

ՀՀ ԿՐԹՈՒԹՅԱՆ ԵՎ ԳԻՏՈՒԹՅԱՆ  
ՆԱԽԱՐԱՐՈՒԹՅՈՒՆ  
ՀՀ ԳԱԱ ԳԻՏԱԿՐԹԱԿԱՆ ՄԻՋԱԶԳԱՅԻՆ  
ԿԵՆՏՐՈՆ  
ՄԱԳԻՍՏՐՈՍԱԿԱՆ ԹԵԶ  
Բաբկեն Վարդանյան Սամվելի

Մասնագիտություն՝	Ինֆորմատիկա և հաշվողական տեխնիկա
Թեմա՝	Սերվերային համակարգերի անվտանգությունը գնահատող ծրագրի մշակում
Գիտական ղեկավար՝	Ֆիզ.-մաթ. գիտ. դոկտոր, պրոֆեսոր Մարիամ Հարությունյան

Թույլատրել պաշտպանության '\_\_\_\_' '\_\_\_\_\_' 2016 թ.

Ամբիոնի վարիչ՝	Ֆիզ.-մաթ. գիտ. թեկնածու, դոցենտ Վլադիմիր Սահակյան
----------------	---

Կցանկանայի խորին երախտագիտությունս հայտնել իմ ղեկավար, ֆիզ.-մաթ. գիտ. դոկտոր, պրոֆեսոր Մարիամ Հարությունյանին (ԻԱՊԻ), ով ինձ աջակցել և խրախուսել է այս աշխատանքի ժամանակ:

Բաբկեն Վարդանյան

# Բովանդակություն

<b>1 Առաջաբան</b>	<b>5</b>
1.1 Ինչ է տեղեկատվական անվտանգությունը . . . . .	5
1.2 Ինչու՞ հոգալ տեղեկատվական անվտանգության մասին . . . . .	5
1.3 Ինչու՞ ինչ-որ մեկը կցանկանա կոտրել որոշակի համակարգ . . . . .	5
1.4 Սերվերային անվտանգության ժամանակակից պրակտիկան . . . . .	6
<b>2 Խնդրի դրվածքը</b>	<b>11</b>
2.1 Խնդրի արդիականությունը . . . . .	11
2.2 Այլընտրանք . . . . .	11
2.3 Նախկին փորձի ուսումնասիրություն . . . . .	12
2.3.1 Microsoft Baseline Security Analyzer . . . . .	12
2.3.2 Buck-Security . . . . .	12
2.3.3 Lynis . . . . .	12
2.3.4 MaxPatrol . . . . .	13
2.3.5 Tiger . . . . .	13
<b>3 Ծրագրին ներկայացվող պահանջներ</b>	<b>14</b>
3.1 Ծրագրային թարմացումներ . . . . .	14
3.1.1 Debian/APT-ի վրա հիմնված համակարգեր . . . . .	14
3.1.2 Red Hat/YUM-ի վրա հիմնված համակարգեր . . . . .	14
3.1.3 Arch Linux/Pacman-ի վրա հիմնված համակարգեր . . . . .	15
3.2 Ֆայլերի և դիրեկտորիաների թույլտվություններ . . . . .	16
3.3 Բաց TCP և UDP պորտեր . . . . .	16
3.4 Մուտք որպես համակարգային օգտագործող (root user) . . . . .	16
3.5 Օգտագործողների Umask ստուգում . . . . .	17
3.6 SSHd սերվիսի կոնֆիգուրացիայի ստուգում . . . . .	17
<b>4 Իրականացում</b>	<b>18</b>
4.1 Ծրագրավորման լեզվի ընտրություն . . . . .	18
4.2 Ծրագրային պահանջներ . . . . .	18
4.3 Մոդուլների իրականացումը . . . . .	18
4.3.1 Հիմնական մոդուլը՝ lmap.py . . . . .	18
4.3.2 Ծրագրային թարմացումներ՝ update.py . . . . .	18
4.3.3 Ֆայլերի և դիրեկտորիաների թույլտվություններ՝ worldwritable.py . . . . .	19
4.3.4 Բաց TCP և UDP պորտեր՝ openports.py . . . . .	20
4.3.5 Մուտք որպես համակարգային օգտագործող՝ root.py . . . . .	20
4.3.6 Օգտագործողների Umask ստուգում՝ umask.py . . . . .	20
4.3.7 SSHd սերվիսի կոնֆիգուրացիայի ստուգում . . . . .	21

<b>5 Եզրակացություն</b>	<b>22</b>
<b>Գրականության ցանկ</b>	<b>23</b>

# 1 Առաջաբան

## 1.1 Ինչ է տեղեկատվական անվտանգությունը

Տեղեկատվական անվտանգությունը տեղեկատվական ռեսուրսների չլիազորված օգտագործման կանխման և հայտնաբերման պրոցեսն է [1]:

Տեղեկատվական ռեսուրսների չլիազորված օգտագործման կանխումը չարամիտ չլիազորված անձանց (նաև ասում են «հակառակորդներ», «հարձակվողներ», «ներխուժողներ», «հաքերներ») կողմից ծրագրային ապահովման կամ տվյալների որոշ մասի օգտագործման դեմ ուղղված միջոցառումների համակարգն է:

Տեղեկատվական ռեսուրսների չլիազորված օգտագործման հայտնաբերումը չլիազորված մուտքի փորձի առկայության ստուգման պրոցեսն է: Եթե նման փորձ առկա է, ապա նաև՝ արդոք այն հաջողվել է, և թե կոնկրետ ինչ է տեղի ունեցել [2]:

## 1.2 Ինչու՞ հոգալ տեղեկատվական անվտանգության մասին

Այսօր համակարգիչները և էլեկտրոնային տեխնիկան օգտագործվում են կյանքի գրեթե բոլոր ոլորտներում: Բանկային համակարգի ու ներդրումների ոլորտից մինչև գնումների և հեռահաղորդակցության ոլորտ համակարգիչները դարձել են յուրաքանչյուր բիզնեսի անբաժանելի մասը: Դժվար է նշել մի ոլորտ, որը օգուտ չի քաղել տեղեկատվական տեխնոլոգիաների բուռն զարգացումից:

Չնայած ընկերությունների կողմից պահվող ոչ բոլոր տվյալները կարելի է դասակարգել որպես «հույժ գաղտնի», ցանցային աղմինիստրատորները հավանաբար չեն ուզենա որ անձանոթ անձինք հնարավորություն ունենան հետևել իրենց ընկերության ներքին հաղորդակցությանը, իրենց անձնական ինֆորմացիային, կամ փոփոխություններ կատարեն իրենց վստահված համակարգերում:

Այդ պատճառով տեղեկատվական անվտանգությունը մնում է բիզնեսի և հասարակության առջև ծառացած ամենակարևոր չհաղթահարված խնդիրներից մեկը [3]:

Սերվերի ղեկավարման հնարավորությունը հակառակորդի կողմից ռիսկի տակ է դնում ոչ միայն ընկերությանը, այլ նաև ընկերության հաճախորդներին, ինչպես օրինակ օրինակ վեբ կայքի այցելուներին:

## 1.3 Ինչու՞ ինչ-որ մեկը կցանկանա կոտրել որոշակի համակարգ

Հակառակորդներին հաճախ չի հուզում, թե ով է օգտագործողը կամ ընկերությունը, որի վրա իրականացվում է հարձակումը:

Հակառակորդի հիմնական նպատակներն են [4]՝

- **Դրամական եկամուտ**

Կոտրված համակարգից կամ սերվերից օգտագործողի կամ ընկերության բանկային հաշվի և վարկային քարտի տեղեկությունները գողանալու միջոցով:

- **Բիզնեսի աշխատանքի խոչնդոտում**

Մի ընկերություն կարող է վարձել հակառակորդին իրենց մրցակցի համակարգչային ցանցում քառս ստեղծելու նպատակով:

- **Ինֆորմացիայի գողություն**

Մի ընկերություն կարող է վարձել հակառակորդին իրենց մրցակից ընկերության գաղտնիքները գողանալու և այդպիսով մրցակցային առավելություն ձեռք բերելու նպատակով:

- **DDoS (Distributed Denial of Service - Բաշխված Ծառայության Ընդհատման գրոհ) գրոհներ իրականացնելու նպատակով այլ սերվերների վրա**

DDoS գրոհի նպատակն է սերվիսը անհասանելի դարձնել՝ դրան տարբեր աղբյուրներից չափազանց շատ հարցումներ իրականացնելու միջոցով [5]:

Նման հարձակման դեպքում կոտրված սերվերների քանակը ուղիղ համեմատական է գրոհի հաջողությանը:

- **SEO (Search Engine Optimization - Որոնման համակարգերի օպտիմալացում)**

Կոտրված կայքը կարող է օգտագործվել այլ կայքերի SEO-ն բարձրացնելու նպատակով՝ կոտրված կայքում տեղադրելով հղումներ դեպի այդ կայքը:

- **Հենակետ հետագա գրոհների համար**

Կոտրված սերվերը կարող է օգտագործվել որպես հենակետ՝

- նույն ընկերության ցանցում հետագա ավելի լայնածավալ հարձակումների համար,
- ավելի շատ սերվերներին տիրանալը օգնում է հակառակորդին թաքցնել իր ինքնությունը (IP հասցեն)՝ այլ ընկերությունների դեմ հետագա հարձակումների ժամանակ:

- **Զվարճանք**

Հակառակորդը կարող է կոտրել սերվերը զուտ հետաքրքրության կամ զվարճանքի համար:

## **1.4 Սերվերային անվտանգության ժամանակակից պրակտիկան**

Սերվերների անվտանգությունը ապահովելու այսօր ընդունված ամենատարածված պրակտիկաներից են [3][6]՝

### **1. Անջատել կամ ջնջել ոչ անհրաժեշտ սերվիսները**

Օպերացիոն համակարգերի լռելյայն կոնֆիգուրացիան երբեմն ապահով չէ: Սովորաբար տեղադրված են բազմաթիվ չօտագործվող սերվիսներ, ինչպես օրինակ՝ պրինտ սերվերը, «Սամբա» ֆայլերի բաշխման համակարգը և այլն: Այս սերվիսները մեծացնում են հարձակման հարթությունը, բացելով ավելի շատ հնարավոր եղանակներ չարամիտ օգտագործողի համար՝ համակարգը չարաշահելու նպատակով:

Ադմինիստրատորները պետք է անջատեն կամ մեկուսացնեն բոլոր չօգտագործվող սերվիսները, օրինակ՝ firewall-ի օգնությամբ:

## 2. Հեռակառավարում

Չպաշտպանված, հանրային ցանցերով մուտքը սերվեր հնարավոր է դարձնում հա-կառակորդների կողմից տարաբնույթ հարձակումներ, ինչպիսին է մարդը մեջտե-ղում (man-in-the-middle) և տվյալների գողություն:

Ադմինիստրատորը պետք է համոզվի, որ բոլոր հեռակառավարման կապերը դեպի սերվեր պաշտպանված են գաղտնագրմամբ և գաղտնաբառով:

## 3. Թույլտվություններ և արտոնություններ

Թույլտվությունների հստակ կառավարման համակարգը կարևոր դեր է խաղում սերվերային անվտանգության մեջ: Եթե չարամիտ օգտագործողը կամ պրոցեսը ունենա ավելի շատ արտոնություններ, քան իրեն անհրաժեշտ է, այդ հանգամանքը կարող է նպաստել սերվերի կոտրմանը:

Ադմինիստրատորը պետք է համոզվի, որ բոլոր օգտագործողները մուտք ունեն միայն այն ֆայլերին և ռեսուրսներին, որոնք իրենց անհրաժեշտ են աշխատանքը իրականացնելու համար, և ոչ ավելին:

## 4. Ժամանակին տեղադրել անվտանգության թարմացումները

Կարևոր է տեղադրել օպերացիոն համակարգը և ծրագրային ապահովումը վերջին թարմացումներով և անվտանգության կարկատաններով (patches):

Օպերացիոն համակարգի և ծրագրային ապահովման ստեղծողները ժամանակ առ ժամանակ թողարկում են թարմացումներ (updates): Դրանք հաճախ պարունակում են անվտանգության թարմացումներ, որոնք փակում են հայտնաբերված խոցե-լիություններն օպերացիոն համակարգում:

Ադմինիստրատորները պետք է համոզվեն որ թարմացումները տեղադրվում են ժա-մանակին:

## 5. Դիտարկում և գրանցամատյանների գրառումների (logs) հաշվեքննություն

Լոգեր ստեղծվում են բոլոր տեսակի ծրագրային ապահովման կողմից - օպերացիոն համակարգի, վեբ հավելվածների, բոլոր տեսակի սերվիսների, տվյալների բազա-ների, ցանցային սարքերի, երթուղավորիչների, կոմուտատորների (network switch) և այլն կողմից:

Այս լոգերը պետք է դիտարկվեն և հաճախ ստուգվեն, քանի որ դրանք երբեմն կարող են զգուշացնել վերահաս վտանգի մասին: Նույնիսկ հաջող հարձակման դեպքում սերվերների լոգերը հաճախ դատական փորձաքննություն իրականացնե-լու միակ միջոցն են:

## 6. Օգտագործողի հաշիվներ

Չօգտագործվող օգտագործողի հաշիվները, ինչպիսիք են աշխատանքից

ազատված աշխատակիցների հաշիվները, պետք է անջատվեն: Պետք է անջատվեն նաև զանազան չօգտագործվող սերվիսների կողմից ստեղծված օգտագործողների հաշիվները:

Յուրաքանչյուր օգտագործողի հաշիվ մեծացնում է հարձակման հարթությունը: Նախկին աշխատակիցը կարող է ընկերությանը փաստ հասցնելու դրդապատճառներ ունենալ, և եթե նրա օգտագործողի հաշիվը անջատված չլինի՝ նա հնարավորություն կունենա ցանկացած գործողություն կատարել իր օգտագործողի իրավասություններով:

Յուրաքանչյուր ադմինիստրատոր և օգտագործող, ով մուտք է գործում սերվեր, պետք է ունենա իր սեփական հաշիվը և գաղտնաբառը, և ճիշտ իրավասություններ: Գաղտնաբառը չպետք է բաշխվի օգտագործողների միջև:

#### **7. Զնջել չօգտագործվող մոդուլներ և ընդլայնումներ**

Հավելվածները, ինչպես օրինակ վեբ սերվերները, հաճախ կարող են պարունակել որոշակի լռելյայն ընդլայնումներ և ծրագրային միավորներ (modules): Այս ծրագրային միավորները կարող են պարունակել խոցելիություններ, և այդպիսով մեծացնել հնարավոր հարձակման հարթությունը հակառակորդի համար:

Ադմինիստրատորը պետք է համոզվի, որ հնարավորության դեպքում միայն վեբ հավելվածների համար անհրաժեշտ միավորներն են առկա:

#### **8. Լինել տեղեկացված**

Այսօր օպերացիոն համակարգերի և ծրագրային ապահովման, այդ թվում՝ դրանց անվտանգության մասին ինֆորմացիան ազատորեն հասանելի է համացանցում:

Ադմինիստրատորները պետք է համոզվեն, որ իրենք և իրենց օգտագործողները մշտապես տեղեկացված են հարձակումների և խոցելիությունների մասին վերջին նորություններին:

#### **9. Օգտագործել սկզբնական կոդի (source code) անվտանգության սկաներներ**

Սկաներները ծրագրեր են, որոնք ավտոմատացնում և հեշտացնում են սերվերի և հավելվածների պաշտպանության գործընթացը:

Ծրագրային կոդի ստատիկ և դինամիկ անալիզի գործիքները, ինչպիսիք են Sonar-ը Java լեզվի համար, Valgrind-ը C լեզվի համար և այլն, օգնում են գտնել ծրագրային սխալներ (bugs) և խոցելիություններ ծրագրի կենսափուլի (lifecycle) վաղ շրջանում:

#### **10. Ընտրել գաղտնագրման և հեշավորման ապահով ալգորիթմներ**

Պետք է խուսափել կոտրված գաղտնագրման, հաղորդակցության և հեշավորման հաղորդակարգերի օգտագործումից, ինչպիսիք են՝ DES, SSL, MD5:

Այս հաղորդակարգերի թուլությունը հարձակման հնարավոր վեկտոր է բացում հակառակորդի համար:



Այսպիսի հաղորդակարգերը պետք է փոխարինվեն ժամանակակից, չկոտրված և գաղտնագրման լայն հանրության վստահությանը արժանացած հաղորդակարգերով:

#### 11. **Օգտագործել հակավիրուս**

Windows օպերացիոն համակարգի վրա հիմնված սերվերներում անհրաժեշտ է տեղադրել հակավիրուսային ծրագրային ապահովում [7]:

Հակավիրուսը սկանավորում է ծրագիրը հետևյալ պայմաններում [8]՝

- (a) ամբողջական սկաներ - թողարկվում են պարբերաբար կամ օգտագործողի կողմից,
- (b) աշխատանքի ժամանակ, այսինքն երբ համակարգով փոխանցվում են տվյալներ:

Հակավիրուսները օգտագործում են վիրուսների հայտնաբերման հետևյալ տեխնոլոգիաները՝

- (a) ստորագրության վրա հիմնված հայտնաբերում, երբ ֆայլը համեմատվում է հայտնի չարամիտ կոդի հետ,
- (b) փորձարարության վրա հիմնված հայտնաբերում, երբ ֆայլի վարվելաձևը համեմատվում է հայտնի չարամիտ նմուշների հետ,
- (c) վարվելակերպի վրա հիմնված հայտնաբերում, որը հաճախ կատարվում է ՆՀՀ-երում:

Linux-ի վրա հիմնված համակարգերում հակավիրուս հաճախ չի օգտագործվում [9]:

Linux-ի վրա հիմնված համակարգերում հակավիրուսի անհրաժեշտություն կարող է առաջանալ միայն այն պարագայում, երբ այն օգտագործվում է Windows համակարգերի միջև ֆայլերի փոխանակաման համար [10]:

#### 12. **Օգտագործել ցանցային սկաներներ**

Ցանցային սկաներները օգնում են ադմինիստրատորներին համոզվել իրենց սերվերների անվտանգության մեջ: Այսպիսի գործիքները կարողանում են հայտնաբերել բաց պորտեր, խոցելի սերվիսներ, և նույնիսկ վիրուսներ: Հայտնի ցանցային սկաներներից են [11]՝

- (a) Nmap,
- (b) Nessus,
- (c) Acunetix:

Համակարգային ադմինիստրատորների տարածված պարտականություններից է իրենց վստահված համակարգերում պորտերի սկանավորման իրականացումը:

Այսպիսի սկանավորումները օգնում են ադմինիստրատորներին գտնել խոցելիություններ իրենց համակարգերում ավելի վաղ, քան հնարավոր հակառակորդը: Ցանցային պորտերի սկանավորման պրոցեսը հաճախ ունի ներքոնշյալ հաջորդականությունը:

- (a) Ադմինիստրատորը որոշում է հասցեների և պորտերի շրջանակը, որոնք պետք է ենթարկվեն սկանավորման:
- (b) Նա ցանցային սկաներին է տալիս այդ պարամետրերը և սկսում է սկանավորման գործընթացը:
- (c) Ծրագիրը փորձարկում է IP հասցեների և պորտերի բոլոր տրված համադրությունները:
- (d) Եթե պարզվում է, որ պորտը բաց է, ապա աշխատեցվում է հատուկ ծրագրային սցենար (script), որը փորձում է գուշակել աշխատող սերվիսի մասին տվյալներ՝ անունը, տարբերակը, կոնֆիգուրացիան, մատչելի օգտագործողների անունները, և այլն:
- (e) Տվյալները տրվում են ադմինիստրատորին նրա նախընտրած ֆորմատով՝ XML, ելք հրամանային տողում կամ ծրագրին հատուկ ֆորմատով:

## 2 Խնդիրի դրվածքը

### 2.1 Խնդրի արդիականությունը

Նախորդ բաժնի վերջին կետում մշված ցանցային սկաներների ներկայիս իրականացումը ունի որոշակի թերություններ:

1. Ցանցում բազմաթիվ համակարգերի գոյության դեպքում յուրաքանչյուր TCP (Transmission Control Protocol) և UDP (User Datagram Protocol) պորտի սկանավորումը պահանջում է բավականին երկար ժամանակ: Սկանավորումը արագացնելու նպատակով հնարավոր է սկանավորել միայն պորտերի սահմանափակ բազմություն, սակայն այդ դեպքում պատկերը ամբողջական չի լինի, քանի որ ոչ հայտնի պորտերի տակ նույնպես հնարավոր է աշխատի ինչ-որ սերվիս, և այն չի հայտնաբերվի նման սկանավորման ժամանակ:
2. Ցանցային սկաները ծախսում է ցանցային ռեսուրսներ և կարող է որոշ համակարգեր անհասանելի դարձնել սկանավորման ընթացքում:
3. Որոշակի սցենարների դեպքում պորտերի սկանավորումը կարող է հանգեցնել IDS-ում (Intrusion Detection System - Ներխուժում Հայտնաբերող Համակարգ) կեղծ ահազանգի:
4. Հնարավոր են կեղծ դրական արդյունքներ և սերվիսների սխալ նույնականացումներ:
5. Չեն հայտնաբերվում բացթողումներ հետևյալ ասպարեզներում՝
  - թույլտվություններ և արտոնություններ,
  - թարմացումների առկայություն,
  - օգտագործողի հաշիվներ,
  - գաղտնագրման և հեշավորման ապահով ալգորիթմների օգտագործում,
  - հակավիրուսի օգտագործում:

Այսպիսով անհրաժեշտ է որոնել սկանավորում իրականացնելու մեկ այլ եղանակ, որը զերծ կլինի վերը նշված թերություններից:

### 2.2 Այլընտրանք

Այս աշխատանքում մենք ներկայացնում ենք սերվերների խոցելիությունների հայտնաբերման այլընտրանքային եղանակ, որը սկանավորում է համակարգերը ներսից, և այդպիսով զերծ է վերը նշված թերություններից:

Այս եղանակի էությունը կայանում է նրանում, որ անվտանգության սկանավորում իրականացնող ծրագիրը ստուգումներ կատարում է ոչ թե համակարգի դրսից՝ ցանցի և բաց

պորտերի միջոցով միայն, այլ այն աշխատում է հենց համակարգի ներսում: Այդ պատճառով այս եղանակը շատ ավելի լայն ստուգումներ իրականացնելու հնարավորություն ունի:

Օրինակ՝ հնարավոր է ստուգել յուրաքանչյուր սերվիսի կոնֆիգուրացիոն ֆայլ, կամ ստուգել առանց գաղտնաբառի օգտագործողի հաշիվների առկայությունը, ինչը անհնար է իրականացնել ցանցային սկանավորման պարագայում:

## **2.3 Նախկին փորձի ուսումնասիրություն**

### **2.3.1 Microsoft Baseline Security Analyzer**

MSBA-ը Windows համակարգերի համար նախատեսված անվտանգության սկաներ է, ստեղծված Microsoft ընկերության կողմից [12]: Այն գնահատում է Windows համակարգի և Microsoft-ի կողմից ստեղծված մի շարք այլ ծրագրային ապահովման անվտանգությունը առավել հաճախ հանդիպող սխալների առկայության համար և արդյունքները ներկայացնում է օգտագործողին:

MSBA-ը ունի որոշակի սահմանափակումներ՝

- աշխատում է միայն Windows ճարտարապետության համակարգերում,
- ստուգումներ իրականացնում է միայն Microsoft ընկերության կողմից ստեղծված ծրագրերում:

Այս ծրագրային ապահովման ճարտարապետությունը մասամբ ոգեշնչվել է MSBA ծրագրի կողմից:

### **2.3.2 Buck-Security**

Buck-Security-ն անվտանգության սկանավորիչ է Debian և Ubuntu Linux օպերացիոն համակարգերի համար [13][14]:

Այս աշխատանքում ներկայացվող ծրագիրը որոշ չափով նման է Buck-Security-ին: Buck-Security-ն նույնպես ունի որոշակի սահմանափակումներ՝

- նախատեսված է միայն Debian և Ubuntu համակարգերի համար,
- գտնվում է Beta փուլում, և խորհուրդ չի տրվում այն օգտագործել արտադրության համակարգերում:

### **2.3.3 Lynis**

Lynis-ը անվտանգության աուդիտի և համակարգի ամրապնդման (hardening) գործիք է UNIX համակարգերի համար: Այն օգնում է ադմինիստրատորներին արագ հայտնաբերել և լուծել անվտանգության սխալները [15]:

