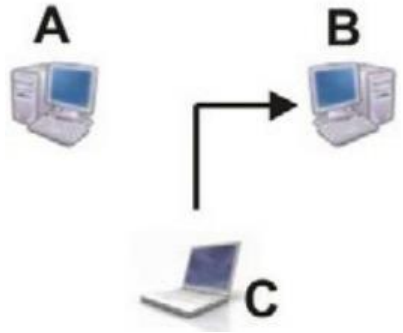
Presretanje (interception) - napad na poverljivost (confidentialy).
Prisluškivanje sabraćaja, nadziranje njegovog intenziteta i uvid u osetljive informacije



Izmena (modification) - napad na integritet (integrity)
Osnovni cilj je neovlašćeno brisanje, umetanje ili izmena podataka.



Uklanjanje - napad na autentičnost (authenticity).
Napadač izvodi ovaj aktivni napad tako što generiše lažne podatke, lažni saobraćaj ili izdaje neovlašćenje komande.

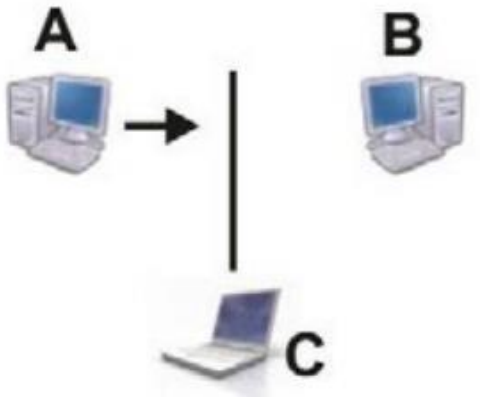


VRSTE NAPADA

Prekid (interruption) - napad na raspoloživost (availability).

Ovim načinom se prekida tok informacija, čime se onemogućava pružanje usluge.

Napadi radi „gušenja“ usluga **(Denial of Service-DOS)**
Onemogućavaju ovlašćenim korisnicima pristup resursima i njihovo korišćenje



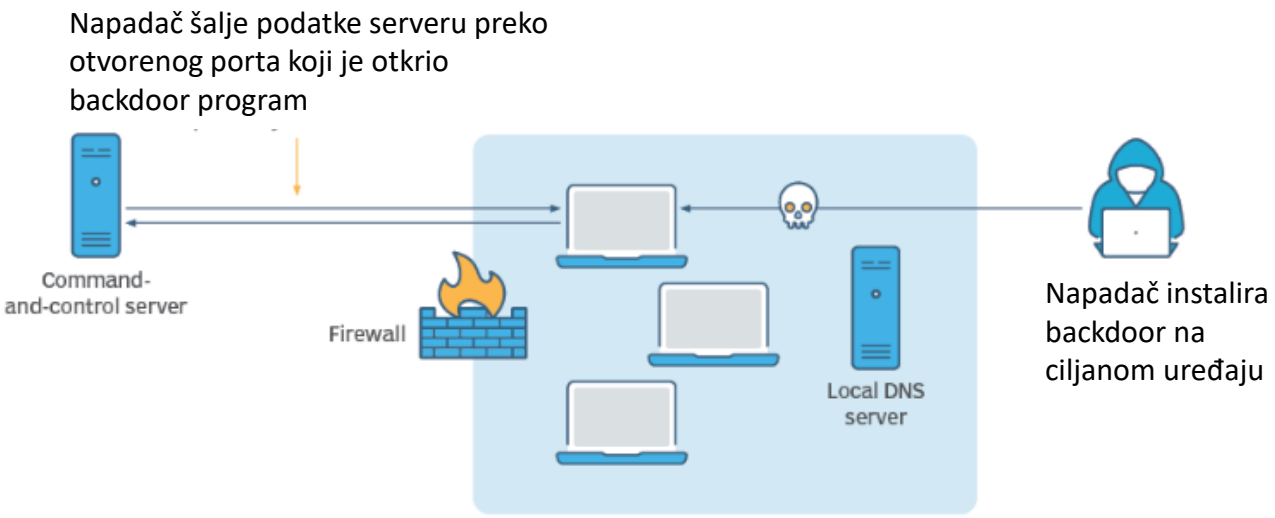
BACKDOOR NAPAD

Backdoors su skriveni mehanizmi koje napadači koriste za pristup **sistemu bez autentifikacije.**

