ХАКЕРЫ

Привет друзья, мы хотим вам немного рассказать о хакерах и безопасности в интернете. Раньше хакером называли высокопрофессионального компьютерного специалиста, который необычным, нестандартным образом решал компьютерные проблемы.

Существует два основных определения:

Бе́лые ха́керы, на сетевом сленге *White hat* (англ.) — специалисты по компьютерной безопасности, который специализируется на тестировании безопасности компьютерных систем. белые хакеры ищут уязвимости на добровольной основе или за плату с целью помочь разработчикам сделать их продукт более защищенным.

Черные хакеры, на сетевом сленге Black hat (англ.**)** это специалисты, которые выявляют слабые места в компьютерных системах и используют их для получения своей выгоды, во вред взломанной компьютерной системе

Чем пользуются хакеры? Что они изучают чтобы взламывать наши компьютеры? Рекомендуем Вам тоже изучить вкратце эти технологии, чтобы вы могли обезопасить себя от взлома.

1. Умение программировать, хотя бы на одном популярном языке программирования.

2. знания компьютерных сетей IPv4, IPv6, DHCP, NAT, подсети, DNS, роутеры и коммутаторы, VLAN, сетевая модель OSI, публичный и локальный IP, MAC адреса, ARP.

3. Linux и Wireshark

Хакеры любят Linux OS. Можно даже сказать, что Linux – самая популярная ОС среди хакеров. Существующие на Linux инструменты для взлома разрабатывались специально для хакеров.

4. Виртуализация

Суть виртуализации для хакера в том, чтобы тестировать свои идеи с помощью виртуальной версии.

5. Беспроводные технологии

Чаще всего взламывают сети Wi-Fi. Чтобы знать как хакеры атакуют беспроводные сети или электронные устройства, нужно знать все их функции. Для этого следует изучить профессиональные алгоритмы шифрования WPA, WEP, WPA2, WPS и handshake.

6. Базы данных и веб-приложения

Благодаря СУБД можно получить доступ или взломать базы данных. Базы данных представляют собой набор данных, хранящихся на компьютере, доступ к которым можно получить разными способами.

А это программы для linux, которыми пользуются хакеры:

1. nmap — Сканер nmap как главный инструмент кино-хакеров.
Данная программа мелькает почти во всех фильмах про хакеров, например: **Matrix Reloaded/матрица:перезагрузка**, **Snowden/Сноуден**, **Dredd/судья дредд**, **Elysium/элизиум-рай не на земле**, **Fantastic Four / Фантастическая четверка**, **Who Am I/ Кто я**, **Bourne Ultimatum / Ультиматум Борна, Die Hard 4 / Крепкий орешек 4, The Girl with the Dragon Tattoo / Девушка с татуировкой дракона, Retaliation 2 /Бросок кобры 2, Abduction / Погоня**
Используется для интернет-разведки: определение оборудования, ОС, структуры сети. Позволяет выявлять открытые порты на удаленных компьютерах и определять названия сервисов и номера версий. Системным администратором может использоваться для выявления сетевых неполадок.

2. **dsniff** — вытаскивает логины и пароли
Хорошо известный многим сниффер. Отличается простотой: запустил и получай себе пароли, которые вводят на сайтах другие члены локальной сети.

3. **httpry** — перехватывает введенные на сайтах пароли
Еще один сниффер, но со специализацией только на HTTP-трафике. Собирает адреса посещенных страницы, логины и пароли.

4. **iptraf** — кто сколько насидел в интернете Учет сетевого трафика.
Программа обязательна для тех пользователей, которые выходят в сеть через мобильные сети с помегабайтной тарификацией. iptraf показывает объемы входящего и исходящего трафика, а также среднюю скорость соединения.

5. **mysql-sniffer** — перехватывает запросы к MySQL и ответы
Незаменимый инструмент для web-разработчика. Программа фиксирует все обращения к локальному серверу MySQL.

6. **ngrep** — поиск в сетевом потоке
Как grep, только для сетевого трафика. Можно, проверять, куда утекают ваши персональные данные

7. **p0f** — детектор операционных систем
Позволяет пассивно определять тип оборудования и установленные операционные системы на машинах. Атакующий не выдаст себя и факт разведки не попадет в журналы.

8. **snort** — система обнаружения вторжений
Система обнаружения сетевых вторжений. Выявит и детально запротоколирует все сетевые атаки на ваш рабочий компьютер или сервер. Кто атаковал, когда, откуда, какие порты, с каким результатом и т.д.

9. **tcpdump** — захват сетевого трафика
Записывает весь трафик в универсальном формате PCAP для дальнейшего изучения. Например, можно записать трафик публичной сети Wi-Fi и дома изучить записанное с помощью Wireshark.

