

Lucrare individuală: Testarea securității unei infrastructuri de rețea

1. Scopul lucrării

Scopul lucrării este identificarea, exploatarea controlată și documentarea vulnerabilităților existente într-o infrastructură de laborator alcătuită dintr-un router MikroTik CHR și sistemele aflate în spatele acestuia.

Instrumente sau SO pentru utilizare la alegerea dumneavoastră: Kali Linux, Nmap, Hydra, Medusa etc.

2. Mediul de testare

Ținta principală a testării este:

- Tip echipament: MikroTik CHR;
- Adresă IP publică: 139.162.175.176;
- Infrastructură internă care se află în spatele CHR

3. Sarcini

Etapa 1 – Recunoașterea infrastructurii

Realizați o analiză inițială a țintei pentru a identifica:

- disponibilitatea sistemului;
- porturile deschise;
- serviciile de rețea disponibile;
- protocoalele utilizate;
- versiunile serviciilor, dacă acestea pot fi determinate;
- posibilele puncte de acces în infrastructură.

Analizați și explicați rezultatele scanării, prezentând totodată dovada realizării acestei recunoașteri a infrastructurii.

Etapa 2 – Obținerea accesului la MikroTik CHR

Identificați conturile și parolele vulnerabile existente pe MikroTik CHR, utilizând tehnici controlate de testare a autentificării, inclusiv atacuri de tip dicționar sau brute-force.

După identificarea unor credențiale valide:

- autentificați-vă pe MikroTik CHR;
- confirmați accesul obținut în raport;
- determinați drepturile contului compromis;
- analizați configurația disponibilă aceluia cont, cât și configurația CHR;
- identificați informații despre infrastructura aflată în spatele CHR;

- documentați modul în care accesul obținut poate afecta securitatea rețelei.

Etapa 3 – Analiza infrastructurii interne

Pe baza informațiilor identificate în configurația CHR, verificați sistemele aflate în spatele acestuia. Identificați alte vulnerabilități prezente în infrastructură.

4. Cerințele raportului

În raport pentru fiecare vulnerabilitate identificată prezentați:

1. Denumirea vulnerabilității.
2. Sistemul sau serviciul afectat.
3. Cauza existenței vulnerabilității.
4. Instrumentele utilizate pentru exploatarea vulnerabilităților.
5. Metoda de identificare.
6. Etapele exploatării.
7. Dovezi ale exploatării reușite.
8. Nivelul de acces obținut.
9. Impactul posibil asupra infrastructurii.
10. Măsurile recomandate pentru remediere și protecție.

Includeți:

- capturi de ecran;
- rezultate relevante ale comenzilor;
- porturile și serviciile identificate;
- confirmarea autentificării;
- informații neconfidențiale din configurație;
- identificarea utilizatorului curent și a drepturilor acestuia.

5. Măsuri de protecție propuse

Pentru fiecare vulnerabilitate exploatată prezentați măsuri de protecție. Recomandările trebuie adaptate vulnerabilităților identificate și configurației analizate.

6. Concluzii

Formulați concluzii asupra lucrării individuale.