Prodavci ponekad kreiraju backdoor u legitimne svrhe, kao što je vraćanje izgubljene lozinke korisnika ili omogućavanje vladinim subjektima pristup šifrovanim podacima.

Ostala pozadinska vrata su stvorena i instalirana od strane hakera.

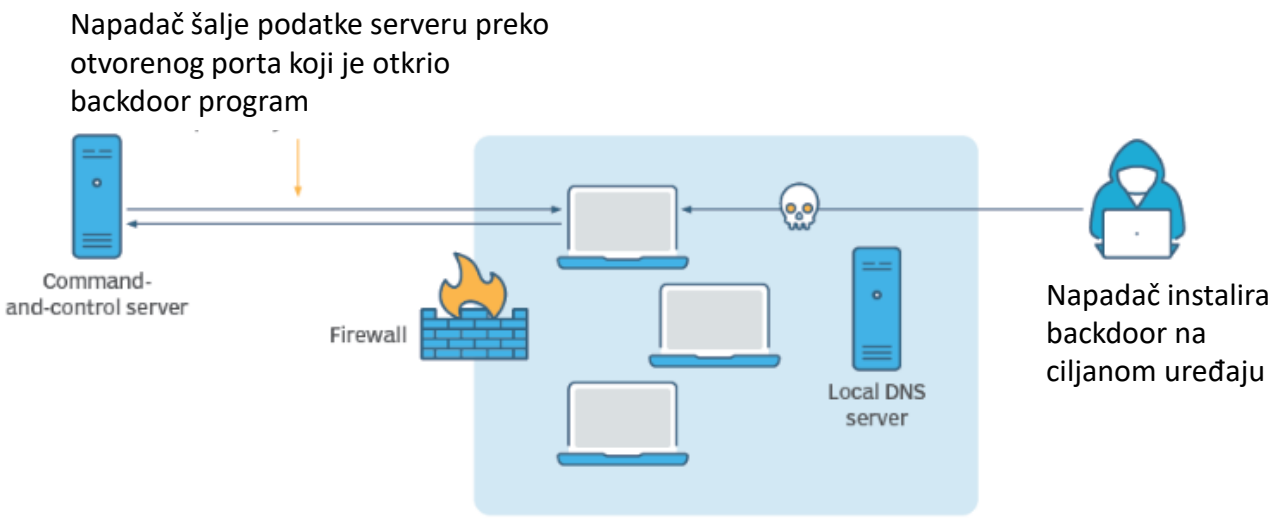
Programeri ponekad koriste backdoor tokom procesa razvoja i ne uklanjaju ih, ostavljajući ih kao potencijalnu tačku ranjivosti



BACKDOOR NAPAD

Zlonamerni softver takođe može da deluje kao backdoor.

U nekim slučajevima, malver je backdoor prve linije, kao platforma za postavljanje drugih modula zlonamernog softvera koji izvode napad.



BACKDOOR VEKTORI NAPADA

Za instaliranje backdoor-a koriste se različiti vektori napada:

Hardver. Napadači koriste modifikovane čipove, procesore, čvrste diskove i USB-ove da bi napravili backdoor.

IoT uređaji. Komponente ovih sistema, kao što su sigurnosne kamere, dronovi i pametni termostati, mogu delovati kao backdoor i pretvoriti se u bezbednosne propuste. IoT uređaji često dolaze opremljeni podrazumevanim lozinkama koje funkcionišu kao backdoor. Administratori ih često ne menjaju, a hakeri ih lako mogu pogoditi.