10. **iftop** — производительность сетевой подсистемы
Мониторинг производительности сетевой подсистемы. Тормозит интернет? Проверьте для начала iftop — может банально не тянет сетевой адаптер.

11. **netstat** — что происходит? Показывает открытые сетевые порты и подключившихся к ним клиентов. Периодически полезно запускать на серверах для проверки, не протроянили ли компьютер.

12. **netcat** — универсальный сетевой инструмент
Наикрутейшая программа, позволяющая открывать сокеты и привязывать их к командной строке. Например, можно связать bash с одним из портов и получить простейшее средство удаленного администрирования.

13. **dhcpdump** — получение данных о локальной сети
Программа предоставляет информацию о широковещательных пакетах от DHCP-сервера, работающего в вашей локальной сети. На основе собранных данных можно легко выяснить адрес шлюза, DNS-сервера и иную информацию еще до подключения.

Некоторые хакеры работают в одиночку. Это касается как тех, кто взламывает системы и занимается кражей информации, так и тех, кто самостоятельно пишет зловредные программы. Группировка хакеров уделяют много внимания написанию вирусов или их модернизации. За последние несколько лет число группировок увеличилось, так же как количество взломов и краж.

Кто может стать жертвой хакера? - Ответ - любой из нас! Любой компьютер имеющий выход в интернет - может стать уязвимым. Думать что ваш стареньких домашний компьютер никому не интересен - не правильно. Всегда помните о безопасности в сети:

-Не выкладывайте свои паспортные данные в сети
-Не выкладывайте данные своих банковских карт
-Ставьте сложные пароли на свои телефоны, компьютеры и аккаунты в соц сетях
-Свои личные и важные файлы которые вы храните на компьютере - храните в запароленных zip архивах
-Помните что чем сложнее и длиннее ваш пароль - тем сложнее будет его взломать

На наших занятиях - мы научим вас как можно обезопасить ваши проекты и сервера.
Удачи друзья и всегда помните о безопасности в интернете!

----------ქართული----------

ჰაკერები

მოგესალმებით, ძვირფასო მეგობრებო! გვინდა მოგიყვეთ ჰაკერების და ინტერნეტში დაცვის შესახებ. ადრე ჰაკერებს ეძახდნენ მაღალკვალიფიცირებულ კომპიუტერულ სპეციალისტს, რომელიც უჩვეულო, არასტანდარტული მეთოდით შეეძლო კომპიუტერული პრობლებების აღმოფხვრა.

არსებობს ორი ძირითადი განმარტება:

თეთრი ჰაკერები, ქსელურ სლენგზე *White hat* (ინგ.) - კომპიუტერული უსაბრთხოების სპეციალისტები, რომელებიც სპეციალიზირებულნი არიან კომპიუტერული სისტემების უსაფრთხოების დატესტვაზე. თეთრი ჰაკერები ეძებენ სუსტ წერტილებს კეთილი ნების საფუძველზე ან ფულადი ჯილდოსთვის, დეველოპერებს ეხმარებიან მათი პროდუქციის უსაფრთხოების დაცვის მიზნით.

შავი ჰაკერები, ქსელურ სლენგზე Black hat (ინგ.**)** - სპეციალისტები, რომლებიც შოულობენ სუსტ წერტილებს კომპიუტერულ სისტემებში და მისი ბიანის მიყენების საფუძველზე შოულიბენ თავიანთ მოგებას.

რას ხმარობენ ჰაკერები? რას იყენებენ იმისთვის, რომ გატეხონ ჩვენი კომპიუტერები? თქვენც გირჩევთ მოკლედ შეისწავლოთ ეს ტექნოლოგიები, იმისთვის, რომ შეძლოთ დაიცვათ თავი გატეხვისგან.

1. პროგრამირების ცოდნა, ერთ პოპულარულ დაპროგრამების ენაზე მაინც.

2. კომპიუტერული ქსელების ცოდნა IPv4, IPv6, DHCP, NAT, ქვექსელი, DNS, როუტერები და კომუტატორები, VLAN, OSI ქსელური მოდელი, საჯარო და ლოკალური IP, MAC მისამართები, ARP.

3. Linux и Wireshark
ჰაკერებს უყვართ Linux OS. შეიძლება ვთქვათ, რომ Linux - ყველაზე პოპულარული ოპერაციული სისტემაა ჰაკერებს შორის.

4. ვირტუალიზაცია
ვირტუალიზაციის არსი ჰაკერებისთვის არის მათი იდეების ტესტირება ვირტუალური ვერსიის დახმარებით.