Աշխատում է Unix ընտանիքի օպերացիոն համակարգերի միջավայրում: Հանրային տարբերակը տարածվում է GPL3 լիցենզիայի տակ, կա նաև վճարովի, առևտրային լիցենզիայով տարբերակ [16]:

#### **2.3.4 MaxPatrol**

MaxPatrol-ը խոցելիությունների և կոնֆիգուրացիայի ստուգման համակարգ է, ստեղծված Positive Technologies ընկերության կողմից [17]: Այն հնարավորություն է տալիս իրականացնել խոցելիությունների և սխալ կոնֆիգուրացիաների նույնականացում ծրագրային հավելվածներում, տվյալների բազայում, ցանցում և օպերացիոն համակարգերում:

Ունի միայն վճարովի առևտրային տարբերակ:

#### **2.3.5 Tiger**

Tiger-ը անվտանգությունը գնահատող ծրագիր է UNIX համակարգերի համար:

Ցավոք, այն ներկայումս ակտիվորեն չի մշակվում: Վերջին կայուն տարբերակը թողարկվել է 2010 թվականին:

Աշխատում է Unix ընտանիքի օպերացիոն համակարգերի միջավայրում: Տարածվում է GPL3 լիցենզիայի տակ [18]:

### 3 Ծրագրին ներկայացվող պահանջներ

Այս աշխատանքի նպատակն է ստեղծել ծրագրային հավելված, որը Linux-ի վրա հիմնված սերվերային համակարգի վրա տեղադրման պարագայում աշխատեցնելիս կգնահատի համակարգերի անվտանգությունը և կհայտնի արդյունքները օգտագործողին:

Ծրագրային հավելվածի առաջնային նպատակն է օգտագործողին ներկայացնել համակարգի անվտանգության ընդհանուր պատկերը:

Ծրագիրը պետք է աշխատի բոլոր ժամանակակից Linux համակարգերի տակ: Հնարավորության դեպքում՝ նաև UNIX ընտանիքի այլ համակարգերում:

Ծրագրի տեղադրումը պետք է լինի հնարավորինս պարզ:

Ծրագրի ստուգումներից յուրաքանչյուրը պետք է հնարավոր լինի անջատել՝ մյուսներից անկախ:

Եթե ծրագրի մի մոդուլը իրականացնում է բազմատեսակ ստուգումներ, ապա դրանցից յուրաքանչյուրը պետք է հնարավոր լինի անջատել՝ մյուսներից անկախ:

Ստորև ներկայացվում է ծրագրի կողմից կատարվող ստուգումների ցանկը:

#### 3.1 Ծրագրային թարմացումներ

Ծրագիրը պետք է ստուգի թե վերջին անգամ երբ է թարմացվել օպերացիոն համակարգը: Եթե դա կատարվել է բավականաչափ ուշ, ապա օգտագործողը պետք է զգուշացվի, հայտնելով վերջին թարմացման ժամանակը [19]:

Այդ ժամանակային միջակայքը պետք է հնարավոր լինի կարգաբերել ծրագրի կոնֆիգուրացիայով:

Ստորև ներկայացված են Linux-ի յուրաքանչյուր տարբերակին առանձնահատուկ վերջին թարմացման ժամանակի ստուգումները՝

##### 3.1.1 Debian/APT-ի վրա հիմնված համակարգեր

Ծրագիրը պետք է որոշի վերջին թարմացման ժամանակը `/var/lib/apt/periodic/update-success-stamp` ֆայլի ստեղծման ժամանակով [20]:

Դա Ubuntu ընտանիքին հատուկ ֆայլ է, որի ստեղծման ժամանակը համընկնում է `apt-get update` հրահանգի վերջին կատարման ժամանակի հետ: Դա պայմանավորված է նրանով, որ նշված հրահանգը կատարելիս աշխատեցվում է `/etc/apt/apt.conf.d/15update-stamp` ծրագիրը, որը և թարմացնում է նշված դրոշմ-ֆայլը՝ վերագրելով նրա ստեղծման ժամանակը այդ ժամանակային պահին (timestamp) [20]:

##### 3.1.2 Red Hat/YUM-ի վրա հիմնված համակարգեր

Ծրագիրը պետք է որոշի վերջին թարմացման ժամանակը՝ `'yum history'` հրահանգի ելքը (output) վերլուծելով [22]:

`yum history` հրահանգը արտաձում է նմանօրինակ ելք՝

## Սկզբնական կոդ 1: .

```
# yum history
Loaded plugins: fastestmirror, refresh-packagekit
ID      | Login user          | Date and time      | Action(s)          | Altered
-----|-----|-----|-----|-----
41 | root <root>          | 2012-04-27 20:17 | Install            | 19
40 | root <root>          | 2011-11-20 10:09 | Install            | 10
39 | root <root>          | 2011-11-20 08:14 | Install            | 1 E<
38 | root <root>          | 2011-11-19 15:46 | Update             | 1
```

Օպերացիոն համակարգի վերջին թարմացման ժամանակը հնարավոր է որոշել այս կերպ՝ այս ելքում վերջից փնտրելով 'Update' բառը, այնուհետև առաջին համընկնող տողում վերլուծելով 'Date and time' սյան արժեքը:

### 3.1.3 Arch Linux/Pacman-ի վրա հիմնված համակարգեր

Pacman փաթեթների մենեջերի գործողությունների գրանցամատյանը գտնվում է '/var/log/pacman.log' ֆայլում [24]: Ծրագիրը պետք է ստուգի վերջին թարմացման ժամանակը վերլուծելով վերոնշյալ ֆայլի պարունակությունը: Այն ունի նմանօրինակ պարունակություն՝

## Սկզբնական կոդ 2: .

```
[2016-04-05 10:22] [ALPM] transaction started
[2016-04-05 10:23] [ALPM] installed pycharm-community (2016.1-1)
[2016-04-05 10:23] [ALPM] transaction completed
[2016-04-05 10:24] [PACMAN] Running 'pacman -S -y -y -u'
[2016-04-05 10:24] [PACMAN] synchronizing package lists
[2016-04-05 10:24] [PACMAN] starting full system upgrade
[2016-04-05 10:24] [PACMAN] Running 'pacman -S -y -y -u'
[2016-04-05 10:24] [PACMAN] synchronizing package lists
[2016-04-05 10:24] [PACMAN] starting full system upgrade
[2016-04-05 10:28] [ALPM] transaction started
[2016-04-05 10:28] [ALPM] upgraded tzdata (2016b-1 -> 2016c-1)
[2016-04-05 10:28] [ALPM] upgraded alsa-utils (1.1.0-1 -> 1.1.0-2)
[2016-04-05 10:28] [ALPM] upgraded graphite (1:1.3.6-1 -> 1:1.3.8-1)
[2016-04-05 10:28] [ALPM] upgraded harfbuzz (1.2.3-1 -> 1.2.4-1)
[2016-04-05 10:28] [ALPM] upgraded fontconfig (2.11.1-2 -> 2.11.94-1)
[2016-04-05 10:28] [ALPM-SCRIPTLET] updating font cache... done.
[2016-04-05 10:28] [ALPM] installed tslib (1.1-1)
[2016-04-05 10:28] [ALPM] upgraded libxkbcommon (0.5.0-1 -> 0.6.0-1)
```

Օպերացիոն համակարգի վերջին թարմացման ժամանակը հնարավոր է որոշել այս ելքում վերջից փնտրելով 'starting full system update' նախադասությունը, այնուհետև առաջին համընկնող տողում վերլուծելով ժամանակը, որը գտնվում է առաջին քառակուսի փակագծերի մեջ:

## 3.2 Ֆայլերի և դիրեկտորիաների թույլտվություններ

Բոլոր ֆայլերը և դիրեկտորիաները պետք է ունենան ճիշտ թույլտվություններ: Հակառակ դեպքում համակարգը խոցելի է: Բոլոր օգտագործողների կողմից գրման հնարավորություն ունեցող (worldwritable) ֆայլերը և դիրեկտորիաները կարող են օգտագործվել հակառակորդի կողմից՝ կամեցած ֆայլի կամ դիրեկտորիայի մեջ ցանկացած բան փոփոխելու կամ ջնջելու համար [25][13]:

Բացառություն են կազմում այն worldwritable դիրեկտորիաները, որոնք ունեն sticky բիթ, ինչպես նաև այն բոլոր ֆայլերը որոնք չեն սկսվում կետով և չեն պատկանում համակարգային օգտագործողին:

Linux-ի ֆայլային համակարգերում sticky բիթը դիրեկտորիայի հատուկ ատրիբուտ է: Եթե այն առկա է, ապա նշանակում է որ նրանում պարունակվող ֆայլերի տերը միայն (owner) և համակարգային օգտագործողը (root user) իրավունք ունեն ջնջել կամ վերանվանել վերոնշյալ ֆայլը [26]:

Այսպիսով, այս ստուգման ժամանակ նման ֆայլերի և դիրեկտորիաներ որոնման ժամանակ պետք է կիրառել հետևյալ ֆիլտրը՝

- worldwritable դիրեկտորիաները պետք է ունենան sticky բիթ
- worldwritable ֆայլերը չպետք է սկսվեն կետով ('')
- worldwritable ֆայլերը չպետք է պատկանեն համակարգային օգտագործողին (root user)

Նման ֆայլերի հայտնաբերման դեպքում ծրագիրը պետք է զգուշացնի, և թվարկի այդ ֆայլերը:

## 3.3 Բաց TCP և UDP պորտեր

Յուրաքանչյուր բաց պորտ մեծացնում է հարձակման հարթությունը [27]:

Այդ պատճառով անհրաժեշտ է սահմանափակել բաց պորտերի քանակը, կամ դրանք ծածկել firewall-ով:

Ծրագիրը պետք է օգտագործողին ներկայացնի բոլոր բաց TCP և UDP պորտերի ցանկը, և դրանց տակ աշխատող սերվիսների անունները, հնարավորության դեպքում՝ նաև այն կատարվող ֆայլի անունը, որը գործարկվել է սերվիսը աշխատեցնելիս:

## 3.4 Մուտք որպես համակարգային օգտագործող (root user)

Համակարգային օգտագործողով մուտքը համակարգ համարվում է վատ գործելակերպ անվտանգության տեսանկյունից ներքոնշյալ պատճառներով [28]:

1. Շատ հաճախ առօրյա աշխատանքում հասարակ օգտագործողի իրավասությունները միանգամայն բավարար են ամենօրյա գործունեությունը իրականացնելու համար: Բացառություն է կազմում համակարգում ծրագրեր տեղադրումը, կոնֆի-



գուրացիայի փոփոխությունը և այլ ադմինիստրատիվ գործեր, որոնք հազվադեպ են անհրաժեշտ լինում:

2. Օգտագործողը կարող է պատահաբար սխալ հրաման գործարկել, ինչը որոշ դեպքերում կարող է կործանարար հետևանքներ ունենալ:
3. Եթե ծրագրերը աշխատեցվեն համակարգային օգտագործողի իրավասություններով, ապա նրանցում առկա խոցելիությունները և ծրագրային սխալները (bugs) շատ ավելի մեծ վնաս կարող են հասցնել, քանի որ հասանելի է ամբողջ համակարգը: Իսկ որպես հասարակ օգտագործող իրականացնելիս խոցելի է միայն նշված օգտագործողին պատկանող ֆայլերը և նրա իրավասության տակ գտնվող արտոնությունները:

Եթե օգտագործողը մուտք է գործել համակարգ որպես համակարգային օգտագործող, ապա պետք է զգուշացնել [29]:

Բացառություն է կազմում այն դեպքը, եթե ծրագիրը իրականացվում է 'sudo' հրահանգով: Այս դեպքում զգուշացում չի կատարվում:

### 3.5 Օգտագործողների Umask ստուգում

Umask-ը օգտագործողի սեսիայի և պրոցեսների ատրիբուտ է, որը որոշում է, թե նոր ստեղծված ֆայլերը ինչ թույլտվություններ պետք է ունենան: Նոր ստեղծված ֆայլի թույլտվությունները լռելյայն վերագրվում են Umask-ի բիթային հակադարձ արժեքին (bitwise not) [30]:

Եթե օգտագործողի Umask-ը այնպիսին է, որ ստեղծում է worldwritable ֆայլեր, ապա սա ունի նույն թերությունները ինչ ֆայլերի և դիրեկտորիաների սխալ թույլտվություններ ունենալը [31]:

Ծրագիրը պետք է ստուգի ներկայիս օգտագործողի Umask-ը, և եթե այն ստեղծում է ֆայլեր, որոնք այլ օգտագործողների կողմից գրելու հնարավորություն ունեն, ապա օգտագործողը զգուշացվում է: Հակառակ դեպքում ստուգումը հաջողված է:

### 3.6 SSHd սերվիսի կոնֆիգուրացիայի ստուգում

SSHd սերվիսի կոնֆիգուրացիոն ֆայլն է /etc/ssh/ssh\_config:

Այսօր խոցելի համարվող SSH v1 հաղորդակարգը չպետք է միացված լինի, քանի որ այն պարունակում է մի շարք խոցելիություններ [32]:

## 4 Իրականացում

Ծրագրի սկզբնական կոդը (source code) հասանելի է <https://github.com/axper/imap> հասցեով:

### 4.1 Ծրագրավորման լեզվի ընտրություն

Ծրագրի իրականացման համար ընտրվել է Python 3 լեզուն: Այն ունի մի շարք առավելություններ նշված խնդրի իրականացման համար [33]՝

1. Python-ի շարահյուսությունը չափազանց հեշտ է և սովորել և հասկանալ,
2. Python-ը անվճար է և ունի ազատական լիցենզիա,
3. Python-ը աշխատում է բոլոր հիմնական օպերացիոն համակարգերում՝ Windows, Linux, OS X,
4. Python-ը ունի ներդրված և հասանելի գրադարանների առատ բազմություն:

### 4.2 Ծրագրային պահանջներ

Ծրագրի աշխատանքի համար անհրաժեշտ է՝

1. Unix-ի վրա հիմնված օպերացիոն համակարգ,
2. Python 3.5.1+
3. 'psutil' (python process and system utilites) Python գրադարանը:

### 4.3 Մոդուլների իրականացումը

#### 4.3.1 Հիմնական մոդուլը՝ `imap.py`

Հիմնական մոդուլը կարդում է ծրագրի կոնֆիգուրացիան `config.yml` ֆայլից, որը գտնվում է նույն դիրեկտորիայում, ինչ և `imap.py` ֆայլը: Այնուհետև հերթով աշխատեցվում են բոլոր ստուգող ենթամոդուլները:

Ամեն ենթամոդուլի աշխատանքից առաջ տպվում է մոդուլի անունը: Աշխատանքի ավարտից հետո տպվում է թե արդյոք ստուգումը հաջող է անցել: Եթե ոչ՝ այնուհետև տպվում է հաղորդագրությունը:

#### 4.3.2 Ծրագրային թարմացումներ՝ `update.py`

Նախ ծրագիրը որոշում է թե ինչ օպերացիոն համակարգի միջավայրում է այն աշխատում: Այս խնդրի լուծման համար օգտագործվել է `platform.linux_distribution()` կանչը: Կախված այդ կանչի արդյունքից աշխատեցվում է օպերացիոն համակարգին հատուկ ծրագիրը, որը որոշում է համակարգի վերջին թարմացման ժամանակը:

- Եթե ծրագիրը աշխատում է Arch Linux միջավայրում, ապա ծրագիրը տող-առ-տող կարդում է `/var/log/pacman.log` ֆայլի պարունակությունը: Եթե հերթական տողում առկա է `'starting full system upgrade'` բառակապակցությունը, ապա ծրագիրը դադարեցնում է կարդալ տողերը և վերջին թարմացման ժամանակը համարում է նշված տողի առաջին քառակուսի փակագծերի միջև գտնվող ժամանակային գրառումը:

Եթե `'starting full system upgrade'` բառակապակցությունը չի հայտնաբերվել, ապա ծրագիրը հայտնում է ստուգման անհնարինության մասին:

- Եթե ծրագիրը աշխատում է Debian կամ Ubuntu Linux միջավայրում, ապա ծրագիրը որոշում է `/var/lib/apt/periodic/update-success-stamp` ֆայլի վերջին փոփոխման ժամանակը:

Եթե ֆայլը չի հայտնաբերվել, ապա ծրագիրը հայտնում է ստուգման անհնարինության մասին:

- Եթե ծրագիրը աշխատում է Red Hat/CentOS միջավայրում, ապա ծրագիրը տող-առ-տող կարդում է `yum history` հրահանգի ելքը: Եթե հերթական տողում առկա է `'Update'` բառը, ապա ծրագիրը դադարեցնում է կարդալ տողերը և վերջին թարմացման ժամանակը համարում է նշված տողի `Date and time` սյունակում գտնվող ժամանակային գրառումը:

Եթե `'Update'` բառը չի հայտնաբերվել, ապա ծրագիրը հայտնում է ստուգման անհնարինության մասին:

Ստացված ամսաթիվը համեմատվում է ծրագրի կոնֆիգուրացիայի `update.warn_last_update_interval_days` գրառման հետ: Եթե վերջին թարմացման ամսաթիվը ավելի նոր է, ապա ստուգումը համարվում է հաջող, հակառակ դեպքում՝ անհաջող:

#### 4.3.3 Ֆայլերի և դիրեկտորիաների թույլտվություններ՝ `worldwritable.py`

Նախ ծրագիրը փնտրում է հետևյալ ֆիլտրին համապատասխանող բոլոր ֆայլերը և դիրեկտորիաները՝

1. ֆայլեր, որոնք `worldwritable` են և սկսվում են կետով,
2. դիրեկտորիաներ, որոնք `worldwritable` են և չունեն `sticky` բիթ,
3. ֆայլեր, որոնք `worldwritable` են և պատկանում են համակարգային օգտագործողին (`root`):

Ֆայլերի և դիրեկտորիաների փնտրումը կատարվում է `os.walk()` կանչի օգնությամբ, իսկ ատրիբուտների ստուգումը՝ `os.stat()` կանչով:

Եթե վերոնշյալ պայմաններին համապատասխանող ֆայլեր կամ դիրեկտորիաներ հայտնաբերվել են, ապա ծրագիրը արտածում է թե որ պայմանն է խախտվել, և այդ ֆայլերի կամ դիրեկտորիաների ցուցակը:

Եթե մի քանի պայմաններ են խախտվել, ապա յուրաքանչյուր պայմանի համար կատարվում է առանձին ելք:

#### 4.3.4 Բաց TCP և UDP պորտեր՝ `openports.py`

Նախ ծրագիրը ստանում է համակարգում առկա բոլոր `inet` տեսակի միացումների ցանկը `psutil.net_connections()` կանչի օգնությամբ [34]: Այնուհետև ֆիլտրվում են բաց և դրսից հասանելի TCP և UDP պորտերի միացումները: Ելքում ստացվում է մի աղյուսակ որի սյուներն են՝

1. պորտի միացման տիպը՝ TCP կամ UDP [35],
2. IP հասցեն,
3. պորտը՝ TCP միացման դեպքում,
4. PID՝ Պրոցեսի նույնականացման համարը,
5. Username՝ Օգտագործողի անունը,
6. Command line՝ Հրահանգը, որը աշխատեցվել է այդ պորտի տակ լսող ծրագիրը գործարկելիս:

#### 4.3.5 Մուտք որպես համակարգային օգտագործող՝ `root.py`

Ծրագիրը ստուգում է ներկայիս օգտագործողի UID-ն:

Նկատենք, որ Unix համակարգերում համակարգային օգտագործողի UID-ն միշտ 0 է: Այլ օգտագործողների UID-ները 0-ից տարբեր են:

Բացի դրանից հնարավոր է որ այս ծրագիրը իրականացվի `sudo` հրամանի միջավայրում: Սա համարվում է նորմալ գործելակերպ: Որպեսզի ստուգենք, թե գտնվում ենք `sudo` միջավայրում թե ոչ՝ պետք է ստուգել `SUDO_UID` միջավայրի փոփոխականի առկայությունը:

Այսպիսով, ծրագիրը գործարկվում է համակարգային օգտագործողի կողմից, եթե՝

1. օգտագործողի UID-ն 0 է,
2. `SUDO_UID` միջավայրի փոփոխականը առկա չէ:

Եթե այս 2 պայմանները բավարարված են, ապա օգտագործողին պետք է զգուշացնել, հակառակ դեպքում ստուգումը հաջողված է:

#### 4.3.6 Օգտագործողների Umask ստուգում՝ `umask.py`

Python-ի `os.umask()` կանչը պահանջում է տեղադրել նոր Umask. Քանի որ չի պահանջվում փոխել Umask-ը, այլ միայն ստանալ դրա արժեքը, ծրագիրը նախ ստանում է այն՝ դնելով նոր արժեքը 0777: Այնուհետև ծրագիրը վերագում է `umask`-ը ստացված արժեքին [36]:

Այնուհետև ստուգվում է ստացված Umask-ի արժեքի stat.S\_IWOTH բիթը: Այդ բիթը ցույց է տալիս այլ օգտագործողների գրելու իրավասությունը: Եթե այդ բիթը առկա չէ, այսինքն լռելայն նոր ֆայլերը կարող են փոփոխվել ցանկացած օգտագործողի կողմից, ապա օգտագործողը զգուշացվում է: Հակառակ դեպքում ստուգումը համարվում է հաջողված:

#### **4.3.7 SSHd սերվիսի կոնֆիգուրացիայի ստուգում**

Ծրագիրը տող-առ-տող զննում է /etc/ssh/ssh\_config ֆայլի պարունակությունը: Եթե հայտնաբերվում է տող, որը պարունակում է Protocol-ի կոնֆիգուրացիան, ապա ստուգվում է, թե արդյոք SSH-ի առաջին տարբերակը միացված է: Եթե Protocol բառը չի հայտնաբերվում, դա նշանակում է որ միայն լռելայն v2-ն է թույլատրված:

Այսպիսով, եթե v1 -ը միացված է, ապա օգտագործողը զգուշացվում է: Հակառակ դեպքում զգուշացում չի կատարվում:

## 5 Եզրակացություն

Ներկայումս օգտագործվող ցանցային սկանավորիչները սահմանափակ են իրենց կարողություններում՝ անվտանգությանը նպաստելու տեսանկյունից:

Այս աշխատանքի շրջանակներում ստեղծվել է Linux սերվերային համակարգերի անվտանգությունը գնահատող ծրագիր՝ գրված Python լեզվով:

Այն օգնում է համակարգային ադմինիստրատորներին տեղեկանալ իրենց վստահված սերվերների անվտանգության մակարդակի մասին, այսպիսով նպաստելով անվտանգության մակարդակի բարձրացմանը:

Նմանօրինակ ծրագրային հավելվածը շատ ավելի արդյունավետ կարող է լինել բազմակողմանի աջակցության (support) և երկարատև զարգացման (development) դեպքում:

## Գրականության ցանկ

1. Definition of "information security (infosec)"  
TechTarget, 2014  
<http://searchsecurity.techtarget.com/definition/information-security-infosec>
2. What is computer security and why should I care about computer security?  
Sanjay Bhalerao, 2005  
[http://cybercellmumbai.gov.in/html/general-tips/what\\_is\\_computer\\_security.html](http://cybercellmumbai.gov.in/html/general-tips/what_is_computer_security.html)
3. Web Server Security and Database Server Security  
acunetix.com  
<http://www.acunetix.com/websitesecurity/webserver-security/>
4. Why Would Hackers Hack My Website ?  
onehoursitefix.com Support, 2016  
<https://www.onehoursitefix.com/why-would-hackers-hack-my-website/>
5. What is a DDoS Attack?  
Arbor Networks, Inc., 2013  
<http://www.digitalattackmap.com/understanding-ddos/>
6. Linux Internet Server Security and Configuration Tutorial  
Greg Ippolito, 2015  
<http://www.yolinux.com/TUTORIALS/LinuxTutorialInternetSecurity.html>
7. Do you run antivirus on your Windows servers?  
Richard Slater, 2009  
<http://serverfault.com/questions/632/do-you-run-antivirus-on-your-windows-servers>
8. How Antivirus Works?  
comodo.com, 2016  
<https://antivirus.comodo.com/how-antivirus-software-works.php>
9. HTG Explains: Why You Don't Need an Antivirus On Linux (and When You Do)  
Chris Hoffman, 01/29/13  
<http://www.howtogeek.com/135392/htg-explains-why-you-dont-need-an-antivirus-on-linux-and-when-you-do/?PageSpeed=noscript>

