━ BIG TUTORIAL ━

PASSWORDS - BIG TUTORIAL BY MRBLACKX & ODIN

We will speak about:

-> Weaknesses in passwords

-> Tools for Hacking Passwords

-> Hacking Passwords of a OS

-> Hacking Password protected files

-> Protect yourself from attacks

⊰⍰⊱┈────────────────────────╌❊╌────────────────────────┈⊰⍰⊱

The hacking from passwords are one of the simplest way to get into Systems, Logins, Networks and so on.

Strong passwords can be easy created and managed.Ideally, you should use longer and more complex passwords. If a password hacked its not easy to trace Back who hacked it.

External or Internal Attacker be used many methods:

-> Can find important infos trough social engineering

-> Shoulder Surfing (looking by pins on bank over shoulder)

-> Keylogger

-> Software which can scan internetprocotols for getting passwords

Note:

If you know a password, you dont have to be an authorized user for a long time.

Vulnerabilitys on Passwords

A big problem that will come is if you leave trust on a "secure" password, the chance is higher that you arent the only person who know it alone. So you cant know if someone else know your password in a other wise such as password is

Bob birthday and his state: oakland0105

So easily some says Bob comes from oakland and has as soon as possible on 01.05 birthday.

Vulnerabilitys can be sorted by two categories:

- Vulnerable into a company or a user

For example : Missing Password policies

- Technical vulnerabilities

Weakness Password or written passwords on paper on a desk

Organically Vulnerabilities of Passwords

Its in human nature to make your work as comfortable as possible what includes if you need to remember on 5,10, or 50 passwords.

With the simple letters of the alphabet and the numbers 0-9 can be generated round about 3 billions of passwords. Length of 8 letters.

They key to strong passwords are two aspects:

- Passwords should be easy to remember

- It should be heavy to hack/crack it

Users loves it to use passwords like Cat135, their username or empty passwords.

As long as users are not persuaded to use strong passwords, the following usually applies to them:

- They are simple to guess
- They won't be change often
- They will used for different logins with same password
- They will noted at unsecure places (monitor,desk,wall)

Note:

If a Attacker got a password maybe they can access to other system like gmail,webmail,psn,netflix

Tip✅:

Use different passwords on different sites/logins/platforms, if not you invite attackers for a attack.

Technical Vulnerabilities of Passwords

If you learn intensive about vulnerabilies about passwords you will get most of time technically vulnerabilies of these:

- Weak Encryption schematic for passwords:

Hacker can crack weak storages mechanisms for passwords. Many Developer believes passwords are save as long as source code for encryption algorithms aren't leaked. False. Attackers with time(much time) can crack it maybe. If the code unlocked, the code will send over internet and this was called leaking.

- Programs that store passwords in memory, unprotected files and easily accessible databases

- Non-Encrypted Databases, which have access to sensible files / data

- Applications/Tools for User which shows password clearly. (without ***)

The National Vulnerability Database has thousand of vulns in context of passwords.

If you want to know more about visit page : http://nvd.nist.gov

Cracking passwords on common way

Hacker use many methods to get passwords.

I will try to explain you some methods.

Social Engineering:

This are one of the known method for getting a password.

So in Social Engineering hacker will abuse the trust of a people / friend, to get information. The Aim of SE is that target speak out their passwords.

That sounds weird but works again and again.

Techniques:

To get passwords about social interaction you need to ask in principle easily.

For example:

Call user and tell him/her important emails hanging into the email queue and you need password for login because only you can access to that email

Note:

Through this way Attacker mostly inside a company like work mates will trying to get passwords.

A another possibility is to get user to give us passwords through a phishing mail. So a phishing mail will ask for sensitive information (passwords,name,creditcard etc…).

So you can ask intern users for a confirmation to a "new" policy, then you can ask into that mail a fake secret question and they need to login to a phishing page.

Tip✅:

If you get passwords into a test from users, try to care that passwords will be changed so if something happens later you dont get in trouble.

Helpful is by during social engineering go to internet and find out Names, Phone Numbers and E-Mails. You can use Social Networks like:

- LinkedIn
- Facebook
- Twitter

etc…

Countermeasures:

You need to work out users for security. The best way is dont give any information away. So you can messages Systemadmin if you get any weird email.

And delete Employees names from websites, its better.

Shoulder Surfing:

Shoulder surfing (looking over your shoulder to get user inputs) is an effective, technically not costly way to spy passwords.

Techniques:

For getting success, you need to get target in your near. You will get password if you looking at the Display or the Keyboard of the user. Masters in this know if users look around if someone watch them. So in banks they have (little) cameras, be aware or use hoodie. Internet coffee shops or Airport are ideally for shoulder surfing.

