Սերվերային համակարգերի անվտանգությունը գնահատող ծրագրի մշակում

Վարդանյան Բաբկեն

Գիտական ղեկավար՝ ֆիզ.-մաթ. գիտ. դոկտոր, պրոֆեսոր Մարիամ Հարությունյան

Մագիստրոսական Թեզ

ՀՀ ԳԱԱ Գիտակրթական Միջազգային Կենտրոն
Ինֆորմատիկայի և Հաշվողական Տեխնիկայի Ամբիոն

Երևան 2016

Ներածություն

Տեղեկատվական անվտանգություն

Տեղեկատվական ռեսուրսների չլիազորված օգտագործման

- կանխման,
- հայտնաբերման

պրոցեսն է:

Կարևորագույն արդի խնդիրներից է:

Հակառակորդի նպատակները

- դրամական եկամուտ,
- բիզնեսի խոչնդոտում,
- ինֆորմացիայի գողություն,
- DDoS, հենակետ հետագա գրոհների համար,
- SEO,
- զվարճանք:

Անվտանգության պրակտիկան

1. սերվիսներ,
2. հեռակառավարում,
3. օգտագործողներ և արտոնություններ,
4. թարմացումներ,
5. գրանցամատյանների դիտարկում (logs),
6. չօգտագործվող մոդուլներ,
7. տեղեկացվածություն,
8. սկզբնական կոդ,
9. ալգորիթմներ,
10. հակավիրուս,
11. ցանցային սկաներներ:

Ցանցային սկաներներ

Հայտնաբերում են՝

- բաց պորտեր,
- սերվիսներ,
- խոցելիություններ,
- վիրուսներ:

Հայտնի ցանցային սկաներներից են՝

- nmap,
- nessus,
- acunetix:

Ցանցային սկաներների աշխատանքը

1. հասցեների և պորտեի շրջանակի որոշում,
2. սկանավորման պարամետրերի մուտքագրում,
3. նշված հասցեների և պորտերի փորձարկում,
4. բաց պորտի առկայության դեպքում սերվիսի մասին տվյալների ստացում,
5. սկանավորման արդյունքների արտածում:

Խնդրի դրվածքը

Ցանցային սկաներների թերությունները

- ժամանակ,
- ցանցային ռեսուրսների վատնում, աշխատանքի խոչնդոտում,
- IDS ահազանգներ,
- ոչ վստահելի արդյունքներ,
- չեն ստուգում՝
  - օգտագործողներ և արտոնություններ,
  - թարմացումներ,
  - ալգորիթմներ,
  - հակավիրուս:

Այլընտրանք

Ներկայացված այլընտրանքը ծրագիր է, որը համակարգերը սկանավորում է ներսից:

Հնարավոր է ստուգումների առավել լայն շրջանակ՝

- թարմացումների առկայության ստուգում (APT, YUM, Pacman),
- ֆայլերի և դիրեկտորիաների թույլտվություններ,
- բաց պորտեր,
- root օգտագործող,
- umask,
- SSHd:

Նախկին փորձ

- MBSA,
- Buck-Security,
- Lynis,
- MaxPatrol,
- Tiger:

Այլընտրանքի իրականացումը

- իրականացված է Python լեզվով,
- սկզբնական կոդը հասանելի է https://github.com/axper/lmap հասցեով:

Եզրակացություն

Իրականացված աշխատանքի առավելությունները ցանցային սկաներների նկատմամբ՝

- արագագործություն,
- հուսալիություն,
- միանշանակ արդյունքներ,
- հնարավոր առավել բազմազան ստուգումներ:

Անհրաժեշտ է՝

- հետագա երկարատև մշակում և կատարելագործում,
- հասանելիություն ներսից,
- վստահություն ադմինիստրատորների կողմից:

Շնորհակալություն