10. Virus scanner on server  
Tyler Larson, 2014  
<http://security.stackexchange.com/a/53462/37546>
11. Top Network Security Tools  
Gordon Lyon, 2011  
<http://sectools.org/>
12. How To: Use the Microsoft Baseline Security Analyzer  
MSDN, 2007  
<https://msdn.microsoft.com/en-us/library/ff647642.aspx>
13. Security Scanner for Debian and Ubuntu Linux  
David Schmidt, 2015  
<http://www.buck-security.net/buck-security.html>
14. Collection of security checks for Linux  
Lazy to Hack, 2010  
<http://lazy2hack.blogspot.am/2010/03/collection-of-security-checks-for-linux.html>
15. Lynis - Security auditing tool  
CISOfy, 2016  
<https://github.com/CISOfy/lynis/>
16. Plans & Pricing  
CISOfy  
<https://cisofy.com/pricing/>
17. Cutting-edge protection against advanced it and ot threats  
Positive Technologies  
<http://www.ptsecurity.com/products/#maxpatrol>
18. Tiger git repository  
Javier Fernandez-Sanguino  
<http://git.savannah.gnu.org/cgiit/tiger.git/>
19. Updates And Patches  
The Board of Trustees at the University of Illinois  
<https://security.illinois.edu/content/updates-and-patches>
20. Find last time update was performed with apt-get  
Tuomas, 2012  
<http://serverfault.com/questions/20747/find-last-time-update-was-performed-with-apt-get>



22. How to check when yum update was last run  
Chakravarthy Girda, 2012  
<http://serverfault.com/questions/389650/how-to-check-when-yum-update-was-last-run>
24. Can I find when I last ran Pacman Update?  
Jason Wryan, 2012  
<https://bbs.archlinux.org/viewtopic.php?id=150428>
25. Detecting world writable files and directories  
Dr. Nikolai Bezroukov, 2013  
[http://www.softpanorama.org/Access\\_control/Permissions/world\\_writable\\_files\\_problem.shtml](http://www.softpanorama.org/Access_control/Permissions/world_writable_files_problem.shtml)
26. Linux Sticky Bit Concept Explained with Examples  
Himanshu Arora, 2013  
<http://www.thegeekstuff.com/2013/02/sticky-bit/>
27. Why is it bad to have open ports?  
Mark Marra, 2009  
<http://superuser.com/questions/82488/why-is-it-bad-to-have-open-ports>
28. Why is it a bad idea to run as root?  
Birck Renan, 2012  
<http://unix.stackexchange.com/questions/52268/why-is-it-a-bad-idea-to-run-as-root>
29. Why is it bad to login as root?  
Marlon Rodriguez, 2010  
<http://askubuntu.com/questions/16178/why-is-it-bad-to-login-as-root>
30. The Open Group Base Specifications Issue 7 - Umask Manpage  
The IEEE and The Open Group, 2013  
<http://pubs.opengroup.org/onlinepubs/9699919799/utilities/umask.html>
31. What is Umask and How To Setup Default umask Under Linux?  
Vivek G, 2007  
<http://www.cyberciti.biz/tips/understanding-linux-unix-umask-value-usage.html>

32. Widespread Exploitation of SSH CRC32 Compensation Attack  
IBM Internet Security Systems X-Force, 2001  
<http://www.iss.net/threats/advises/100.html>
33. Why learn Python  
wikiversity.org  
[https://en.wikiversity.org/wiki/Python/Why\\_learn\\_Python](https://en.wikiversity.org/wiki/Python/Why_learn_Python)
34. psutil documentation  
Giampaolo Rodola  
<https://pythonhosted.org/psutil/>
35. Python 2 documentation  
Python Software Foundation  
<https://docs.python.org/2/library/socket.html>
36. Python: Getting umask without change  
Orkus, 2011  
<https://orkus.wordpress.com/2011/04/17/python-getting-umask-without-change/>

ՀԱՎԵԼՎԱԾ

## Սկզբնական կոդ

Սկզբնական կոդ 3: config.yml

```
update:
  warn_last_update_interval_days: 5
```

Սկզբնական կոդ 4: scan\_status.py

```
from enum import Enum
```

```
class ScanStatus(Enum):
    success = 1
    fail = 2
    unknown = 3
```

Սկզբնական կոդ 5: base\_scanner.py

```
class BaseScanner:
    def scan(self):
        # Returns a tuple:
        # (ScanStatus, message)
        raise NotImplementedError()
```

Սկզբնական կոդ 6: lmap.py

```
import os

import yaml

from openports import OpenPorts
from root import Root
from ssh import Ssh
from umask import Umask
from update import Update
from worldwritable import WorldWritable

def main():
    """
    Runs the program
    """
    config = get_config()
    scanners = [
        Update(config),
        OpenPorts(config),
        Root(config),
        Umask(config),
        Ssh(config),
        WorldWritable(config),
```

```

]
for scanner in scanners:
    print('-' * 79)
    print('Running:', scanner.__class__.__name__)
    result = scanner.scan()
    print('Status:', result[0])
    print('Message:\n' + result[1])

def get_config():
    """
    :return: A dictionary containing the program's configuration.
    """
    with open(os.path.dirname(os.path.realpath(__file__)) + '/' + 'config.yml',
              'r') as f:
        return yaml.load(f)

if __name__ == '__main__':
    main()

```

#### Սկզբնական կոդ 7: test\_lmap.py

```

import unittest
from unittest.mock import MagicMock

import lmap

def raise_file_not_found_error(x):
    raise FileNotFoundError

class Test(unittest.TestCase):
    def test_get_config(self):
        # Prepare data and mocks

        # Run test scenario
        result = lmap.get_config()

        # Assertions
        self.assertIsNotNone(result)
        self.assertIsInstance(result, dict)

    @unittest.mock.patch('lmap.OpenPorts')
    @unittest.mock.patch('lmap.Update')
    @unittest.mock.patch('lmap.WorldWritable')
    @unittest.mock.patch('lmap.Umask')
    def test_main(self, mock_open_ports, mock_update, mock_world_writable, mock_

```

```

    umask):
    # Prepare data and mocks
    config = MagicMock()
    lmap.get_config = MagicMock(return_value=config)

    # Run test scenario
    lmap.main()

    # Assertions
    lmap.get_config.assert_called_once_with()

if __name__ == '__main__':
    unittest.main()

```

### Սկզբնական կոդ 8: openports.py

```

from socket import SOCK_DGRAM
from socket import SOCK_STREAM

import psutil

from base_scanner import BaseScanner
from scan_status import ScanStatus

class OpenPorts(BaseScanner):
    def __init__(self, config):
        # config is a dictionary of this program's configuration
        self.config = config

    def scan(self):
        """
        :returns: a tuple of (ScanStatus, message).
        """
        output = 'Type, IP, Port, PID, Username, Command line\n'
        for connection in psutil.net_connections(kind='inet'):
            if self.is_port_is_open_and_externally_accessible(connection):
                output += self.get_line_for_connection(connection)
        return ScanStatus.success, output

    def get_line_for_connection(self, connection):
        """
        :returns: the single-line information about given connection. The line e
            nds with a newline.
        """
        line = [
            self.get_connection_type_string(connection.type),
            str(connection.laddr[0]) + ':' + str(connection.laddr[1]),

```

```

        connection.pid,
    ]
    if connection.pid is not None:
        process = psutil.Process(connection.pid)
        line.append(process.username())
        line.append(' '.join(process.cmdline()))
    return ' '.join(str(i) for i in line)

def is_port_is_open_and_externally_accessible(self, connection):
    # Checks whether given connection's port is open and externally accessible
    # Returns True if is, otherwise False
    if connection.type == SOCK_STREAM:
        return connection.status == 'LISTEN'
    if connection.type == SOCK_DGRAM:
        return True

def get_connection_type_string(self, connection_type):
    # connection_type: socket.SOCK_STREAM or friends
    # Returns 'tcp' for socket.SOCK_STREAM, 'udp' for socket.SOCK_DGRAM
    # Raises ValueError if connection_type is anything else
    if connection_type == SOCK_DGRAM:
        return 'udp'
    elif connection_type == SOCK_STREAM:
        return 'tcp'
    else:
        raise ValueError('Unknown connection type: ', connection_type)

```

### Աղբյուրական կոդ 9: test\_openports.py

```

import unittest
from socket import SOCK_DGRAM, SOCK_STREAM
from unittest.mock import MagicMock, call

from openports import OpenPorts
from scan_status import ScanStatus

def raise_file_not_found_error(x):
    raise FileNotFoundError

class Test(unittest.TestCase):
    @unittest.mock.patch('openports.psutil')
    def test_scan(self, mock_psutil):
        # Prepare data and mocks
        test_subject = OpenPorts(None)
        mock_psutil.net_connections = MagicMock(return_value=[
            'closed connection', 'open connection'])

```

```

test_subject.is_port_is_open_and_externally_accessible = MagicMock(side_
    effect=[False, True])
test_subject.get_line_for_connection = MagicMock(return_value='open conn
    ection line')

# Run test scenario
result = test_subject.scan()

# Assertions
self.assertEqual(result[0], ScanStatus.success)
self.assertIsNotNone(result[1])
mock_psutil.net_connections.assert_called_once_with(kind='inet')
test_subject.is_port_is_open_and_externally_accessible.assert_has_calls(
    [
        call('closed connection'),
        call('open connection')
    ]
)
test_subject.get_line_for_connection.assert_called_once_with('open conne
    ction')

def test_port_is_open_and_externally_accessible_when_udp(self):
    # Prepare data and mocks
    test_subject = OpenPorts(None)
    connection = MagicMock()
    connection.type = SOCK_DGRAM

    # Run test scenario
    result = test_subject.is_port_is_open_and_externally_accessible(connecti
        on)

    # Assertions
    self.assertTrue(result)

def test_port_is_open_and_externally_accessible_when_tcp_and_connection_stat
    us_is_listen(self):
    # Prepare data and mocks
    test_subject = OpenPorts(None)
    connection = MagicMock()
    connection.type = SOCK_STREAM
    connection.status = 'LISTEN'

    # Run test scenario
    result = test_subject.is_port_is_open_and_externally_accessible(connecti
        on)

    # Assertions
    self.assertTrue(result)

```



```

def test_port_is_open_and_externally_accessible_when_tcp_and_connection_status_is_not_listen(self):
    # Prepare data and mocks
    test_subject = OpenPorts(None)
    connection = MagicMock()
    connection.type = SOCK_STREAM
    connection.status = 'Not LISTEN'

    # Run test scenario
    result = test_subject.is_port_is_open_and_externally_accessible(connection)

    # Assertions
    self.assertFalse(result)

def test_get_connection_type_string_when_tcp(self):
    # Prepare data and mocks
    test_subject = OpenPorts(None)

    # Run test scenario
    result = test_subject.get_connection_type_string(SOCK_STREAM)

    # Assertions
    self.assertEqual(result, 'tcp')

def test_get_connection_type_string_when_udp(self):
    # Prepare data and mocks
    test_subject = OpenPorts(None)

    # Run test scenario
    result = test_subject.get_connection_type_string(SOCK_DGRAM)

    # Assertions
    self.assertEqual(result, 'udp')

def test_get_connection_type_string_when_other(self):
    # Prepare data and mocks
    test_subject = OpenPorts(None)

    # Run test scenario
    with self.assertRaises(ValueError):
        test_subject.get_connection_type_string(None)

    # Assertions

def test_get_line_for_connection_when_unknown_pid(self):
    # Prepare data and mocks

```

```

test_subject = OpenPorts(None)
connection = MagicMock()
connection.type = SOCK_DGRAM
connection.laddr = ('127.0.0.1', 80)
connection.pid = None
test_subject.get_connection_type_string = MagicMock(return_value='udp')

# Run test scenario
result = test_subject.get_line_for_connection(connection)

# Assertions
self.assertEqual('udp 127.0.0.1:80 None', result)

@unittest.mock.patch('openports.psutil')
def test_get_line_for_connection_when_known_pid(self, mock_psutil):
    # Prepare data and mocks
    test_subject = OpenPorts(None)
    connection = MagicMock()
    connection.type = SOCK_DGRAM
    connection.laddr = ('127.0.0.1', 80)
    connection.pid = 300
    process = MagicMock()
    process.username = MagicMock(return_value='Babken')
    process.cmdline = MagicMock(return_value=['ls', '-l', '-a'])
    test_subject.get_connection_type_string = MagicMock(return_value='udp')
    mock_psutil.Process = MagicMock(return_value=process)

    # Run test scenario
    result = test_subject.get_line_for_connection(connection)

    # Assertions
    self.assertEqual('udp 127.0.0.1:80 300 Babken ls -l -a', result)
    mock_psutil.Process.assert_called_once_with(connection.pid)

if __name__ == '__main__':
    unittest.main()