Pecanje. Naizgled legitimne e-poruke se koriste da prevare korisnike da hakerima daju osetljive informacije i mogu se koristiti za instaliranje zlonamernog softvera u pozadini.

Steganografija. Malver je sakriven unutar slike. Napadač ugrađuje kod unutar piksela slike. Kada se slika otvori u ranjivoj aplikaciji ili sistemu, zlonamerni kod može biti izvršen.

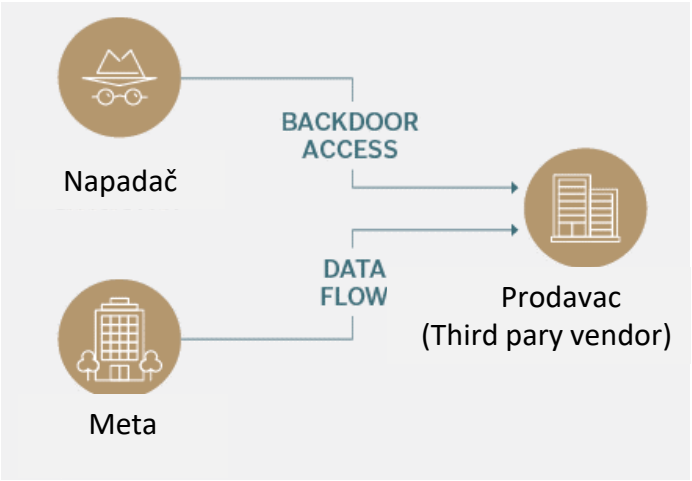
Različiti tipovi malvera se koriste u backdoor napadima:

Ransomvare je malver koji sprečava korisnike da pristupe sistemu i datotekama koje on sadrži. Napadači obično zahtevaju plaćanje otkupa za resurse koji će biti otključani.

Špijunski softver je zlonamerni softver koji krade osetljive informacije i prenosi ih drugim korisnicima bez znanja vlasnika informacija. Može da ukrade brojeve kreditnih kartica, podatke za prijavu na nalog i informacije o lokaciji.

Keyloggeri su oblik špijunskog softvera koji se koristi za snimanje korisničkih pritisaka na tastere i krađu lozinki i drugih osetljivih podataka.