5. უსადენო ტექნოლოგიები
ყველაზე ხშირად ტეხავენ Wi-Fi. იმისთვის, რომ გავიგოთ როგორ უტევენ ჰაკერები უსადენო ქსელებს ან ელექტრონულ მოწყობილობებს, საჭიროა ვიცოდეთ მათი ყველა ფუნქციები. ამისათვის უნდა შევისწავლოთ პროფესიონალური დაშიფრვის ალგორითმები WPA, WEP, WPA2, WPS და handshake.

6. მონაცემთა ბაზები და ვებ-აპლიკაციები.

მონაცემთა ბაზების მართვის სისტემის წყალობით შეიძლება მივიღოთ წვდომა ან გავტეხოთ მონაცემთა ბაზები. მონაცემთა ბაზები შეიცავენ მოაცემების კრებულს, რომელიც ინახება კომპიუტერზე, რომელთანაც წვდომა შეიძლება მივიღოთ სხვადასხვა გზებით.

ეს კი linux-ის პროგრამებია, რომლებსაც იყენებენ ჰაკერები:

1. **nmap** სკანერი — ეს არის კინო-ჰაკერების მთავაარი ინსტრუმენტი

ეს პროგრამა გვხვდება თითქმის ყველა ფილმში სადაც არიან ჰაკერები, მაგალითად: **Matrix Reloaded/მატრიცა: გადატვირთვა**, **Snowden/სნოუდენი**, **Dredd/მოსამართლე დრედი**, **Elysium/ელიზიუმი**, **Fantastic Four / ფანტასტიური ოთხეული**, **Who Am I/ ვინ ვარ მე**, **Bourne Ultimatum / ბორნის ულტიმატუმი, Die Hard 4 / კერკეტი კაკალი 4, The Girl with the Dragon Tattoo / გოგონა დრაკონის ტატუთი, Retaliation 2 /G.I. Joe: შურისძიება, Abduction / დევნა**

გამოიყენება ინტერნეტ დაზვერვისთვის: მოწყობილობების, ოპერაციული სისტემის, ქსელის სტრუქტურის ამოცნობისთვის. გვაძლევს საშუალებას დაშორებულ კომპიუტერზე ამოვიცნოთ ღია პორტები და გვაძლევს საშუალებას ამოვიცნოთ სერვისის სახელი და ვერსიის ნომერი. სისტემური ადმინისტრატორისგან შეიძლება გამოყენეგული იყოს, როგორც ქსელური გაუმართაობის მაძიებლი.

2. **dsniff** — მოაქვს ლოგინი და პაროლი

ყველასთვის კარგად ცნობილი სნიფერი. განსხვავდება სიმარტივით: გაუშვი და მიიღე პაროლები, რომლებიც შეჰყავთ საიტზე ლოკალური ქსელის სხვა წევრებს.

3. **httpry** — იჭერს საიტებზე შეყვანილ პაროლს

კიდევ ერთი სნიფერი, მაგრამ მხოლიდ HTTP-ტრაფიკის სპეციალიზირებით. აგროვებს მონახულებული გვერდების მისამართებს, ლოგინებს და პაროლებს.

4. **iptraf** — ვინ რამდენი ხანი იჯდა ინტერნეტში, ქსელური ტრაფიკის აღრიცხვა.

აუცილებელი პროგრამა იმათთვის, ვინც შედის ქსელში მობილურიდან მეგაბაიტური ტარიფიკაციით. iptraf გამოსახავს შემოსულ და გასულ ტრაფიკს, ასევე დაკავშირების საშუალო სიჩქარეს.

5. **mysql-sniffer** — იჭერს MySQL კითხვებს და ბრძანებებს

ვებ-დეველოპერისთვის შეუცვლელი ინსტრუმენტი. პროგრამა აფიქსირებს ყელა მიმართვას MySQL-ის ლოკალ სერვერთან.

6. **ngrep** — ძიება ქსელურ დინებაში

როგორც grep, ოღონდ ქსელური ტრაფიკისთვის. შეიძლება შეამოწმოთ სად მიდის თქვენი პერსონალური მონაცემები.

7. **p0f** — ოპერაციული სისტემების დეტექტორი

იძლება საშუალებას პასიურად განვსაზღვროთ მოწყობილობის ტიპი და მანქანებზე დაინსტალირებული ოპერაციული სისტემები. შემტევი არ გამოჩნდება და დაზვერვის ფაქტი არ გამოისახება ჟურნალში.