```

### Սկզբնական կոդ 10: update.py

```

import os
import platform
import re
from datetime import datetime, timedelta

from base_scanner import BaseScanner
from scan_status import ScanStatus

```

```

class Update(BaseScanner):
    def __init__(self, config):
        # config is a dictionary of this program's configuration
        self.config = config

    def scan(self):
        distribution_name = platform.linux_distribution()[0]
        if distribution_name == 'arch':
            return self.scan_arch()
        elif distribution_name == 'debian':
            return self.scan_debian()
        elif distribution_name == 'redhat':
            return self.scan_redhat()
        else:
            return ScanStatus.unknown, ''

    def scan_arch(self):
        # Scans the pacman log file, and checks whether the last system update d
        ate is older than required
        # Returns a tuple: (ScanStatus, message)
        config_update_interval_days = int(self.config['update']['warn_last_updat
        e_interval_days'])
        with open('/var/log/pacman.log') as f:
            last_update_date = self.get_pacman_last_update_date(f.readlines())
            if last_update_date is None:
                return ScanStatus.unknown, ''
            elif datetime.today() - last_update_date < timedelta(days=config_upd
            ate_interval_days):
                return ScanStatus.success, ''
            else:
                return ScanStatus.fail, ''

    def get_pacman_last_update_date(self, contents):
        # contents: list of lines of pacman.log
        # Returns the datetime instance of last update date or None if last upda
        te date is not found
        for line in reversed(contents):
            if 'starting full system upgrade' in line:
                match_date = re.search('\[(.*?)\]', line)
                if match_date:
                    last_update_date_string = match_date.group(1)
                    return datetime.strptime(last_update_date_string, '%Y-%m-%d
                    %H:%M')

    def scan_debian(self):
        # Scans update-success-stamp file's creation date and checks whether it'
        s older than the last system update date
        # Returns a tuple: (ScanStatus, message)

```

```

config_update_interval_days = int(self.config['update']['warn_last_update_interval_days'])
last_update_date = self.get_apt_last_update_date('/var/lib/apt/periodic/update-success-stamp')
if last_update_date is None:
    return ScanStatus.unknown, ''
elif datetime.today() - last_update_date < timedelta(days=config_update_interval_days):
    return ScanStatus.success, ''
else:
    return ScanStatus.fail, ''

def get_apt_last_update_date(self, update_success_stamp_file_location):
    # update_success_stamp_file_location: usually `/var/lib/apt/periodic/update-success-stamp`
    # Returns the datetime instance of last update date or None if last update date is not found
    try:
        file_modification_epoch = os.path.getmtime(update_success_stamp_file_location)
    except FileNotFoundError:
        return None
    return datetime.fromtimestamp(file_modification_epoch)

def scan_redhat(self):
    # Not implemented, returns (ScanStatus.unknown, '')
    # Returns a tuple: (ScanStatus, message)
    return ScanStatus.unknown, ''

```

### Սկզբնական կոդ 11: test\_update.py

```

import os
import unittest
from datetime import datetime, timedelta
from tempfile import NamedTemporaryFile
from unittest.mock import patch, mock_open, MagicMock

from scan_status import ScanStatus
from update import Update

def raise_file_not_found_error():
    raise FileNotFoundError

class Test(unittest.TestCase):
    def test_get_pacman_last_update_date_when_not_found(self):
        # Prepare data and mocks
        file_contents_list = ['no such lines here']

```

```

# Run test scenario
last_update_date = Update(None).get_pacman_last_update_date(file_contents_list)

# Assertions
self.assertIsNone(last_update_date)

def test_get_pacman_last_update_date_when_found(self):
    # Prepare data and mocks
    file_contents_list = ['line1', '[2016-04-05 10:24] [PACMAN] starting full system upgrade', 'line3']

    # Run test scenario
    last_update_date = Update(None).get_pacman_last_update_date(file_contents_list)

    # Assertions
    self.assertEqual(last_update_date, datetime.strptime('2016-04-05 10:24', '%Y-%m-%d %H:%M'))

def test_scan_arch_when_is_older(self):
    # Prepare data and mocks
    with patch('builtins.open', mock_open()) as mock_file:
        config = {
            'update': {
                'warn_last_update_interval_days': '2'
            }
        }
        update = Update(config)
        update.get_pacman_last_update_date = MagicMock(return_value=datetime.today() - timedelta(days=10))

    # Run test scenario
    result = update.scan_arch()

    # Assertions
    self.assertEqual(result[0], ScanStatus.fail)
    mock_file.assert_called_once_with('/var/log/pacman.log')
    update.get_pacman_last_update_date.assert_called_once_with([])

def test_scan_arch_when_is_newer(self):
    # Prepare data and mocks
    with patch('builtins.open', mock_open()) as mock_file:
        config = {
            'update': {
                'warn_last_update_interval_days': '2'
            }
        }

```

```

    }
    update = Update(config)
    update.get_pacman_last_update_date = MagicMock(return_value=datetime
        e.today() - timedelta(days=1))

    # Run test scenario
    result = update.scan_arch()

    # Assertions
    self.assertEqual(result[0], ScanStatus.success)
    mock_file.assert_called_once_with('/var/log/pacman.log')
    update.get_pacman_last_update_date.assert_called_once_with([])

def test_scan_arch_when_last_update_date_not_found(self):
    # Prepare data and mocks
    with patch('builtins.open', mock_open()) as mock_file:
        config = {
            'update': {
                'warn_last_update_interval_days': '2'
            }
        }
        update = Update(config)
        update.get_pacman_last_update_date = MagicMock(return_value=None)

    # Run test scenario
    result = update.scan_arch()

    # Assertions
    self.assertEqual(result[0], ScanStatus.unknown)
    mock_file.assert_called_once_with('/var/log/pacman.log')
    update.get_pacman_last_update_date.assert_called_once_with([])

def test_scan_when_unknown(self):
    # Prepare data and mocks
    with patch('platform.linux_distribution', lambda: ('Unknown linux distri
        bution', None, None)):
        update = Update(None)

    # Run test scenario
    result = update.scan()

    # Assertions
    self.assertEqual(result[0], ScanStatus.unknown)

def test_scan_when_arch(self):
    # Prepare data and mocks
    with patch('platform.linux_distribution', lambda: ('arch', None, None)):
        update = Update(None)

```

```

        update.scan_arch = MagicMock(return_value=(ScanStatus.success, 'message'))

        # Run test scenario
        result = update.scan()

        # Assertions
        self.assertEqual(result, (ScanStatus.success, 'message'))
        update.scan_arch.assert_called_once_with()

def test_scan_when_debian(self):
    # Prepare data and mocks
    with patch('platform.linux_distribution', lambda: ('debian', None, None)):
        update = Update(None)
        update.scan_debian = MagicMock(return_value=(ScanStatus.success, 'message'))

        # Run test scenario
        result = update.scan()

        # Assertions
        self.assertEqual(result, (ScanStatus.success, 'message'))
        update.scan_debian.assert_called_once_with()

def test_scan_when_redhat(self):
    # Prepare data and mocks
    with patch('platform.linux_distribution', lambda: ('redhat', None, None)):
        update = Update(None)
        update.scan_redhat = MagicMock(return_value=(ScanStatus.unknown, 'message'))

        # Run test scenario
        result = update.scan()

        # Assertions
        self.assertEqual(result, (ScanStatus.unknown, 'message'))
        update.scan_redhat.assert_called_once_with()

def test_get_apt_last_update_date_when_file_does_not_exist(self):
    # Prepare data and mocks
    with patch('builtins.open', raise_file_not_found_error):
        update = Update(None)

        # Run test scenario
        result = update.get_apt_last_update_date('/tmp/this/file/does/not/exist')

```

```

        # Assertions
        self.assertIsNone(result)

def test_get_apt_last_update_date_when_file_exists(self):
    # Prepare data and mocks
    with patch('builtins.open', raise_file_not_found_error), NamedTemporaryFile() as temp_file:
        update = Update(None)
        seconds_epoch_in_1999 = 923398970
        os.utime(temp_file.name, (seconds_epoch_in_1999, seconds_epoch_in_1999))

    # Run test scenario
    result = update.get_apt_last_update_date(temp_file.name)

    # Assertions
    self.assertEqual(result.timestamp(), seconds_epoch_in_1999)

def test_scan_debian_when_is_older(self):
    # Prepare data and mocks
    config = {
        'update': {
            'warn_last_update_interval_days': '2'
        }
    }
    update = Update(config)
    update.get_apt_last_update_date = MagicMock(return_value=datetime.today() - timedelta(days=10))

    # Run test scenario
    result = update.scan_debian()

    # Assertions
    self.assertEqual(result[0], ScanStatus.fail)
    update.get_apt_last_update_date.assert_called_once_with('/var/lib/apt/periodic/update-success-stamp')

def test_scan_debian_when_is_newer(self):
    # Prepare data and mocks
    config = {
        'update': {
            'warn_last_update_interval_days': '2'
        }
    }
    update = Update(config)
    update.get_apt_last_update_date = MagicMock(return_value=datetime.today() - timedelta(days=1))

```



```

# Run test scenario
result = update.scan_debian()

# Assertions
self.assertEqual(result[0], ScanStatus.success)
update.get_apt_last_update_date.assert_called_once_with('/var/lib/apt/pe
riodic/update-success-stamp')

def test_scan_debian_when_last_update_date_not_found(self):
    # Prepare data and mocks
    config = {
        'update': {
            'warn_last_update_interval_days': '2'
        }
    }
    update = Update(config)
    update.get_apt_last_update_date = MagicMock(return_value=None)

    # Run test scenario
    result = update.scan_debian()

    # Assertions
    self.assertEqual(result[0], ScanStatus.unknown)
    update.get_apt_last_update_date.assert_called_once_with('/var/lib/apt/pe
riodic/update-success-stamp')

def test_scan_redhat(self):
    # Prepare data and mocks
    update = Update(None)

    # Run test scenario
    result = update.scan_redhat()

    # Assertions
    self.assertEqual(result[0], ScanStatus.unknown)

if __name__ == '__main__':
    unittest.main()

```

## Սկզբնական կոդ 12: worldwritable.py

```

import os
import stat

from base_scanner import BaseScanner
from scan_status import ScanStatus

```

```

class WorldWritable(BaseScanner):
    def __init__(self, config):
        # config is a dictionary of this program's configuration
        self.config = config

    def scan(self):
        # Scans the file system for world writable files and directories with pe
        # rmission anomalies
        worldwritable_files_starting_with_dot = self.scan_worldwritable_files_st
        arting_with_dot()
        worldwritable_directories_with_no_sticky_bit_set = self.scan_worldwritab
        le_directories_with_no_sticky_bit_set()
        worldwritable_files_owned_by_root = self.scan_worldwritable_files_owned_
        by_root()
        if not worldwritable_files_starting_with_dot and \
            not worldwritable_directories_with_no_sticky_bit_set and \
            not worldwritable_files_owned_by_root:
            scan_status = ScanStatus.success
            message = ''
        else:
            scan_status = ScanStatus.fail
            message_parts = []
            if worldwritable_files_starting_with_dot:
                message_parts.append(self.get_scan_text('World writable files st
                arting with dot',
                                                         worldwritable_files_star
                                                         ting_with_dot))
            if worldwritable_directories_with_no_sticky_bit_set:
                message_parts.append(self.get_scan_text('World writable director
                ies with no sticky bit set',
                                                         worldwritable_directorie
                                                         s_with_no_sticky_bit
                                                         _set))
            if worldwritable_files_owned_by_root:
                message_parts.append(self.get_scan_text('World writable files ow
                ned by root',
                                                         worldwritable_files_owne
                                                         d_by_root))
            message = '\n'.join(message_parts)
        return scan_status, message

    def get_scan_text(self, check_name, locations):
        # Generates a formatted string for given check's name and file locations
        if locations:
            return 'Failure: ' + check_name + ':\n\t' + '\n\t'.join(locations)
        else:
            return 'Success: ' + check_name

