ОӘЖ 004.056

АНДРОИД ҚҰРЫЛҒЫЛАРЫ НЕГІЗІНДЕ ЖАСАЛҒАН КОМПЬЮТЕРЛІК ЖЕЛІЛЕР МЕН ҚОЛДАНБАЛАРДЫҢ ҚАУІПСІЗДІГІН ТАЛДАУҒА АРНАЛҒАН КӨППРОФИЛЬДІ АППАРАТ

Момбай Нұржігіт Қанатұлы
Nurik.nn98@gmail.com
Л.Н.Гумилев атындағы Еуразия ұлттық университеті, Ақпараттық технологиялар факультеті, ақпараттық қауіпсіздік кафедрасы, «Ақпараттық қауіпсіздік әдістері мен технологиялары» мамандығы, Магистрант 2-курс.
Ғылыми жетекші – Оспанова А.Б.

Аңдатпа. Қазіргі таңда, ақпараттық қауіпсіздік саласының өте өзекті болуының салдарынан, желідегі осалдықтарды тексеру, құпиясөздердің беріктігін тексеру, сонымен қатар сымсыз желілердің осалдықтарын анықтау секілді іс-әрекеттерді жүргізу маңызды болып табылады. Осындай тапсырмаларды шешу үшін көбінесе габаритті емес мобильді жабдықты қолдану дұрыс шешімдердің бірі болып табылады. Сол себепті, бұл мақалада мәселені шешудің бір жолы ретінде Kali Linux Nethunter-ді қалай орнату керек екендігі қарастырылған. Сонымен қатар, онымен қалай жұмыс жасау қажет екені жайында ақпараттар келтірілген.

Түйін сөздер: ақпараттық қауіпсіздік, желілік қауіпсіздік, операциялық жүйе, дистрибутив, рұқсатсыз қатынау, порт, протокол, осалдықтар, сканерлеу.

I. Кіріспе

Соңғы жылдары компьютерлік қосымшаларға қарағанда мобильді құрылғыларға арналған қосымшалар үлесінің қарқынды өсу үрдісі байқалады. Екінші жағынан, компьютерлік желінің қауіпсіздік міндеттеріне компьютерлік желілерді және сымсыз желілерді тестілеу, парольдердің беріктігін тексеру, дербес компьютерді қорғау жүйелері секілді тапсырмалар кіреді. Осындай тапсырмаларды шешу үшін көбінесе габаритті емес мобильді жабдықты қолданған жөн.

Kali Linux - Linux ядросындағы операциялық жүйе (дистрибутив). Kali операциялық жүйесі рұқсатсыз енуге және қауіпсіздік аудитін озық тестілеу үшін құрылған. Kali рұқсатсыз қатынауды тестілеу (Penetration Testing), Ақпараттық қауіпсіздік саласындағы зерттеулер (Security research), компьютерлік криминалистика (Computer Forensics) және кері инженерия (Reverse Engineering) сияқты ақпараттық қауіпсіздіктің түрлі міндеттеріне бағытталған бірнеше жүздеген (600-ден астам) құралдардан тұрады. Kali Linux-ті ақпараттық қауіпсіздікті ұйымдастыру саласындағы көшбасшы компания Offensive Security әзірлейді, қаржыландырады және қолдайды[1].

Nethunter – Android смартфондары үшін оңтайландырылған Kali дистрибутивінің нұсқасы. Онда кейбір опцияларды басқару үшін графикалық софт енгізілген, сонымен қатар шабуылдар мен жұмыстарға арналған Android-қосымшалар жиынтығы бар (DriveDroid, Hacker's Keyboard және т.б.). Жалпы стандартты құралдардан: Aircrack, BTCrack, Btscanner, Metasploit, Kismet, Bluebugger, Nmap және басқалары бар[2].

Дистрибутивті Nexus типті девайстарына және басқа да смартфондармен планшеттерге орнатуға болады. Олардың тізімі келесідей: Samsung Galaxy, LG, HTC, Sony Xperia және т.б. Төмендегі кестеде құрылғылар және қажетті Android операциялық жүйесінің нұсқасы жайында толық ақпарат көрсетілген. Бұл тізімдегі құрылғыларға Kali Linux Nethunter-дің ресми нұсқасын орнату мүмкіндігі бар[3].