The view over shoudler can you test always.

So you can walk around your office and let the view randomly wandering, then go to desks of users and demand them To login on their network, email or computer. (dont tell them your practice)

And try to get infos.

Countermeasures:

Look at your surroundings and dont enter passwords if someone can look over your shoulder.

Inference:

By infernces you will guess passwords through conclusions to be dawn to known userdata for example Birthday-Date, Favourite Series, Phone Numbers.

It sounds weird but attackers found out keywords through guess.

The best defense against inference is to bring users to use strong passwords without any context to private infos.

Weak Authentication:

If you use older or unprotected operating systems, there you can login without passwords, external attackers hasn't any problem to get inside system. So the same is for tablets and phones.

Use passwords / pins or fingerprint.

Bypass Authentication:

So you can bypass authentication if computer configured that automatically login if user click enter (No password). Into the system you can looking for passwords.

You can use some softwares like:

- Proactive System Password Recovery (www.elcomsoft.com/pspr.html)

- Cain & Abel (www.oxid.it/cain.hmtl)

Countermeasures:

The best defense is that any device if they are powered on, asking for a password. Second is update your

System.

Tip✅:

Modern Authentic action systems like Kerberos (Windows) and directorys services (Microsoft Active Directory) encrypt passwords and doesn't transfer it over a network.

Cracking Passwords

The encryption of passwords counts to the tasks that attackers makes funny.

Where and how can i begin with encrypting passwords??

Generally it working popular user passwords.

So if you get a Admin password, you can control a network and a full Computer.

Adminpasswords are the pot of gold. If you want to study vulnerabilities of passwords in a company, you should be begin a high access level like Root/Admin.

Technically Demanding Password Determination

So here by technically demanding cracking from passwords, we will use softwares. Its very demanding but you computer do it automatically.

The important methods of cracking / hacking passwords running about a wordlist with violence (bruteforcing) or tables (rainbow-tables).

Softwares For Cracking Passwords

You can try to crack passwords with some softwares.

I show you softwares and give a little explanation.

Before starting, i want to remember, most of tools will be detect from virus scanner because for exmaple brutus or pwdump are Hacking-Tools for bad interactions. (turn off virusscanner)

- Brutus (http://www.hoobie.net/brutus/brutus-aet2.zip)

It will try to crack HTTP, FTP, TELNET and other logins. (the website is secure but your browser will detect it as an threat).

- Cain & Abel (www.oxid.it/cain.html)

cracks hashcodes from LM and NT LanManager (NTLM), Windows-RPD passwords, Cisco-, IOS- and PIX-hashes, VNC Passwords, RADIUS-Hashcodes and many other. (Hashes or Hashcodes are cryptographic represented from passwords. Shortly called hashes).

- Elcomsoft Distributed Password Recovery (www.elcomsoft.com/edpr.html)

cracks passwords from Windows, Microsoft office, PGP, Adobe, iTunes and many others. This software can use the GPU for speed up the attack.

- Elcomsoft System Recovery (www.elcomsoft.com/esr.hmtl)

cracks passwords from Windows Users and can reset them, can reset expire dates of passwords, can misuse admin rights.

This all from a bootable 💿.

- John the Ripper (www.openwall.com/john) will crack hashed Linux/Unix/Windows passwords.

- Ophcrack (http://ophcrack.sourceforge.net)

Cracks passwords of Windows users by using rainbow tables, from a bootable cd.

Rainbow tables are already calculated hashes from passwords which helps to speed up the attack.

- Proactive Password Auditor (www.elcomsoft.com/ppa.html)

Will running bruteforce wordlists and rainbowtables against extracted LM- and NTLM-Password hashes.

- Proactive System Password Recovery (www.elcomsoft.com/pspr.hmtl)

Will setup all lokal saved passwords and recover it. For example login passwords:

> WEP/WPA Passwords

> SYSKEY Passwords

> RAS/VPN Passwords

- Pwdump7 (http://www.tarasco.org/security/pwdump_7/)

Extract Windows Password Hashes from SAM-Database. (Database for Security Account Manager)

- Rainbowcrack (http://project-rainbowcrack.com)

cracks very fast hashes of LanManager (LM) and MD5 hashes, rainbow crack use rainbow tables.

- THC-Hydra (https://sectools.org/tool/hydra/)

cracks Logins for HTTP, FTP, IMAP, SMTP, VNC and many more.

Some Of these tools/applications needs physically access to the testing systems.