```

```

def scan_worldwritable_directories_with_no_sticky_bit_set(self):
    # Searches for worldwritable directories in the system which do not have
    # the sticky bit set
    # Returns a list of such directories
    result = []
    for directory, subdirectories, files in os.walk('/'):
        if self.is_world_writable(directory) and not self.is_sticky_bit_set(
            directory):
            result.append(directory)
    return result

def scan_worldwritable_files_starting_with_dot(self):
    # Searches for worldwritable files in the system whose name starts with
    # dot
    # Returns a list of such files
    result = []
    for directory, subdirectories, files in os.walk('/'):
        for file in files:
            if self.is_world_writable(file) and self.is_starts_with_dot(fil
                e):
                result.append(file)
    return result

def scan_worldwritable_files_owned_by_root(self):
    # Searches for worldwritable files in the system which are owned by root
    # Returns a list of such files
    result = []
    for directory, subdirectories, files in os.walk('/'):
        for file in files:
            if self.is_world_writable(file) and self.is_owned_by_root(file):
                result.append(file)
    return result

def is_world_writable(self, path):
    # Checks whether the file or directory at given path is world writable
    # Only the "Others" number in permission triple is checked for the prese
    # nce of "Writeable" bit
    # Returns true if is world writable, false otherwise
    # Returns false if the file is not found
    try:
        file_statistics = os.stat(path)
    except FileNotFoundError:
        return False
    return bool(file_statistics.st_mode & stat.S_IWOTH)

def is_sticky_bit_set(self, path):
    # Checks whether the file or directory at given path has sticky bit set

```

```

# Returns true if is set, false otherwise
# Returns false if the file is not found
try:
    file_statistics = os.stat(path)
except FileNotFoundError:
    return False
return bool(file_statistics.st_mode & stat.S_ISVTX)

def is_owned_by_root(self, path):
    # Checks whether the file or directory at given path is owned by the root user
    # A root user has UID of 0
    # Returns true if is owned by root, false otherwise
    # Returns false if the file is not found
    try:
        file_statistics = os.stat(path)
    except FileNotFoundError:
        return False
    return file_statistics.st_uid == 0

def is_starts_with_dot(self, path):
    # Checks whether name of the file or directory at given path starts with dot
    # Returns true if does, false otherwise
    # Returns false if the file is not found
    basename = os.path.basename(path)
    if not basename:
        return False
    return basename[0] == '.'

```

### Սկզբնական կոդ 13: test\_worldwritable.py

```

import os
import unittest
from unittest.mock import patch, MagicMock, call

from scan_status import ScanStatus
from worldwritable import WorldWritable

def raise_file_not_found_error(x):
    raise FileNotFoundError

class Test(unittest.TestCase):
    def test_scan_when_success(self):
        # Prepare data and mocks
        test_subject = WorldWritable(None)
        test_subject.scan_worldwritable_files_starting_with_dot = MagicMock(retu

```

```

        rn_value=[])
test_subject.scan_worldwritable_directories_with_no_sticky_bit_set = MagicMock(return_value=[])
test_subject.scan_worldwritable_files_owned_by_root = MagicMock(return_value=[])

# Run test scenario
result = test_subject.scan()

# Assertions
test_subject.scan_worldwritable_files_starting_with_dot.assert_called_once_with()
test_subject.scan_worldwritable_directories_with_no_sticky_bit_set.assert_called_once_with()
test_subject.scan_worldwritable_files_owned_by_root.assert_called_once_with()
self.assertEqual(result[0], ScanStatus.success)
self.assertEqual(result[1], '')

def test_scan_when_two_failures(self):
    # Prepare data and mocks
    test_subject = WorldWritable(None)
    test_subject.scan_worldwritable_files_starting_with_dot = MagicMock(return_value=[])
    test_subject.scan_worldwritable_directories_with_no_sticky_bit_set = MagicMock(return_value=['/some/failure'])
    test_subject.scan_worldwritable_files_owned_by_root = MagicMock(return_value=['/other/failure'])
    test_subject.get_scan_text = MagicMock(side_effect=['Test2 Failed', 'Test3 Failed'])

    # Run test scenario
    result = test_subject.scan()

    # Assertions
    test_subject.get_scan_text.assert_has_calls(
        [
            call('World writable directories with no sticky bit set', ['/some/failure']),
            call('World writable files owned by root', ['/other/failure']),
        ]
    )
    test_subject.scan_worldwritable_files_starting_with_dot.assert_called_once_with()
    test_subject.scan_worldwritable_directories_with_no_sticky_bit_set.assert_called_once_with()
    test_subject.scan_worldwritable_files_owned_by_root.assert_called_once_with()

```

```

self.assertEqual(result[0], ScanStatus.fail)
self.assertEqual(result[1], 'Test2 Failed\nTest3 Failed')

def test_get_scan_text_when_list_does_not_have_items(self):
    # Prepare data and mocks
    test_subject = WorldWritable(None)

    # Run test scenario
    result = test_subject.get_scan_text('Check name', [])

    # Assertions
    self.assertEqual(result, 'Success: Check name')

def test_get_scan_text_when_list_has_items(self):
    # Prepare data and mocks
    test_subject = WorldWritable(None)

    # Run test scenario
    result = test_subject.get_scan_text('Check name', ['file1', 'file2'])

    # Assertions
    self.assertEqual(result, 'Failure: Check name:\n\tfile1\n\tfile2')

@unittest.mock.patch('worldwritable.os')
def test_scan_worldwritable_directories_with_no_sticky_bit_set(self, mock_o
s):
    # Prepare data and mocks
    test_subject = WorldWritable(None)
    mock_os.walk.return_value = [
        ('/world/writable/not/sticky', (), ()),
        ('/not/world/writable/not/sticky', (), ()),
        ('/world/writable/sticky', (), ()),
    ]
    test_subject.is_world_writable = MagicMock(side_effect=[True, False, Tru
e])
    test_subject.is_sticky_bit_set = MagicMock(side_effect=[False, True])

    # Run test scenario
    result = test_subject.scan_worldwritable_directories_with_no_sticky_bit_
set()

    # Assertions
    self.assertEqual(result, ['/world/writable/not/sticky'])
    mock_os.walk.assert_called_once_with('/')
    test_subject.is_world_writable.assert_has_calls(
        [
            call('/world/writable/not/sticky'),
            call('/not/world/writable/not/sticky'),

```

```

        call('/world/writable/sticky'),
    ]
)
test_subject.is_sticky_bit_set.assert_has_calls(
    [
        call('/world/writable/not/sticky'),
        call('/world/writable/sticky'),
    ]
)

@unittest.mock.patch('worldwritable.os')
def test_scan_worldwritable_files_starting_with_dot(self, mock_os):
    # Prepare data and mocks
    test_subject = WorldWritable(None)
    mock_os.walk.return_value = [
        ('/dir1', ('/dir1/subdir1',), ('world_writable_starting_with_dot', '
        not_world_writable_starting_with_dot')),
        ('/dir2', (), ()),
        ('/dir3', ('/dir3/subdir3',), ('world_writable_not_starting_with_dot',)),
    ]
    test_subject.is_world_writable = MagicMock(side_effect=[True, False, True])
    test_subject.is_starts_with_dot = MagicMock(side_effect=[True, False])

    # Run test scenario
    result = test_subject.scan_worldwritable_files_starting_with_dot()

    # Assertions
    self.assertEqual(result, ['world_writable_starting_with_dot'])
    mock_os.walk.assert_called_once_with('/')
    test_subject.is_world_writable.assert_has_calls(
        [
            call('world_writable_starting_with_dot'),
            call('not_world_writable_starting_with_dot'),
            call('world_writable_not_starting_with_dot'),
        ]
    )
    test_subject.is_starts_with_dot.assert_has_calls(
        [
            call('world_writable_starting_with_dot'),
            call('world_writable_not_starting_with_dot'),
        ]
    )

@unittest.mock.patch('worldwritable.os')
def test_scan_worldwritable_files_owned_by_root(self, mock_os):
    # Prepare data and mocks

```

```

test_subject = WorldWritable(None)
mock_os.walk.return_value = [
    ('/dir1', ('/dir1/subdir1',), ('world_writable_owned_by_root', 'not_
        world_writable_owned_by_root')),
    ('/dir2', (), ()),
    ('/dir3', ('/dir3/subdir3',), ('world_writable_not_owned_by_root',))
]
test_subject.is_world_writable = MagicMock(side_effect=[True, False, True])
test_subject.is_owned_by_root = MagicMock(side_effect=[True, False])

# Run test scenario
result = test_subject.scan_worldwritable_files_owned_by_root()

# Assertions
self.assertEqual(result, ['world_writable_owned_by_root'])
mock_os.walk.assert_called_once_with('/')
test_subject.is_world_writable.assert_has_calls(
    [
        call('world_writable_owned_by_root'),
        call('not_world_writable_owned_by_root'),
        call('world_writable_not_owned_by_root'),
    ]
)
test_subject.is_owned_by_root.assert_has_calls(
    [
        call('world_writable_owned_by_root'),
        call('world_writable_not_owned_by_root'),
    ]
)

@unittest.mock.patch('worldwritable.os')
def test_is_world_writable_when_file_does_not_exist(self, mock_os):
    # Prepare data and mocks
    test_subject = WorldWritable(None)
    mock_os.stat.side_effect = raise_file_not_found_error
    path = '/does/not/actually/exist'

    # Run test scenario
    result = test_subject.is_world_writable(path)

    # Assertions
    self.assertFalse(result)
    mock_os.stat.assert_called_once_with(path)

@unittest.mock.patch('worldwritable.os')
def test_is_world_writable_when_is(self, mock_os):

```



```

# Prepare data and mocks
test_subject = WorldWritable(None)
mock_os.stat.return_value = os.stat_result((0o40002, 0, 0, 0, 0, 0, 0,
    0, 0, 0))
path = '/does/not/actually/exist'

# Run test scenario
result = test_subject.is_world_writable(path)

# Assertions
self.assertTrue(result)
mock_os.stat.assert_called_once_with(path)

@unittest.mock.patch('worldwritable.os')
def test_is_world_writable_when_is_not(self, mock_os):
    # Prepare data and mocks
    test_subject = WorldWritable(None)
    mock_os.stat.return_value = os.stat_result((0o40005, 0, 0, 0, 0, 0, 0,
        0, 0, 0))
    path = '/does/not/actually/exist'

    # Run test scenario
    result = test_subject.is_world_writable(path)

    # Assertions
    self.assertFalse(result)
    mock_os.stat.assert_called_once_with(path)

@unittest.mock.patch('worldwritable.os')
def test_is_sticky_bit_set_when_is_not_set(self, mock_os):
    # Prepare data and mocks
    test_subject = WorldWritable(None)
    mock_os.stat.return_value = os.stat_result((0o00000, 0, 0, 0, 0, 0, 0,
        0, 0, 0))
    path = '/does/not/actually/exist'

    # Run test scenario
    result = test_subject.is_sticky_bit_set(path)

    # Assertions
    self.assertFalse(result)
    mock_os.stat.assert_called_once_with(path)

@unittest.mock.patch('worldwritable.os')
def test_is_sticky_bit_set_when_is_set(self, mock_os):
    # Prepare data and mocks
    test_subject = WorldWritable(None)
    mock_os.stat.return_value = os.stat_result((0o01000, 0, 0, 0, 0, 0, 0,

```

```

        0, 0, 0))
    path = '/does/not/actually/exist'

    # Run test scenario
    result = test_subject.is_sticky_bit_set(path)

    # Assertions
    self.assertTrue(result)
    mock_os.stat.assert_called_once_with(path)

@unittest.mock.patch('worldwritable.os')
def test_is_sticky_bit_set_when_file_does_not_exist(self, mock_os):
    # Prepare data and mocks
    test_subject = WorldWritable(None)
    mock_os.stat.side_effect = raise_file_not_found_error
    path = '/does/not/actually/exist'

    # Run test scenario
    result = test_subject.is_sticky_bit_set(path)

    # Assertions
    self.assertFalse(result)
    mock_os.stat.assert_called_once_with(path)

@unittest.mock.patch('worldwritable.os')
def test_is_owned_by_root_when_is_not(self, mock_os):
    # Prepare data and mocks
    test_subject = WorldWritable(None)
    mock_os.stat.return_value = os.stat_result((0, 0, 0, 0, 1, 0, 0, 0, 0,
        0))
    path = '/does/not/actually/exist'

    # Run test scenario
    result = test_subject.is_owned_by_root(path)

    # Assertions
    self.assertFalse(result)
    mock_os.stat.assert_called_once_with(path)

@unittest.mock.patch('worldwritable.os')
def test_is_owned_by_root_when_is(self, mock_os):
    # Prepare data and mocks
    test_subject = WorldWritable(None)
    mock_os.stat.return_value = os.stat_result((0, 0, 0, 0, 0, 0, 0, 0, 0,
        0))
    path = '/does/not/actually/exist'

    # Run test scenario