Кесте 1 Nethunter-ді ресми түрде қолдайтын құрылғылар мен ОЖ түрлері

Құрылғы атауы	**Android ОЖ-ның нұсқасы**
Nexus 9 (flounder)	5.1.1 немесе 6.0.1
Nexus 10 (manta)	5.1.1
OnePlus One (oneplus1)	CM 12.1 немесе 13.0
OnePlus 2 (oneplus2)	CM 12.1 - 16.0
Galaxy S7 (herolte)	TouchWiz 6.0.1
Galaxy S7 edge (hero2lte)	TouchWiz 6.0.1
LG V20 T-Mobile (h918)	7.0.0
HTC One M7 GPE (onem7gpe)	5.1.1
Sony Xperia ZR (dogo)	6.0.1
Ескертпе – [4] әдебиет көзінен алынған	

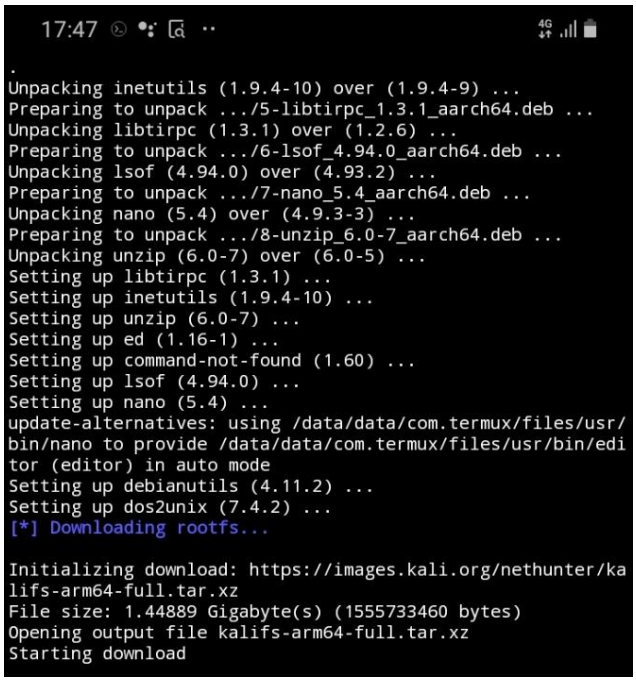
Жоғарыдағы кестеден Kali Linux Nethunter-дің ресми нұсқасын бірнеше құрылғылар типтеріне орнатуға болатынын көреміз. Эксперттер Kali дистрибутивін осы тізімдегі CM 12.1 немесе 13.0 ОЖ-ға орнатылған OnePlus One (oneplus1) құрылғысына қондыруды ұсынады.

Мақалада Kali Linux Nethunter-ді рут-құқықтарын қолданбай Андроид құрылғыларына ешқандай зақымсыз орнату нұсқаулығы көрсетілген. Kali Linux Nethunter-ді практика жүзінде іске асыру бойынша мысалдар келтірілген. Дистрибутив Samsung Galaxy құрылғысына орнатылған. Сонымен қатар ОЖ нұсқасы – Android 9.

I. Kali Linux Nethunter-ді рут-құқықтарын қолданбай Андроид құрылғыларына ешқандай зақымсыз орнату нұсқаулығы

Жұмысты бастамас бұрын ең алдымен, NetHunter-Store бағдарламасын құрылғымызға орнатып аламыз. NetHunter-Store-дан Termux, NetHunter-KeX client және

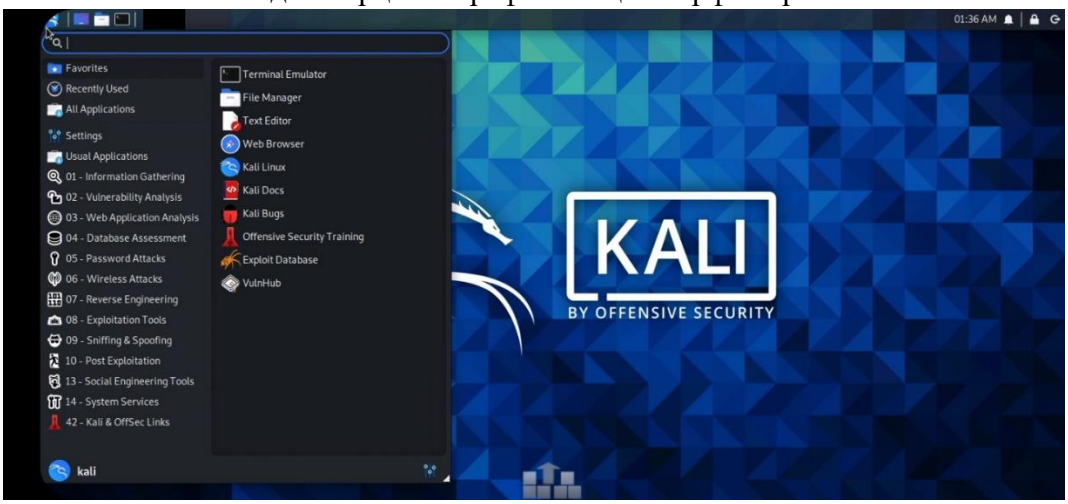
Hacker's keyboard-ты жүктеп аламыз. Келесі ретте *wget* қосымшасын орнатамыз: *pkg install wget.* Содан соң, *wget* көмегімен керек файлдарды жүйеге көшіреміз: *wget -O install-nethunter-termux https://offs.ec/2MceZWr* [5].