8. **snort** — შემოჭრის აღმომჩენი სისტემა

ქსელური შემოჭრის აღმომჩენი სისტემა. აღმოაჩენს და დეტალურად დააპროტოკოლებს თქვენ კომპიუტერზე ან სერვერზე ყველა ქსელურ შემოტევას. ვინ შემოგიტიათ, როდის, საიდან, როგორი პორტი, როგორი შედეგით და ა.შ.

9. **tcpdump** — ქსელური ტრაფიკის გადაჭერა

იწერს მთელ ტრაფიკს უნიერსალურ PCAP ფორმატში მომავალი შესწავლისთვის. მაგალითად, შეიძლება ჩავწეროთ საჯარო Wi-Fi ქსელის ტრაფიკი და სახლში Wireshark-ის საშუალებით შევისწავლოთ ჩაწერილი.

10. **iftop** — ქსელის ქვესისტემური წარმადობა

ქსელის ქვესისტემური წარმადობის მონიტორინგი. ინტერნეტი ამუხრუჭებს? დასაწყისისთვის შეამოწმეთ iftop - შეიძლება ქსელური ადაპტორი ვერ ქაჩავდეს.

11. **netstat** — რა ხდება? გვიჩვენებს გახსნილ ქსელურ პორტებს და მათთან დაკავშირებულ კლიენტებს. პერიოდულად სასარგებლოა გაუშვათ სერვერზე შესამოწმებლად, ხომ არ დაატროიანეს კომპიუტერი.

12. **netcat** — უნივერსალური ქსელური ინსტრუმენტი
უმაგრესი პროგრამა, რომელიც გვაძლევს საშუალებას გავხსნათ სოკეტები და გადავაბათ ისინი ბრძანების ველს. მაგალითად, შეიძლება გადავაბათ bash-ი ერთ-ერთ პორტს და მივიღოთ დაშორებული ადმინისტრირების საშუალება.
13. **dhcpdump** — ლოალურ ქსელზე მონაცემების მიღება
პროგრამა გვაწვდის ინფორმაციას ფართოგადაცემის პაკეტებზე DHCP-სერვერისგან, რომელიც მუშაობს ჩვენ ლოკალურ ქსელზე. მოგროვილი ინფორმაციის შეიძლება ადვილად გავიგოთ შლუზის მისამართი, DNS-სერვერი და სხვა ინფორმაცია იქამდე, სანამ ჩავერთვებით.
ზოგი ჰაკერი მუშაობს მარტო. ეს ეხება როგორც იმას ვინც ტეხავს სისტემას და იპარავს ინფორმაციას, ასევე მათ ვინც დამოუკიდებლად წერს მავნე პროგრამებს. ჰაკერების ჯგუფი დიდ დროს უთმობენ ვირუსის დაწერას ან მათ მოდერნიზაციას. ბოლო დროს დაჯგუფებეის რაოდენობა გაიზარდა, ისევე როგორც გატეხვის და მოპარვის რაოდენობა.

ვინ შეიძლება გახდეს ჰაკერების მსხვერპლი? - პასუხი: ნებისმიერი ჩვენგანი! ნებისმიერი კომპიუტერი რომელსაც აქვს კავშირი ინტერნეტთან - შეიძლება ახდეს დაცველი. ფიქრი ინაზე, რომ თქვენი ძველი სახლის კომპიურეტი არავის არ აინტერესებს - არასწორია. ყოველთვის გახსოვდეთ ქსელში უსაფრთხოება:
-ნუ აქვეყნებთ თქვენ პირად მონაცემებს ქსელში
-ნუ აქვეყნებთ საბანკო ანგარიშის მონაცემებს
-დაადეთ რთული პაროლი თქვენ ტელეფონს, კომპიუტერს და აქაუნთს სოციალურ ქსელში
-თქვენი პირადული და მნიშვნელოვანი ფაილები, რომლებსაც კომპიუტორზე ინახავთ - შეინახეთ პაროლიან zip არქივში
-გახსოვდეთ, რომ რითაც უფრო გრძელი და რთული პაროლი გიდევთ - მით უფრო ძნელია მისი გატეხვა
ჩვენ გაკვეთილებზე თქვენ ისწავლით, თუ როგორ უზრუნველყოთ თქვენი პროექტების და სერვერის უსაფრთხოება.
წარმატებები, მეგობრებო და ყოველთვის გახსოვდეთ ინტერნეტში უსაფრთხოების შესახებ!

----------ENGLISH----------

HACKERS

Hello friends, we want to tell you a little about hackers and security on the Internet. Previously, a hacker was called a highly professional computer specialist who in an unusual, non-standard way solved computer problems.

There are two main definitions:

White hackers, on network slang *White hat* (engl.) - computer security specialists who specialize in computer system security testing. White hackers are looking for vulnerabilities on a voluntary basis or for a fee in order to help developers make their product more secure.