Understanding Process of Tools

For understanding how to use this softwares, you need to know how passwords will be encrypted. So by encryption we use hashes like MD5 SHA256 or SHA2. So passwords can't be decrypted. Under linux has hashed passwords random numbers, for example that no passwords are same.

Tools which be used for cracking passwords will using known password from a wordlist.

For cracking hashes it will so:

The created encrypted hashs will be compared extremely quickly with the password hashed from the original password database.

If there's a match, the password was cracked.

Other tools for cracking passwords will trying only to login and will using defined user names and passwords.

Many tools working with it like:

- Brutus (http://www.hoobie.net/brutus/brutus-aet2.zip)

- SQLPing3 (www.sqlsecurity.com/downloads)

This are only wordlists password cracking tools.

Where are passwords stored?

So before i telling you where passwords are stored, you need to know if you try to crack a account your account or the target account will blocked so be aware for doing this.(but not always)

Where passwords are saved will depends on the operating system:

• **Windows:**

Windows saved normally all password on:

- SAM Database (Security Account Managers), located at C:\Windows\System32\config

- The Active Directory-Databasefile will either saved lokal or over the domaincontroller (ntds.dit).

Windows password exist also in directory :

C:\Windows\Repair

C:\Winnt\Repair

• **Linux/Unix**:

In Linux or Unix its a little big different.

Here we need admin/root to access to the given folders/directorys:

/etc/passwd (can be read by everyone)

/etc/shadow (only root)

/etc/security/passwd (only root)

/.secure/etc/passwd (only root)

Some Windows applications will save passwords into the registry or in simple text documents. A simple search for password, passwort reach for finding our txt. (but its seldom) @MrBlackX

Starting Attack with Word list [Bruteforce]

So here we begin our first attack with a known method called bruteforce.

During a bruteforce attack, known password and words will used from a wordlist or a password database.

A password datei is not more than a text document with 100.000 passwords or more.

So we can use a written wordlist or a self created.

So we can created a specify personally wordlist using script cupp (https://github.com/Mebus/cupp).

Or we can download some wordlists:

• German:

http://debuggen.com

• English:

ftp://ftp.cerias.purdue.edu/pub/dict

www.outpost9.com/files/wordlists.html

[Note]:

Dictionary attacks are only as good as the word lists provided to password cracking programs.

So maybe you need days/weeks for finding a match. So bruteforcing worked on the best way by weakness passwords.

So for bruteforcing you need time, because it will try to crack all possible combinations, all characters, password length etc. (a example is the tool Proactive Password Auditor (windows))

Infos/Tips:

• Bruteforce attacks depends on the complexity of passwords and the speed of the computer

• Do a Attack after working time. For example at midnight so systemlogs dont save the failed logins

• Can prevent expired passwords hacker attacks? --> Yes

For simple passsword generation use this:

https://passwordsgenerator.net/

@MrBlackX

Starting Rainbow Attacks

In rainbow attacks password hashes from LM, NTLM, Cisco, PIX and md5 are cracked faster with very high success rates.

Unlike dictionary attacks / bruteforce attacks, rainbow attacks cant crack indefinitely long passwords.

The maximum of length of LM-hashes are 14 characters. For the dictionary based Hashes since Windows Vista (NT-Hashes) are the maximum at 16 characters.

You can download the Rainbow table from:

http://ophcrack.sourceforge.net.

Since creating rainbow tables costs a lot of time there were length limitations.

For cracking hashes in seconds/minutes/days/

Downloas this two files:

- http://project-rainbowcrack.com

Or

- http://ophcrack.sourceforge.net

Unlock/Cracking windows password with pwdump7 & JTR by MrBlackX

For cracking windows passwords we can use two tools:

- pwdump7
- John the Ripper

<Download:>

https://mega.nz/#!LTghkYrZ!I6JHdVdYQ0IpQC5glioWQz0DzbhfFFE6P2KXTju1dpE

(pack by me, it will get hits by testing on virustotal because they are bad tools for dumping passwords)

[NOTE:] Admin rights needed. Easily ask admin for using any word installation,so i use social engineering skills.

1. Create a folder in C: called passwords

2. Download WinZIP (www.winzip.com)

3. Download the tools and files and extract these into passwords folder:

- pwdump7
- John The Ripper (john179)

extract both into passwords.

4. Open cmd as an Administrator and type

```
C:\passwords\PwDump7>pwdump7 > cracked.txt
```

This save it as an txt file called "cracked.txt"

It will dump password so it will need minutes/hours/days. Because its hashes From Windows-SAM database.

