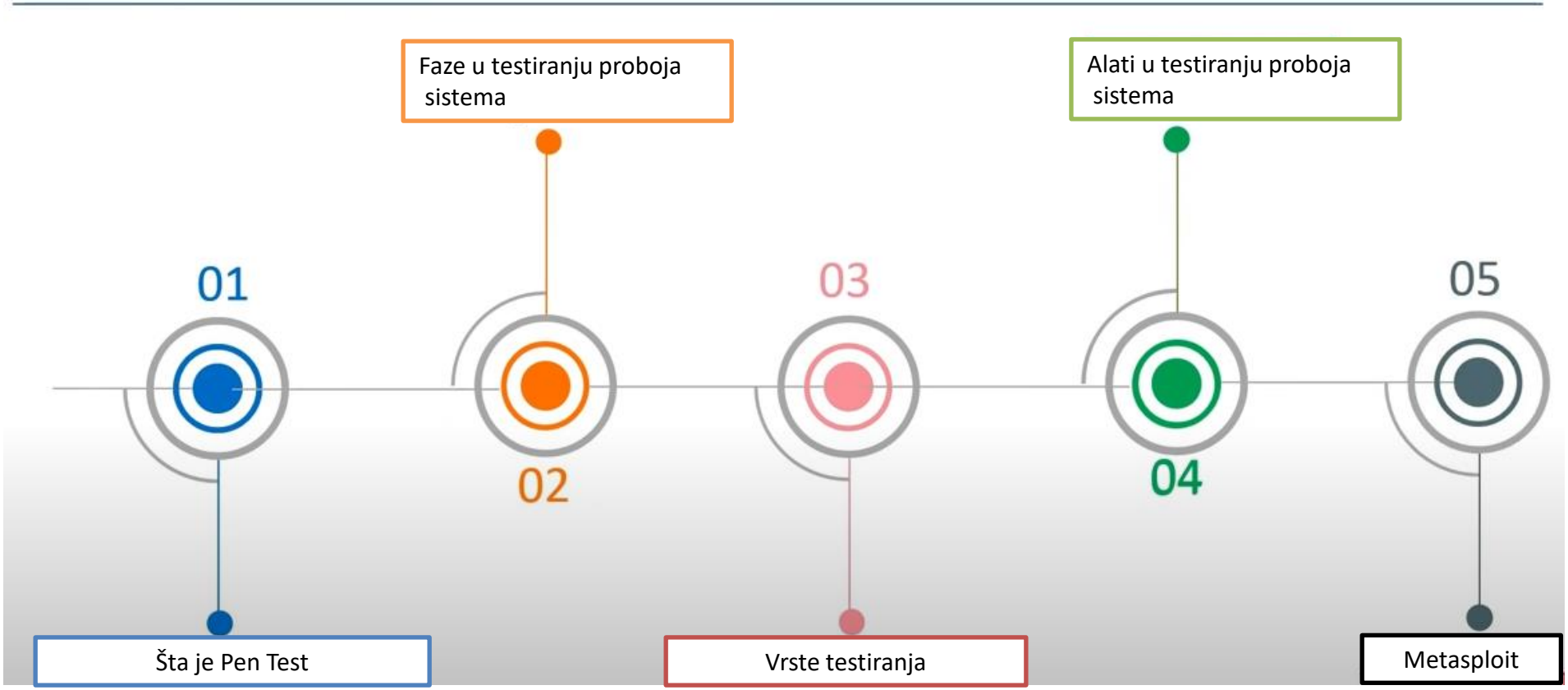
Bezbednost Aplikacija
Pen Test

Predmet: Bezbednost Aplikacija

Predavač: dr Dušan Stefanović

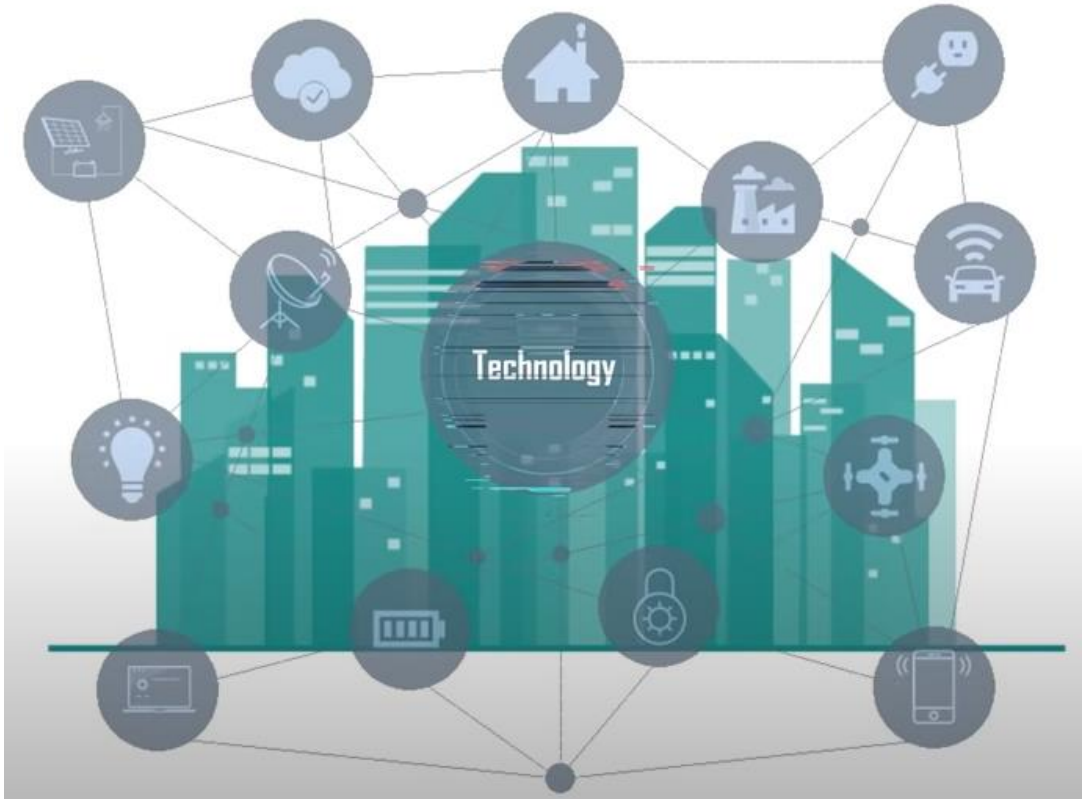
Pen Testing

- Pen test je simulirani cyber security napad radi provere i procene bezbednosti IT sistema
- Proaktivni načini testiranja web aplikacija izvršavanjem napada koji su slični stvarnim napadima



Ranjivost sistema

- Dizajn sistema
- Loša konfiguracija sistema
- Nebezbedna mreža
- Složenost sistema (sistem se oslanja na raznovrsne tehnologije)
- Ljudske greške (deljenje lozinke)



Termini koji se koriste u testiranju

Etičko hakovanje

Etički haker je profesionalac koji radi na identifikaciji nedostataka (rupa) u informacionom sistemu obaveštavajući i pomažući vlasniku sistema da otkloni otkrivene ranjivosti.

Etički haker koristi identične alate i metodologiju kao i zlonamerni haker ali im je cilj drugačiji.

Penetraciono testiranje

Odnosi se na opis zadataka koje radi etički haker