Сурет 1. Kali Linux Nethunter-ді құрылғыға орнату барысы

Сонымен қатар ыңғайлы жұмыс жасау үшін *nethunter kex* командасы арқылы дистрибутивтің графикалық интерфейсіне көшуге болады.

Төмендегі бейнеден дистрибутивтің графикалық нұсқасы жүйеге енгізілгенін байқай аламыз. *nethunter kex* командасы арқылы графикалық интерфейс режиміне өтеміз.



Сурет 2. Kali Linux Nethunter-дің графикалық интерфейсі

Бұл жерде Kali Linux-тегідей бірнеше утилиталармен жұмыс істеуге қол жеткізуге болады. Утилиталарды қолданып жүйенің осылдықтарына бағытталған, пентестингке бағытталған іс-әрекеттерді жүзеге асыра аламыз.

Келесі бейнеден Hacker's keyboard қосымшасының құрылғымызға сәтті орнатылғанын байқаймыз. Бұл қосымша жұмысты біршама жеңілдетеді. Стационарлы компьютер немесе ноутбукты қолданғандай жұмыс атқаруға мүмкіндік береді.

Сурет 3. Hacker's keyboard қосымшасының сәтті орнатылуы (бартырмалар)

Осылайша Kali Linux Nethunter-ді құрылғыға орнату сәтті аяқталды. Келесі бөлімде мобильді хакерлік құрылғымен қалай жұмыс жасау керектігі жөнінде мысал келтірілетін болады.

II. Kali Linux Nethunter-ді практика жүзінде іске асыру

Мысал ретінде Kali Linux-тегі қарапайым, әрі өнімділігі өте жоғары саналатын nmap утилитасы арқылы мысалдар көрсетіп өтсем. Nmap-бұл қауіпсіздік күйін сканерлеу немесе желідегі серверлерді анықтау сияқты әртүрлі мақсаттарда қолдануға бағытталған өте қуатты құрал.

Тест үшін мен пәрменді қолданамын

$ nmap -A -v <IP>

-A параметрі ОЖ-ні сканерлеуді, оның нұсқасын, сценарийлерді сканерлеуді, сондай-ақ маршрутты бақылауды (traceroute) қосуға жауап береді. -V параметрі қосымша ақпаратты көрсетеді.

Сканерлеу нәтижелерінің шығуын төмендегі скриншоттан көре аласыз.

```
┌──(kali㉿localhost)-[~]
└─$ nmap -A scanme.nmap.org
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-23 13:41
 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.25s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c0
1::f03c:91ff:fe18:bb2f
Not shown: 986 closed ports
PORT      STATE    SERVICE      VERSION
22/tcp    open     ssh          OpenSSH 6.6.1p1 Ubuntu 2ubu
ntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (D
SA)
|   2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (R
SA)
|   256 96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (EC
DSA)
|_  256 33:fa:91:0f:e0:e1:7b:1f:6d:05:a2:b0:f1:54:41:56 (ED
25519)
80/tcp    open     http         Apache httpd 2.4.7 ((Ubuntu
))
|_http-favicon: Nmap Project
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Go ahead and ScanMe!
1026/tcp  filtered LSA-or-nterm
1027/tcp  filtered IIS
1028/tcp  filtered unknown
1029/tcp  filtered ms-lsa
1030/tcp  filtered iad1
1031/tcp  filtered iad2
1032/tcp  filtered iad3
1033/tcp  filtered netinfo
1034/tcp  filtered zincite-a
1035/tcp  filtered multidropper
9929/tcp  open     nping-echo   Nping echo
31337/tcp open     tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect re
sults at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 31.91 second
```

Сурет 4. Орындаулардың нәтижесі

Nmap-бұл ең алдымен порт сканері. Жүйедегі әрбір желілік сервис 1-ден 65535-ке дейінгі диапазондағы желілік порттарды "тыңдайды". Мысалы, SSH (Secure Shell) қызметі 22 портын тыңдайды, ал Веб-Сервердің HTTP қызметі (Hypertext Transfer Protocol) 80 портын тыңдайды. Nmap сияқты порт сканері жұмыс істейтін желілік қызметтерді анықтау үшін IP мекен-жайы бойынша порттармен байланыс орнатуға тырысады.

