Predmet: Bezpečnosť informačných technológii

Autor: Michal Greguš

Návrh zadania

16 – Looking for vulnerabilities in large networks

Cieľom zadania je napísať vlastný nse skript, ktorý bude schopný detegovať relatívne novú zraniteľnosť detekovateľnú po sieti pre nástroj na bezpečnostné auditovanie sietí nmap. A následne overiť funkčnosť tohto skriptu na prototype SW disponujúceho vybranou zraniteľnosťou.

Analytická časť:

1. Opis nástroja nmap a možností rozšírenia jeho funkcionality prostredníctvom vlastného nse(nmap scripting engine) skriptu
2. Rozdelenie a popis *nse* skriptov, bližšie sa budeme venovať skriptom z kategórie *vuln*
3. Výber nejakej nedávno publikovanej zraniteľnosti detekovateľnej zo siete z portálu *nvd*
4. Popísanie vybranej zraniteľnosti a možností jej detegovania, prípadne jej odstránenia-nápravy
5. Popísanie fungovania a spôsobu inštalácie SW disponujúceho danou zraniteľnosťou
6. Spustenie skriptu na protopyp aplikácie pred odstránením zraniteľnosti a po jej odstránení

Očakávané výstupy:

1. Funkčná aplikácia s vybranou zraniteľnosťou, ktorá bude rozbehaná vo virtuálnom prostredí
2. Vlastný nse skript pre nástroj nmap schopný detegovať vybranú zraniteľnosť
3. Zdokumentovaný postup rozbehania aplikácie s vybranou zraniteľnosťou, možností jej detekcie prostredníctvom vlastného nse skriptu, opis možností následného odstránenia tejto zraniteľnosti a overenie jej odstránenia prostredníctvom opätovného spustenia nse skriptu slúžiaceho na jej detekciu