5. Now we will use JTR for running hashes cracking.

Before we copy cracked txt into : C:\passwords\john179\run

Now Type:

```
C:\passwords\john179\run> john cracked.txt
```

So this can need some time.

Linux and Unix passwords:

So like in windows download from www.openwall.com/john.

1. In Linux / Unix passwords will be saved on /etc/passwd or /etc/shadow.

After downloading john cd to download and type this:

```
[root@localhost mrblackx]#~: tar -zxf john-1.8.0.tar.gz
```

If version newer customize it.

2. Now goto /src and type

```
make generic
```

Choose in directory /run and type these command:

```
[root@localhost mrblackx]#~: ./unshadow /etc/passwd /etc/shadow > cracked.txt
```

Note: the tool shadow isn't compatible with all unix versions.

3. For cracking type

```
[root@localhost mrblackx]#~: ./john cracked.txt
```

If john ready (need time) then you will get output.

Cracking password protected files

You want to know how to crack password protected files?

It gaves great tools for cracking password protected files.

Cracking Files:

The most password protected are cracked in seconds or minutes.

The following scenario will show you how it works:

1. The management of the finance department do a document with trusted infos. (excel table).

2. The table will get a password while saving file.

3. So for more secure they'll maybe compress to a Zip file with a another password.

4. The file send via email

5. The admin save the file and remember to a tool that cracks files, Archive Password Recovery (www.elcomsoft/archpr.html).

The cracking of a password protected file is really easily.

✅**Tip:**

If you use Advanced Archive Password Recovery goto settings, there you can setup the time.

Countermeasures:

The best way is to ask for a entryption winzip with AES or PGP encryption.

More options, to get Passwords

Logging entries using the keyboard:

One of the best proceedings, to get passwords is the logging of keystrokes.

We need to use a Software by during a Keystroke logging or Keylogging Attack.

Because the Softwares will read all inputs.

[Note]:

Installing Keylogger-Softwares on a pc or keywords for monitoring without permission

you can get in trouble.

Logging-Tools:

With keylogger you can access log files to determine the passwords which used.

Keylogger can install on a target Computer.

I recommend the keylogger software spyrix. (http://www.spyrix.com/de/download.php).

If you want of all software a combined folder of all tools, let me know.

Hardware based tools like KeyGhost(www.keyghost.com) are clamped between keyboard and computer.

Tip:

If you install keyloggers on shared computers, they will log the entries and passwords of all users who use this computer. (Remember this next time you visit the Internet Cafe)

Countermeasures:

The best defense against the Installation of a Keylogger is the insert of a Anti Malware programs.

For physical keyloggers only a regular inspection of the systems helps.

[Note]:

Some keyloggers will hide as an Malware, Shareware, Freeware or attach emails.

Dont download tools/program from unknown source.

Invisible Password Storage

Many older programs and only local applications like email, softwares and apps for internet banking store passwords locally.

You can search for local saved password manually or automatically through programss like FileLocator(http://filelocator-lite.findmysoft.com/)

Searching:

You can do a search with your tool, for example:

findstr, grep

It gaves much programs which writes passwords clearly to your harddrive.

Uncertainly stored passwords is the dream of criminal hackers..

Countermeasures:

The only reliable measure against an insecure password repository is to only use applications that store passwords securely.

So if a tool get an update you maybe read new changelog about saving passwords.

Network Analysators

So here they Network Analysators wil analyze the network transfered packets, so hacker will do it aswell if they want to get access to PC, WLAN or something else.

Testing:

For example we use the network tool Cain&Abel (www.oxid.it/chain.html) this tool can print passwords. If we run this tool for 1 hour, they can get 1000 of passwords. (remember if you are back in school).

Cain & Abel can be configured by different ports:

FTP, HTTP, Teller and more.

[Note]:

If traffic not running over a vpn, ssh or any third application tunneled, the traffic is attackable.

Finally Cain and Abel is a tool for cracking passwords, through analyzing network traffic.

If you want tools for only scanning / analyzing i can give you 3:

• OmniPeek [Price] (www.savvius.com/products/overview/omnipeek_family)

• CommView [Price] (www.tamos.com/products/commview)

• Wireshark [Free] (www.wireshark.org)

If you want,you can try to get cracked version of all the given softwares.

You can use network tools for different ways.

You can enter filters for example udp,tcp.

If you search for POP3-passes then search for PASS.

Countermeasures:

Some countermeasures against networks attacks 🙏□:

• Use Networks Switches no hubs.