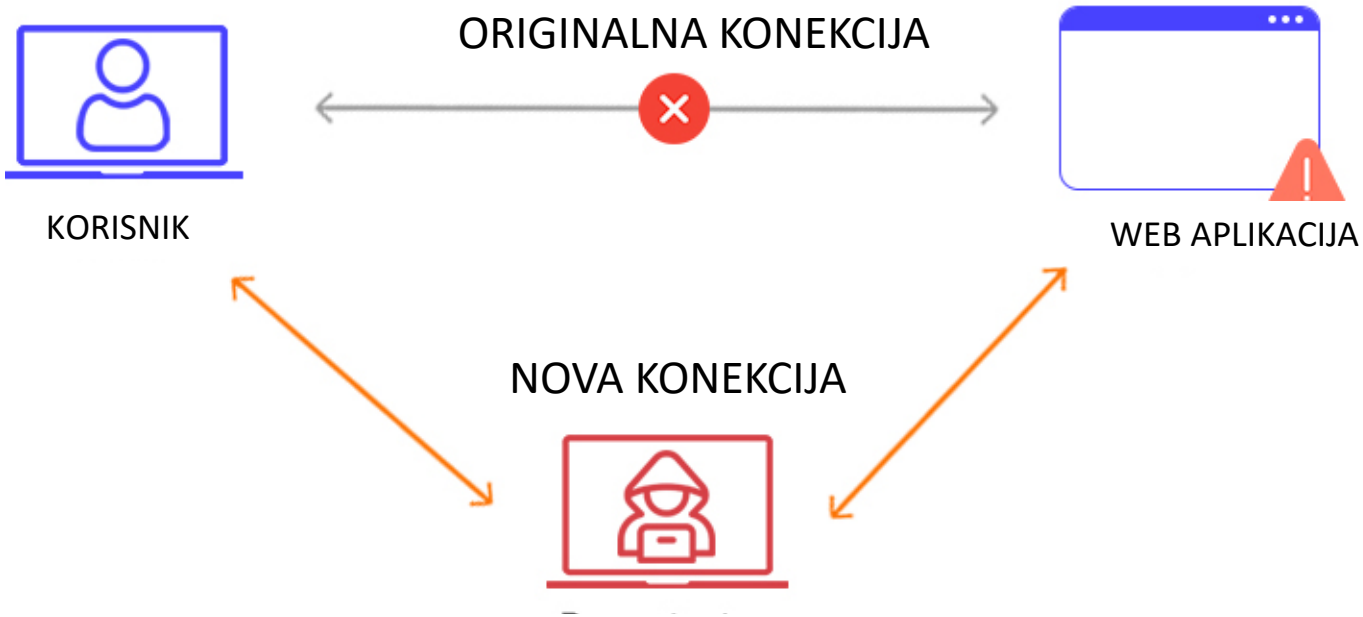
Trojanski konj je zlonamerni program koji se često instalira preko backdoor-a i izgleda bezopasan. Backdoor Trojanac uključuje backdoor koji omogućava daljinsku administrativnu kontrolu ciljanog sistema.



MAN IN THE MIDDLE (MITM) NAPAD

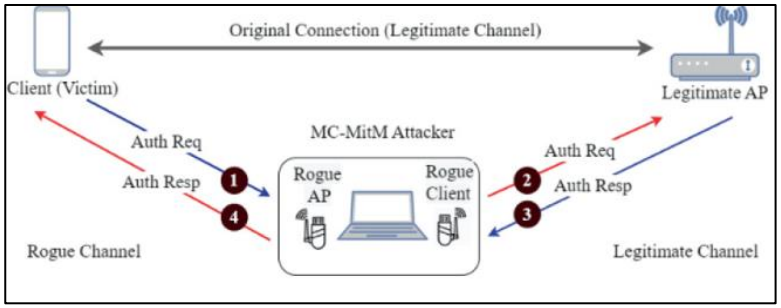
Napad tipa man-in-the-middle je prilično složen u tehničkom smislu.

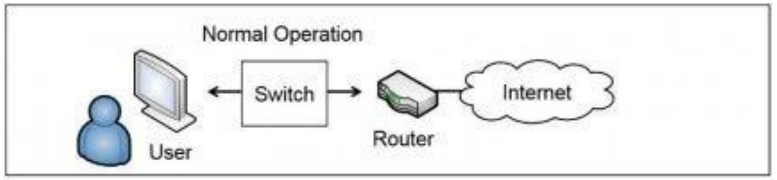
Pripada grupi pristupnih napada, mada se može posmatrati kao početni korak u napadu s ciljem izmene podatka.

