Provjera ranjivosti

Luka Pauk
CARNet CERT

CERT.hr

Sadržaj

- Što je provjera ranjivosti?
- Tipovi provjere ranjivosti
- Alati
- Postupak mrežne provjere ranjivosti
- Usluga CARNet CERT-a

CERT.hr

Što je provjera ranjivosti?

- *vulnerability scanning, vulnerability assessment*
- Automatizirani postupak
- Identificira poznate ranjivosti
- Izvodi se specijaliziranim alatima (skenerima)

Tipovi provjere ranjivosti

- Lokalna provjera ranjivosti
  - Ispituje sustav “iznutra”
  - Zahtijeva administratorski ili korisnički pristup sustavu
  - Može se obavljati i na udaljenom sustavu uporabom protokola za udaljenu administraciju

Tipovi provjere ranjivosti

- Mrežna provjera ranjivosti
  - “Izvana” ispituje sustav koji se nalazi unutar crne kutije
  - Provjere se obavljaju preko mrežnog sučelja
  - Ne zahtijeva administratorski ili korisnički pristup sustavu
  - Daje sigurnosnu sliku sustava iz perspektive vanjskog napadača

Alati

- Microsoft Baseline Security Analyzer
  - Lokalne provjere Windows sustava
  - Mogućnost prijave na udaljeni sustav
  - Zahtijeva administratorske ovlasti na ispitivanom sustavu
  - Besplatan

Alati

- Nessus
  - Najpopularniji alat za provjeru ranjivosti
  - Podržava mrežne i lokalne provjere različitih sustava
  - *Plug-in* tehnologija
  - NASL – jezik za pisanje *plug-inova*
  - Klijent/poslužitelj arhitektura

Postupak mrežne provjere ranjivosti

1) Prikupljanje informacija
2) Identificiranje računala
3) Skeniranje portova
4) Odabir provjera
5) Analiza rezultata

Prikupljanje informacija

- IP adresa ili skup adresa
- Vrsta sustava (produkcijski, testni)
- Vrijeme skeniranja
- Dozvola vlasnika sustava

Identificiranje računala

- Popisivanje aktivnih IP adresa kod “slijepog” skeniranja
- Metode:
  - ICMP ping
    - Koristan kad je skener unutar iste podmreže
  - TCP ping
    - Koristan kad je skener u drugoj podmreži, a ICMP je blokiran na vatrozidu

Skeniranje portova

- Popisivanje aktivnih portova
- Parametri:
  - točnost
  - brzina
  - diskrecija
- Najčešće metode
  - `connect()` skeniranje
  - `SYN` skeniranje

Odabir provjera

- Provjere se dijele:
  - prema vrsti sustava za kojeg su namijenjene
  - po riziku koji predstavljaju za testirani sustav
- Ovisno o informacijama iz prve faze:
  - uključiti/isključiti pojedine provjere
  - postaviti dodatne parametre za pojedine testove

Analiza izvještaja

- Identificiranje lažno pozitivnih rezultata. Najčešći uzroci:
  - provjere verzija programa
  - neočekivani, ali valjani rezultati
- Procjena rizika
- Pronalaženje rješenja

CERT.hr

Usluga CARNet CERT-a

- Usluga namijenjena ustanovama članicama CARNeta
- Alati: Nessus i Shadow Security Scanner
- Izvještaji na hrvatskom jeziku
- Bez naknade
- Više informacija na http://www.cert.hr/

CERT.hr

Ciljevi usluge provjere ranjvosti

- Pravovremeno otkrivanje poznatih sigurnosnih propusta
- Sprječavanje sigurnosnih incidenata
- Otkrivanje kompromitiranih sustava
- Pomoć sistem administratorima
- Edukacija

CERT.hr

Motivi za uvođenje usluge provjere ranjivosti

- Velik broj klijentskih i poslužiteljskih računala
- Izravna i brza veza na Internet
- Povećani broj malicioznih programa i neovlaštenih aktivnosti
- Nedostatak sigurnosnih kontrola i mehanizama
- Nedostatnost stručnog kadra

CERT.hr

Što provjera ranjivosti nije

- Kontrola sistem administratora i koordinatora
- Provaljivanje u Vaše informacijske sustave
- Pokušaj dohvata Vaših povjerljivih podataka

Kraj!

Zahvaljujem na pažnji!

CARNet CERT
http://www.cert.hr
ccert@cert.hr