If you need to use hubs, programs like sniffdet(http://sniffdet.sourceforge.net for unix) or PromicsDetect(http://nsecurity.nu/toolbox/promiscdetect for windows) exlore, which will be in a promiscuity mode.

• Dont let someone touch your switch or network connections.

Tip:✓

Switches hasnt full security, they have weaknesses about ARP-Poisoning Attacks.

Weak BIOS Passwords

The most BIOS-settings will allow that computer has a boot password.

So can you bypass password:

- Reset password through deleting cmos-batterie or place a jumper on motherboard

- Search for BIOS Password Cracker Softwares

- If you can delete a harddisk and use it on a another computer.

A good system password list with different Creators of PC can you find here:

www.cirt.net/passwords

With bad passwords into mischief

Hackers using often new created user accounts, or accounts of network admins which was reseted by helpdesk.

Accounts must be reseted if user forgot their passwords.

Vulnerabilitys:

- If user accounts will be reset, they will get often easy crackable passwords (like username or "password")

So the time Between changing password is the best point for a password attack.

- Many systems has either common accounts or not used accounts with weak password are a good target.

Countermeasures:

The best defense is configure the helpdesk so that users/admins can't create weak passwords.

- Ask users to stay connected to the help desk by phone.

- Talk to users and task them that they need to change password while your presence.

- For the maximum of security you can implement stronger authentication, (challenge-response, smartcards, digital certification).

- Automate reseting of password means give users tools so they can control it by there self Without help of admins.

You can manage password with a passwordmanager:

- Lastpass (http://lastpass.com/)

- Password Safe (https://pwsafe.org/)

However, this program only manage passwords, they arent protected against attacks.

Tip✓:

Dont note passwords on your desks/monitor.

PASSWORD TIPS:

For password we can use some password policies:

- Show Users how easily we can get passwords.

- Use lowercase and uppercase letters

- Use Typing errors like scr3en, or use sentences

- Use puntuaction marks

- Changes Passwords all 6-12 months

- Use different passwords on different system. In pactular for hosts of networks. (server, firewall, router)

- Use different long passwords from 6-20.

- Don't use any simple words which can be hacked by dictionary attacks

- Use for e -> 3 or a -> 4 or o -> 0

- Don't write passwords on a paper and put it on your desk

Other countermeasures:

- Activate Security Checks (2FA- 2 factor authenticating)

- Check your Apps that they don't storage your passwords

We can use a tool called WinHex (www.winhex.com/winhex/index-m.html)

Tip✅:

Some trojans which can cracks passwords will transfered over Emails. Good software are :

- Bit9 (https://www.carbonblack.com/company/news/press-releases/bit9-carbon-black-is-now-carbon-black/)

- Webroot (https://www.webroot.com/us/en/home/products/wsa-installer-download)

- Update your Systems always

- Know the IDs of your user's.

If a account never used, delete or deactivate it.

You can use a tool called DumpSec (www.systemtools.com/somarsoft/?somarsoft.com)

- Automatically reseting of passwords

- Protect your BIOS with passwords.

Protecting OS Systems

So guys here are on last tutorial. Attention attention.

You can use different methods to secure your operating systems.

Try to do more than 1-5 attacks for the best security on your system.

Windows:

Some Windows Passwords can be find out easily, so we can for example read it in registry database (win+r --> regedit).

So it's better you allow to set Admin permission, then if someone want to open register editor user need admin.

Protect your operating system through the known activities

- SANS (www.sans.org)
- NIST (http://crcs.nist.gov)
- Internet Security (www.cisecurity.org)

--> Keep copies of SAM-Database

--> Disable all saves of LM-Hashes under 15 characters

You can create a registry entry NoLMHash in:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa set the value to 1.

--> Use our password tips

--> Activate Windows Firewalls

--> Do not Allow Anonymous Enumeration of SAM accounts and share

Linux and UNIX:

--> Use Shadow passwords with MD5

--> Don't create weak passwords (use cracklib or npasswd or passwd+)

--> Check in /etc/passwd if UID0 (root) has more entries or not

So thanks for reading this.

I wrote this since two weeks. Sorry for last inactive on my channels.

Your ViperZCrew Team and MrBlackX

Best regards, soon a Network Host Hacking Guide. :)

⊰⍰⊱┈──╌❊╌──┈⊰⍰⊱

MrBlackX to Nihkil (ؕتؕ)

╭∩╮（￣▽￣）╭∩╮

+++ BONUS TUTORIAL BY MRBLACKX +++

https://anonfiles.com/c498AeVam5/How_to_Dox_Anyone_ViperZCrew_pdf

+++ DOWNLOAD LINK GIVEN +++