Black hackers, on network slang Black hat (engl.**)** - these are specialists who identify weaknesses in computer systems and use them to get their benefit, to the detriment of a hacked computer system

What do hackers use? What are they learning to hack our computers? We recommend that you also study in brief these technologies so that you can protect yourself from hacking.

1. The ability to program in at least one popular programming language.

2. knowledge of computer networks IPv4, IPv6, DHCP, NAT, subnets, DNS, routers and switches, VLAN, OSI network model, public and local IP, MAC addresses, ARP.

3. Linux and Wireshark
Hackers love Linux OS. You could even say that Linux is the most popular OS among hackers. The existing hacking tools on Linux were developed specifically for hackers.

4. Virtualization
The essence of virtualization for a hacker is to test your ideas using a virtual version.

5. Wireless technology
Most often hack Wi-Fi networks. To know how hackers attack wireless networks or electronic devices, you need to know all their functions. To do this, you should study the professional encryption algorithms for WPA, WEP, WPA2, WPS, and a handshake.

6. Databases and Web Applications
Thanks to the DBMS, you can access or hack databases. Databases are a set of data stored on a computer that can be accessed in various ways.

These are the linux programs used by hackers:

1. nmap — Nmap scanner as the main tool for movie hackers.
This program flashes in almost all films about hackers, for example: **Matrix Reloaded**, **Snowden**, **Dredd**, **Elysium**, **Fantastic Fou**, **Who Am I**, **Bourne Ultimatum, Die Hard 4, The Girl with the Dragon Tattoo, Retaliation 2, Abduction**

Used for Internet intelligence: definition of equipment, OS, network structure. Allows you to identify open ports on remote computers and determine the names of services and version numbers. The system administrator can use it to troubleshoot network problems.

2. **dsniff** — pulls out logins and passwords
Well known to many people sniffer. Differs in simplicity: you can launch it and get yourself passwords that other members of the local network enter on the sites.

3. **httpry** — intercepts passwords entered on sites
Another sniffer, but with specialization only on HTTP traffic. Collects addresses of visited pages, logins and passwords.

4. **iptraf** — how many time who spent on the Internet. Accounting for network traffic.
The program is required for those users who access the network via mobile networks with megabyte charging. iptraf shows the amount of incoming and outgoing traffic, as well as the average connection speed.

5. **mysql-sniffer** — intercepts requests to MySQL and responses
An indispensable tool for web developer. The program records all calls to the local MySQL server.

6. **ngrep** — search in the network stream
Like grep, only for network traffic. You can check where your personal data is leaking.

7. **p0f** — operating system detector
Allows you to passively determine the type of equipment and installed operating systems on machines. The attacker will not reveal himself and the fact of intelligence will not fall into the logs.

8. **snort** — intrusion detection system
Network intrusion detection system. Identify and record in detail all network attacks on your work computer or server. Who attacked, when, from where, what ports, with what result, etc.

9. **tcpdump** — network traffic capture
Records all traffic in universal PCAP format for further study. For example, you can record the traffic of a public Wi-Fi network and at home examine the recorded using Wireshark.
10. **iftop** — network subsystem performance
Monitoring the performance of the network subsystem. Do you have braken Internet? Check at the start iftop - it may be trite weak work of the network adapter.
11. **netstat** — what's happening? Shows open network ports and clients connected to them. Periodically it is useful to run on servers to check if the computer has not been infected by trojan.
12. **netcat** — universal network tool
The coolest program that allows you to open sockets and bind them to the command line. For example, you can associate bash with one of the ports and get the simplest remote administration tool.
13. **dhcpdump** — local network data retrieval
The program provides information about broadcast packets from a DHCP server running on your local network. On the basis of the collected data, you can easily find out the gateway address, DNS server and other information before connecting.
Some hackers work alone. This applies to both those who hack into the system and is engaged in the theft of information, as well as those who independently write malicious programs. Grouping hackers pay a lot of attention to writing viruses or upgrading them. Over the past few years, the number of groupings has increased, as well as the number of burglaries and thefts.

Who can fall victim to a hacker? - The answer is any of us! Any computer with Internet access may become vulnerable. To think that your old home computer is not interesting to anyone is not correct. Always remember about network security:

-Do not post your passport data online
-Do not post your bank card details
-Set complex passwords on your phones, computers and accounts in social networks
-Your personal and important files that you store on your computer - store in zip-password-protected archives
-Remember that the harder and longer your password is, the harder it will be to crack
In our classes - we will teach you how to secure your projects and servers.
Good luck friends and always remember about the safety in the Internet!