Սերվերային համակարգերի անվտանգությունը գնահատող ծրագրի մշակում

Վարդանյան Բաբկեն

ՀՀ ԳԱԱ Գիտակրթական Միջազգային Կենտրոն
Ինֆորմատիկայի և Հաշվողական Տեխնիկայի Ամբիոն

Երևան 2016

Ներածություն

Տեղեկատվական անվտանգություն

Տեղեկատվական ռեսուրսների չլիազորված օգտագործման

- կանխում
- հայտնաբերում

Կարևորագույն արդի խնդրիներից 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 պոտեր
- 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

Նախկին փորձ

- MBSA
- Buck-Security
- Lynis
- MaxPatrol
- Tiger

Այլընտրանք

Ներկայացված այլընտրանքը՝

- Իրականացված է Python լեզվով
- Սկզբնական կոդը հասանելի է՝ `https://github.com/axper/lmap`
- Համակարգերը սկանավորում է ներսից
- Ստուգումների առավել լայն շրջանակ
  - Թարմացումների առկայության ստուգում (APT, YUM, Pacman)
  - Ֆայլերի և դիրեկտորիաների թույլտվություններ
  - Բաց պորտեր
  - Root օգագործող
  - Umask
  - SSHd

Եզրակացություն

Առավելություններ՝

- Արագագործություն
- Հուսալիություն
- Միանշանակ արդյունքներ
- Հնարավոր բազմազան ստուգումներ

Թերություններ՝

- Անհրաժեշտ է հետագա երկարատև մշակում
- Անհրաժեշտ է հասանելիություն ներսից
- Անհրաժեշտ է վստահություն ադմինիստրատորների կողմից

Շնորհակալություն