Мысалдан жүйеде іске асырылған порттарды көре аламыз. Және олардың ашық тұрғанын байқаймыз. Сонымен қатар, жоғарыдағы суреттен жүйедегі жұмыс жасап тұрған сервистің бар екенін көруге болады. Http протоколы бойынша 80-ші порт арқылы Apache 2.4.7 нұсқасындағы және Ubuntu ОЖ орнатылған сервердің жұмыс атқарып тұрғанын көре аламыз. Бұл ақпарат шабуылдаушы үшін өте маңызды болып табылады. Осы сервистің ақауларын және осалдықтарын пайдаланып, жүйеге үлкен қауіп төндіруі мүмкін. Сол себепті жүйедегі мұндай осалдықтарды жойып, оны сырт көзден жасыру өте маңызды іс-әрекеттердің бірі болып табылады.

III. Қорытынды

Қорытындылай келе, сымсыз желідегі осалдықтарды тексеру және жүйелердің осал тұстарын анықтау секілді ақпараттық қауіпсіздікті қамтамасыз ету іс-шараларын жүзеге асыру барысында, габаритті емес мобильді жабдықты қолданған дұрыс шешімдердің бірі болып табылатынына көз жеткіздік. Ал осы іс-әрекеттерді жүзеге асыруға мобильді құрылғыға орнатылған Kali Linux Nethunter дистрибутиві толықтай мүмкіндік береді.

Бұл зерттеу жұмысында Kali Linux Nethunter-ді қалай орнату керек екені қарастырылған. Сонымен қатар, бірнеше құрылғылар және оларға орнатылған ОЖ-лардың мүмкіндіктері жайында салыстырмалы анализдер келтірілген. Олардың тізімінде Nexus, HTC, Samsung Galaxy, Sony Xperia, LG секілді девайстар бар. Дистрибутив Samsung Galaxy құрылғысына сәтті орнатылып, орнату барысы жайында нұсқаулық көрсетілген. Мобильді құрылғыға Nethunter-дің графикалық интерфейсін орнатып, Hacker's keyboard қосымшасының көмегімен ыңғайлы жұмыс атқаруға болатыны көрсетілген.

Сонымен қатар, Nethunter орнатылған мобильді құрылғымен, желілерді сканерлеу барысында nmap утилитасы сәтті тестілеуден өтті. Желідегі ашық порттар мен жұмыс атқарып тұрған сервистер туралы ақпарат ала алдық. Бұл ақпараттардың көмегімен шабуылдаушылардың жүйеге ену мүмкіндігі жоғарылайды. Сондықтанда бұл мәселе АҚ мамандары үшін өте өзекті.

Алайда, мақалада бұл мобильді хакерлік құрылғының мүмкіндіктері толықтай дерлік көрсетілмеген. Себебі, бұл құрылғыда Kali Linux-тың барлық утилиталарын орнатып жүзеге асыруға болады. Толығырақ мысалдармен ақпараттар келесі зерттеу жұмысында жүргізілетін болады.

Пайдаланылған әдебиеттер тізімі

1. Johansen G. et al. Kali Linux 2–Assuring Security by Penetration Testing. – Packt Publishing Ltd, 2016.
2. Rahmadani M. A., Rizal M. F., Gunamawan T. Implementasi Hacking Wireless Dengan Kali Linux Menggunakan Kali Nethunter //eProceedings of Applied Science. – 2017. – Т. 3. – №. 3.
3. Parasram S. V. N. et al. Kali Linux 2018: Assuring Security by Penetration Testing: Unleash the full potential of Kali Linux 2018, now with updated tools. – Packt Publishing Ltd, 2018.
4. https://github.com/offensive-security/kali-nethunter/wiki
5. https://www.kali.org/docs/nethunter/nethunter-rootless/
6. Ansari J. A. Web Penetration Testing with Kali Linux. – Packt Publishing Ltd, 2015.
7. Фленов, М.Е. Linux глазами хакера / М.Е. Фленов. - М.: БХВ-Петербург, 2008. - 544 с.