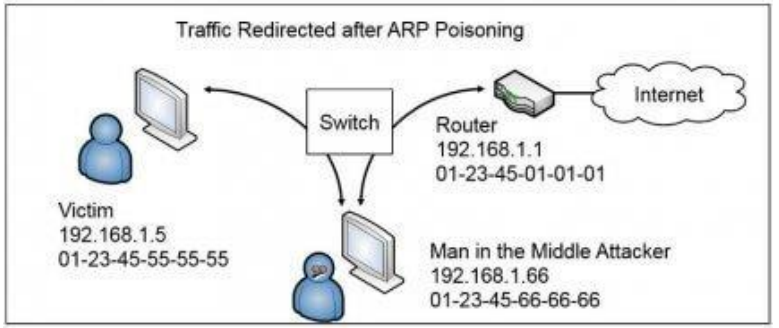


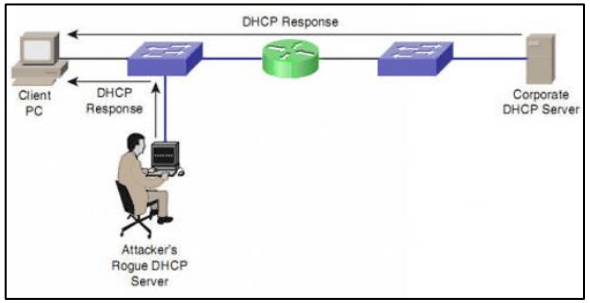
MAN IN THE MIDDLE (MITM) NAPAD

- Između servera i klijenta se postavlja odgovarajući softver tako da administrator i korisnici ne budu svesni njegovog prisustva.
- Ubačen softver beleži presretnute podatke radi kasnijeg pregleda, menja podatke ili na bilo koji drugi način ugrožava sigurnost korisničkih sistema i sesije a zatim ih šalje na server, kao da se ništa nije desilo.
- Server reaguje normalno na tako dobijene podatke, uveren da se komunikacija odvija s legitimnim klijentom.
- Softver ``napadač`` i dalje nastavlja slanje podataka na server i kompletan proces se produžava









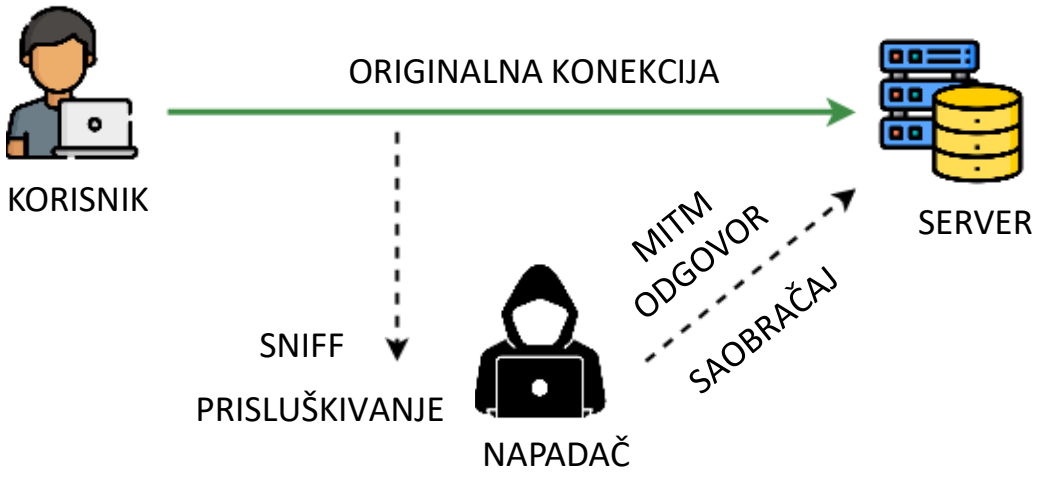
REPLAY NAPAD

Izvode se zadržavanjem podataka koji se razmenjuju na mreži, u cilju osiguranja pristupa mreži (pristupni napad) ili izmenu podataka

U distribuiranom okruženju između klijenata i sistema za identifikaciju se stalno šalju podaci o imenu i lozinci korisnika.

Napadač može zadržati takve podatke i naknadno ih ponovo poslati.

Isto važi i za sigurnosne certifikate u sistemima poput Kerberos-a.



METODE EKSPLOTACIJE SLABOSTI

Odbijanje usluga (*Denial of Service, DoS*).

DoS izaziva prestanak rada servisa ili programa, čime se drugima onemogućava rad s tim servisima ili programima. DoS napad se najlakše izvršava na transportnom sloju, slanjem velikog broja SYN paketa (TCP CONNECTION REQUEST), zaštita se postiže kontrolisanjem broja SYN paketa u jedinici vremena.