Opisuje način za identifikaciju ranjivosti u sistemima i utvrđivanju da li se ranjivost može ili ne može eksploatisati

Reguliše se ugovorom između vlasnika sistema izvršioca i vlasnika sistema

Procena ranjivosti

Izveštaj u kojem se opisuju pronađene ranjivosti u sistemu sortirane prema stepenu rizika.

Ne uključuje eksploatisanje i dobijanje pristupa

Provera bezbednosti

Sistemska procedura za merenje stanja sistema u odnosu na unapred određeni skup standarda (industrijska najbolja praksa ili interna kontrolna lista)

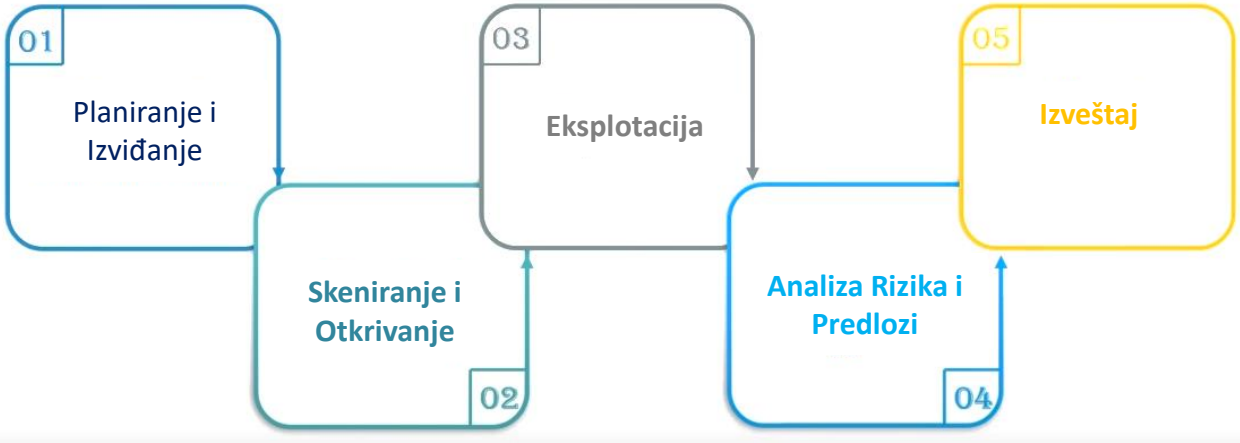
Cilj je izveštaj o usklađenosti

Šta je Pen Test

- Način da se otkriju slabosti sistema na serveru, mreži ili aplikaciji se može postići iterativnim postupkom koji je poznat kao **pen test**.
- Cilj pen test-a je da se otkriju ranjivosti u sistemu i da se pronađene ranjivosti iskoriste (exploit) da bi se odredio nivo neautorizovanog pristupa ili druga maliciozna aktivnost (dubina kompromitovanja mete)

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 Web aplikacije
  - 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