```

```

    result = test_subject.is_owned_by_root(path)

    # Assertions
    self.assertTrue(result)
    mock_os.stat.assert_called_once_with(path)

@unittest.mock.patch('worldwritable.os')
def test_is_owned_by_root_when_file_does_not_exist(self, mock_os):
    # Prepare data and mocks
    test_subject = WorldWritable(None)
    mock_os.stat.side_effect = raise_file_not_found_error
    path = '/does/not/actually/exist'

    # Run test scenario
    result = test_subject.is_owned_by_root(path)

    # Assertions
    self.assertFalse(result)
    mock_os.stat.assert_called_once_with(path)

def test_is_starts_with_dot_when_does(self):
    # Prepare data and mocks
    test_subject = WorldWritable(None)
    path = '/starts/with/.dot'

    # Run test scenario
    result = test_subject.is_starts_with_dot(path)

    # Assertions
    self.assertTrue(result)

def test_is_starts_with_dot_when_does_not(self):
    # Prepare data and mocks
    test_subject = WorldWritable(None)
    path = '/does/not/start/with/dot'

    # Run test scenario
    result = test_subject.is_starts_with_dot(path)

    # Assertions
    self.assertFalse(result)

def test_is_starts_with_dot_when_empty_string(self):
    # Prepare data and mocks
    test_subject = WorldWritable(None)
    path = ''

    # Run test scenario

```

```

        result = test_subject.is_starts_with_dot(path)

    # Assertions
    self.assertFalse(result)

if __name__ == '__main__':
    unittest.main()

```

#### Սկզբնական կոդ 14: root.py

```

import os

from base_scanner import BaseScanner
from scan_status import ScanStatus

class Root(BaseScanner):
    def __init__(self, config):
        # config is a dictionary of this program's configuration
        self.config = config

    def scan(self):
        """
        Checks whether the user running this program is the root user with UID of 0.
        Takes into account the usage of the program sudo.
        :returns: a tuple of (ScanStatus, message).
        """
        if os.getuid() == 0:
            if os.environ.get('SUDO_UID'):
                return ScanStatus.success, ''
            else:
                return ScanStatus.fail, 'Do not use the root user account'
        else:
            return ScanStatus.success, ''

```

#### Սկզբնական կոդ 15: test\_root.py

```

import unittest
from unittest.mock import patch, MagicMock

from root import Root
from scan_status import ScanStatus

class Test(unittest.TestCase):
    @unittest.mock.patch('root.os')
    def test_scan_when_getuid_is_other(self, mock_os):
        # Prepare data and mocks

```

```

mock_os.getuid = MagicMock(return_value=1000)

# Run test scenario
result = Root(None).scan()

# Assertions
mock_os.getuid.assert_called_once_with()
self.assertEqual(result[0], ScanStatus.success)

@unittest.mock.patch('root.os')
def test_scan_when_getuid_is_0_and_environ_sudo_uid_is_set(self, mock_os):
    # Prepare data and mocks
    mock_os.getuid = MagicMock(return_value=0)
    mock_os.environ.get = MagicMock(return_value=1000)

    # Run test scenario
    result = Root(None).scan()

    # Assertions
    mock_os.getuid.assert_called_once_with()
    mock_os.environ.get.assert_called_once_with('SUDO_UID')
    self.assertEqual(result[0], ScanStatus.success)

@unittest.mock.patch('root.os')
def test_scan_when_getuid_is_0_and_environ_sudo_uid_is_not_set(self, mock_o
s):
    # Prepare data and mocks
    mock_os.getuid = MagicMock(return_value=0)
    mock_os.environ.get = MagicMock(return_value=None)

    # Run test scenario
    result = Root(None).scan()

    # Assertions
    mock_os.getuid.assert_called_once_with()
    mock_os.environ.get.assert_called_once_with('SUDO_UID')
    self.assertEqual(result[0], ScanStatus.fail)

if __name__ == '__main__':
    unittest.main()

```

### Սկզբնական կոդ 16: umask.py

```

import os
import stat

from base_scanner import BaseScanner
from scan_status import ScanStatus

```

```

class Umask(BaseScanner):
    def __init__(self, config):
        # config is a dictionary of this program's configuration
        self.config = config

    def scan(self):
        """
        Checks whether current user's umask value is secure.
        Only the last digit of the umask is checked (the Others digit).
        If the Others digit's write bit is set, the check fails.
        Otherwise the check succeeds.
        :returns: a tuple of (ScanStatus, message).
        """
        umask = self.get_umask_without_change()
        if umask & stat.S_IWOTH:
            return ScanStatus.success, ''
        else:
            return ScanStatus.fail, 'Current user\'s umask gives write permissions OTHERS group by default'

    def get_umask_without_change(self):
        """
        Gets current user's umask value without changing it.
        :returns: an integer of current user's umask.
        """
        current_umask = os.umask(0o0777)
        os.umask(current_umask)
        return current_umask

```

#### Սկզբնական կոդ 17: test\_umask.py

```

import unittest
from unittest.mock import patch, MagicMock, call

from scan_status import ScanStatus
from umask import Umask

class Test(unittest.TestCase):
    def test_scan_when_ok(self):
        # Prepare data and mocks
        umask = 0o0072
        test_subject = Umask(None)
        test_subject.get_umask_without_change = MagicMock(return_value=umask)

        # Run test scenario
        result = test_subject.scan()

```

```

    # Assertions
    test_subject.get_umask_without_change.assert_called_once_with()
    self.assertEqual(result[0], ScanStatus.success)

def test_scan_when_wrong(self):
    # Prepare data and mocks
    umask = 0o0025
    test_subject = Umask(None)
    test_subject.get_umask_without_change = MagicMock(return_value=umask)

    # Run test scenario
    result = test_subject.scan()

    # Assertions
    test_subject.get_umask_without_change.assert_called_once_with()
    self.assertEqual(result[0], ScanStatus.fail)

@unittest.mock.patch('umask.os')
def test_get_umask_without_change(self, mock_os):
    # Prepare data and mocks
    mock_os.umask = MagicMock(return_value=0o123)

    # Run test scenario
    result = Umask(None).get_umask_without_change()

    # Assertions
    mock_os.umask.assert_has_calls(
        [
            call(0o0777),
            call(0o123),
        ]
    )
    self.assertEqual(result, 0o123)

if __name__ == '__main__':
    unittest.main()

```

### Սկզբնական կոդ 18: ssh.py

```

import os
import stat
import re

from base_scanner import BaseScanner
from scan_status import ScanStatus

```

```

class Ssh(BaseScanner):
    def __init__(self, config):
        # config is a dictionary of this program's configuration
        self.config = config

    def scan(self):
        """
        Checks whether the system SSHd daemon configuration file is secure or not.
        :returns: a tuple of (ScanStatus, message).
        """
        if self.check_protocol('/etc/ssh/ssh_config'):
            return ScanStatus.success, ''
        else:
            return ScanStatus.fail, 'The vulnerable SSHv1 is enabled in /etc/ssh/ssh_config'

    def check_protocol(self, sshd_config_path):
        """
        Checks SSHd service's configuration file – whether the vulnerable v1 protocol is enabled.
        :param sshd_config_path: the SSHd service's configuration file location, usually /etc/ssh/ssh_config.
        :returns: True if no protocol is selected or the default protocol 2 is selected.
        :returns: False if protocol 1 is selected or is selected as fallback.
        """
        is_comment_line = re.compile('^\\s*#')
        with open(sshd_config_path) as config_file:
            for line in config_file.readlines():
                if not is_comment_line.match(line):
                    if line.split() and line.split()[0] == 'Protocol' and '1' in ''.join(line.split()[1:]):
                        return False
            return True

```

#### Սկզբնական կոդ 19: test\_ssh.py

```

import unittest
from unittest.mock import patch, mock_open, MagicMock

from scan_status import ScanStatus
from ssh import Ssh

class Test(unittest.TestCase):
    def test_scan_when_ok(self):
        # Prepare data and mocks
        test_subject = Ssh(None)

```



```

test_subject.check_protocol = MagicMock(return_value=True)

# Run test scenario
result = test_subject.scan()

# Assertions
test_subject.check_protocol.assert_called_once_with('/etc/ssh/ssh_config')
self.assertEqual(result[0], ScanStatus.success)

def test_scan_when_failed(self):
    # Prepare data and mocks
    test_subject = Ssh(None)
    test_subject.check_protocol = MagicMock(return_value=False)

    # Run test scenario
    result = test_subject.scan()

    # Assertions
    test_subject.check_protocol.assert_called_once_with('/etc/ssh/ssh_config')
    self.assertEqual(result[0], ScanStatus.fail)

def test_check_protocol_when_ok_no_protocol(self):
    # Prepare data and mocks
    with patch('builtins.open', mock_open(read_data='# $OpenBSD: s\n\n# Host *\nSomeConfig')) as mock_file:
        test_subject = Ssh(None)

        # Run test scenario
        result = test_subject.check_protocol('/etc/ssh/ssh_config')

        # Assertions
        mock_file.assert_called_once_with('/etc/ssh/ssh_config')
        self.assertTrue(result)

def test_check_protocol_when_ok_protocol_commented(self):
    # Prepare data and mocks
    with patch('builtins.open',
                mock_open(read_data='# $OpenBSD: s\n\n# Host *\nSomeConfig\n# Protocol 1')) as mock_file:
        test_subject = Ssh(None)

        # Run test scenario
        result = test_subject.check_protocol('/etc/ssh/ssh_config')

        # Assertions
        mock_file.assert_called_once_with('/etc/ssh/ssh_config')

```

```

        self.assertTrue(result)

def test_check_protocol_when_ok(self):
    # Prepare data and mocks
    with patch('builtins.open',
                mock_open(read_data='#    $OpenBSD: s\n\n# Host *\nSomeConfig\n\n Protocol 2')) as mock_file:
        test_subject = Ssh(None)

    # Run test scenario
    result = test_subject.check_protocol('/etc/ssh/ssh_config')

    # Assertions
    mock_file.assert_called_once_with('/etc/ssh/ssh_config')
    self.assertTrue(result)

def test_check_protocol_when_fail(self):
    # Prepare data and mocks
    with patch('builtins.open',
                mock_open(read_data='#    $OpenBSD: s\n\n# Host *\nSomeConfig\n\n Protocol 1')) as mock_file:
        test_subject = Ssh(None)

    # Run test scenario
    result = test_subject.check_protocol('/etc/ssh/ssh_config')

    # Assertions
    mock_file.assert_called_once_with('/etc/ssh/ssh_config')
    self.assertFalse(result)

def test_check_protocol_when_fail_fallback(self):
    # Prepare data and mocks
    with patch('builtins.open',
                mock_open(read_data='#    $OpenBSD: s\n\n# Host *\nSomeConfig\n\n Protocol 2, 1')) as mock_file:
        test_subject = Ssh(None)

    # Run test scenario
    result = test_subject.check_protocol('/etc/ssh/ssh_config')

    # Assertions
    mock_file.assert_called_once_with('/etc/ssh/ssh_config')
    self.assertFalse(result)

if __name__ == '__main__':
    unittest.main()

```

# Իրականացման աշխատանքը

## Նկար 1: Իրականացման աշխատանքի օրինակ

```
Running: Update
Finished: Update
Status: ScanStatus.fail
Message:

-----
Running: OpenPorts
Finished: OpenPorts
Status: ScanStatus.success
Message:
Type, IP, Port, PID, Username, Command line
tcp 127.0.0.1:63342 20837 babken /opt/pycharm-community/bin/./jre/jre/bin/java -Xbootclasspath/a:/op
-----
Running: WorldWritable
Finished: WorldWritable
Status: ScanStatus.fail
Message:
Failure: World writable directories with no sticky bit set:
/home/babken/Quake 2
/home/babken/Quake 2/docs
/home/babken/Quake 2/docs/quake2_manual
/home/babken/Quake 2/docs/quake2_manual/images
/home/babken/Quake 2/Q2
/home/babken/Quake 2/Q2/docs
/home/babken/Quake 2/Q2/docs/quake2_manual
/home/babken/Quake 2/Q2/docs/quake2_manual/images
/home/babken/Quake 2/Q2/ROGUE
/home/babken/Quake 2/Q2/baseq2
/home/babken/Quake 2/Q2/baseq2/video
/home/babken/Quake 2/Q2/baseq2/maps
```