Lažiranje IP adresa (*spoofing*).

Napadač prati IP adrese u IP paketima i predstavlja se kao drugi računar. Kako DNS ne proverava odakle dolaze informacije, napadač može da izvrši napad lažiranjem tako što DNS servisu daje pogrešnu informaciju.

Njuškanje (*sniffing*).

Napadač specijalnim programima presreće TCP/IP pakete koji prolaze kroz određeni računar i po potrebi pregleda njihov sadržaj. Kako kroz mrežu obično kreću nešifrovani podaci, program za njuškanje (***snifer***) lako može doći do poverljivih informacija.

ZLONAMERNI PROGRAMI

Zlonamerni programi se klasifikuju:

1) Na osnovu prisutnog nosioca

- Zavisni program

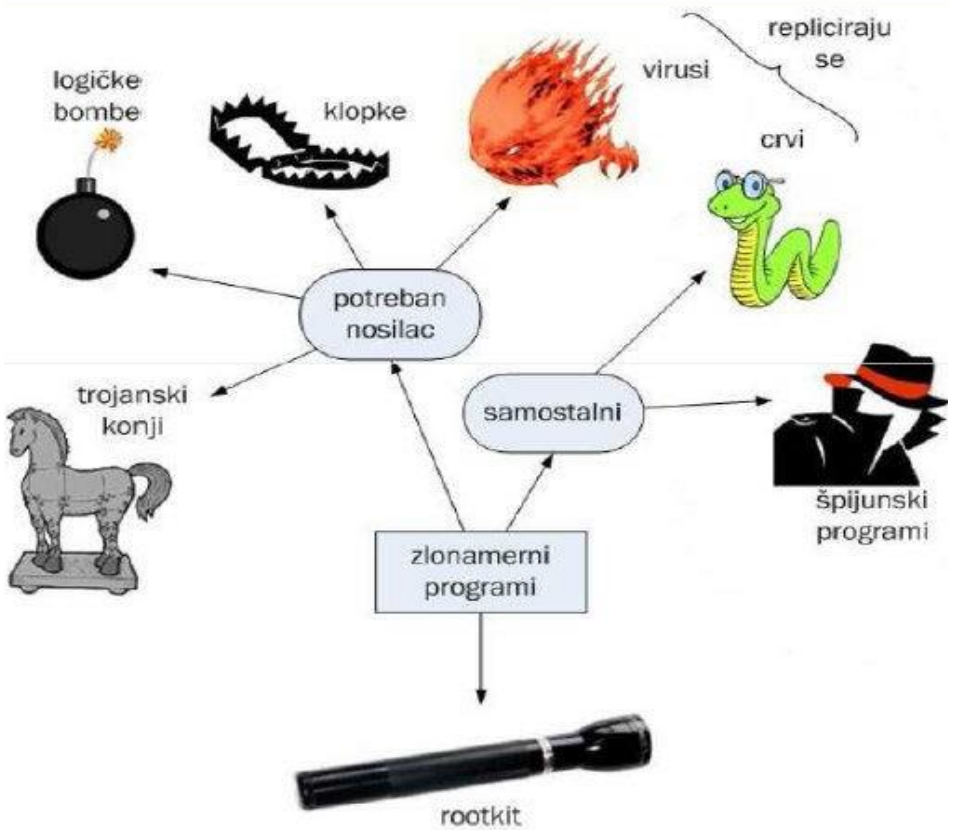
(nephodan nosilac odnosno program u kome će biti sakriveni npr. trojanski konji i virusi)

- Nezavisni (samostalni)

kojima nije neophodan nosilac npr. crvi i špijunski programi

2) Na osnovu umnožavanja

- **Replikatori** (virusi, crvi)
- **Nereplikatori** (trojanski konji, logičke bombe, rootkit ...)



