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 խոչընդոտում,
- 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 պորտրեի 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 խոչընդոտում,
- 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:

Նախկին փորձ

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

Թարմացումների առկայության ստուգում

- APT - Debian, Ubuntu

  `/var/lib/apt/periodic/update-success-stamp`

- Pacman - Arch Linux

  `/var/log/pacman.log`

Ֆայլեր և դիրեկտորիաներ

- world writable ֆայլեր որոնք սկսվում են կետով,
- world writable դիրեկտորիաներ որոնք չունեն sticky bit,
- world writable ֆայլեր որոնք պատկանում են համակարգային օգտագործողին:

Բաց պորտեր

- օգտագործվել է psutil գրադարանը,
- ցույց է տալիս բոլոր բաց TCP և UDP պորտերը:

Համակարգային օգտագործող

- համակարգային օգտագործողով մուտք գործելը համարվում է ոչ անվտանգ,
- ստուգում է `SUDO_UID` միջավայրային փոփոխականի առկայությունը:

Umask

- ստուգում է `S_IWOTH` (write by others) բիթի առկայությունը:

SSHd

- SSHd սերվիսի կոնֆիգուրացիոն ֆայլն է `/etc/ssh/sshd_config`,
- ստուգում է Protocol տողում 1 թվի բացակայությունը:

Այլընտրանքի իրականացումը

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

```
[root@ws14 lmap]# ./lmap.py
--------------------------------------------------------------------------------
Running: OpenPorts
Status: ScanStatus.success
Message: Type, IP, Port, PID, Username, Command line
tcp 127.0.0.1:631 515 root /usr/bin/cupsd -l
udp 0.0.0.0:631 545 root /usr/bin/cups-browsed
tcp ::1:631 515 root /usr/bin/cupsd -l
udp 0.0.0.0:45614 520 avahi avahi-daemon: running [ws14.local]
udp 0.0.0.0:5353 520 avahi avahi-daemon: running [ws14.local]
udp :::5353 520 avahi avahi-daemon: running [ws14.local]
udp :::37168 520 avahi avahi-daemon: running [ws14.local]
udp 0.0.0.0:68 555 root /usr/bin/dhcpcd -q -b


--------------------------------------------------------------------------------
Running: Root
Status: ScanStatus.fail
Message: Do not use the root user account

--------------------------------------------------------------------------------
Running: Ssh
Status: ScanStatus.fail
Message: The vulnerable SSHv1 is enabled in /etc/ssh/sshd_config

--------------------------------------------------------------------------------
Running: Umask
Status: ScanStatus.fail
Message: Current user's umask gives write permissions OTHERS group by default

--------------------------------------------------------------------------------
Running: Update
Status: ScanStatus.fail
Message: System last update date is too old - 2016-05-12 14:41:00

[root@ws14 lmap]#
```

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