PROGRAMSKE PRETNJE
TROJANSKI KONJ

Ilegalan segment koda, podmetnut u kod nekog legitimnog programa.

Trojanac koji otvara zadnja vrata

Program koji omogućava udaljenom korisniku da pristupi inficiranom računaru

Kradljivci informacija

PSW trojanac pokušaće da pretraži računar kako bi došao do poverljivih informacija kao što su lozinke, privatni i javni ključevi, sertifikati i podaci sa kreditnih kartica.

Trojanski špijuni (*trojan spy*) i ***obaveštajci*** (*keylogging*)

Snima ekrane ili na neki drugi način omogućava napadaču da prati rad korisnika.

Nosioci softvera su obično realizovani u vidu trojanskih konja koji se nakon instalacije ponašaju kao magnet za drugi zlonameran softver.

Trojanski proksi server*(trojan proxy)*

Pokušaće da pretvori inficirani računar u proksi server, čime se udaljenim korisnicima dozvoljava da preko inficiranog računara anonimno pristupe Internetu (DoS napad).

TROJANSKI KONJ

Metode infekcije:

e-maila

preuzimanjem zaraženih datoteka s interneta

zlonamernih reklama, igrica i aplikacija koje su navodno korisne

Namena:

krađa ličnih podataka

uništavanje podataka na računaru

udaljeni pristup računaru

pokretanje napadačkih bot mreža

Trojanci mogu biti deo većih napada poput ransomware-a (koji šifrira podatke i traži otkupninu za njihovo dešifrovanje) ili bankarskih trojanaca (koji ciljaju bankovne podatke korisnika).

Maskiranje:

Trojanci obično dolaze maskirani kao legitimni softver ili datoteke.

Mogu se sakriti u prividno bezopasne datoteke poput slika, dokumenata ili izvršnih programa.

TROJANSKI KONJ

Prevencija:

Prevencija protiv trojanaca uključuje pažljivo pregledavanje e-pošte i preuzimanje datoteka s nepouzdanih izvora

Redovno ažuriranje antivirusnih programa

Upotreba firewall-a

Uklanjanje:

Antivirusni softver za skeniranje računara i uklanjanje zlonamjernog softvera.

Promena lozinke za sve važne naloge

TROJANSKI KONJ - PRIMERI

Zeus Trojan:

Zeus je jedan od najpoznatijih bankarskih trojanaca koji je ciljao bankovne račune širom sveta.

Kreiran je da bi krao finansijske podatke korisnika, kao što su korisnička imena, lozinke i druge osetljive informacije.

CryptoLocker:

Ransomware trojanac koji je ciljao Windows korisnike.

Nakon infekcije, šifrirao bi datoteke na računaru i tražio otkupninu u bitkoinima kako bi dešifrovao podatke.

Emotet:

Emotet je trojanac koji se obično distribuira putem zlonamernih e-mailova.

Nakon što inficira računar,

Emotet se može koristiti za krađu informacija, širenje drugih zlonamjernih programa ili stvaranje bot mreže za izvršavanje napada na druge sisteme.

PROGRAMSKE PRETNJE

1. **Klopka** (*trap door*)

   Autor programa može slučajno ili namerno ostaviti prazna mesta u svom kodu (klopku) pa potencijalni uljez koji zna za ta mesta može da podmetne svoj kod

2. **Prekoračenje tj. prelivanje bafera** (*buffer overrun, bufer overflow*) na steku ili u dinamičkom delu memorije

   Prekoračenje bafera je najčešći napad sa mreže pri pokušaju neovlašćenog pristupanja sistemu.

   Ovlašćeni korisnici mogu da odaberu ovu vrstu napada kako bi prevarili sistem i ostvarili veća prava od onih koja imaju.

   Napadač koristi grešku u programu, to jest, neodgovarajuću kontrolu razdvajanja steka, podataka i koda.