

# Обнаружение уязвимостей. – Telegraph

T [telegra.ph/Obnaruzhenie-uyazvimostej-06-27](https://telegra.ph/Obnaruzhenie-uyazvimostej-06-27)

Life-Hack - Linux/Хакинг/Хакер/ИБ/Osint

June 27, 2024



Теперь, когда мы завершили составление карты сети, следующее, что нам нужно сделать, – это определить, какие из служб, которые мы только что обнаружили, уязвимы для сетевой атаки. Итак, нам нужно ответить на следующие вопросы:

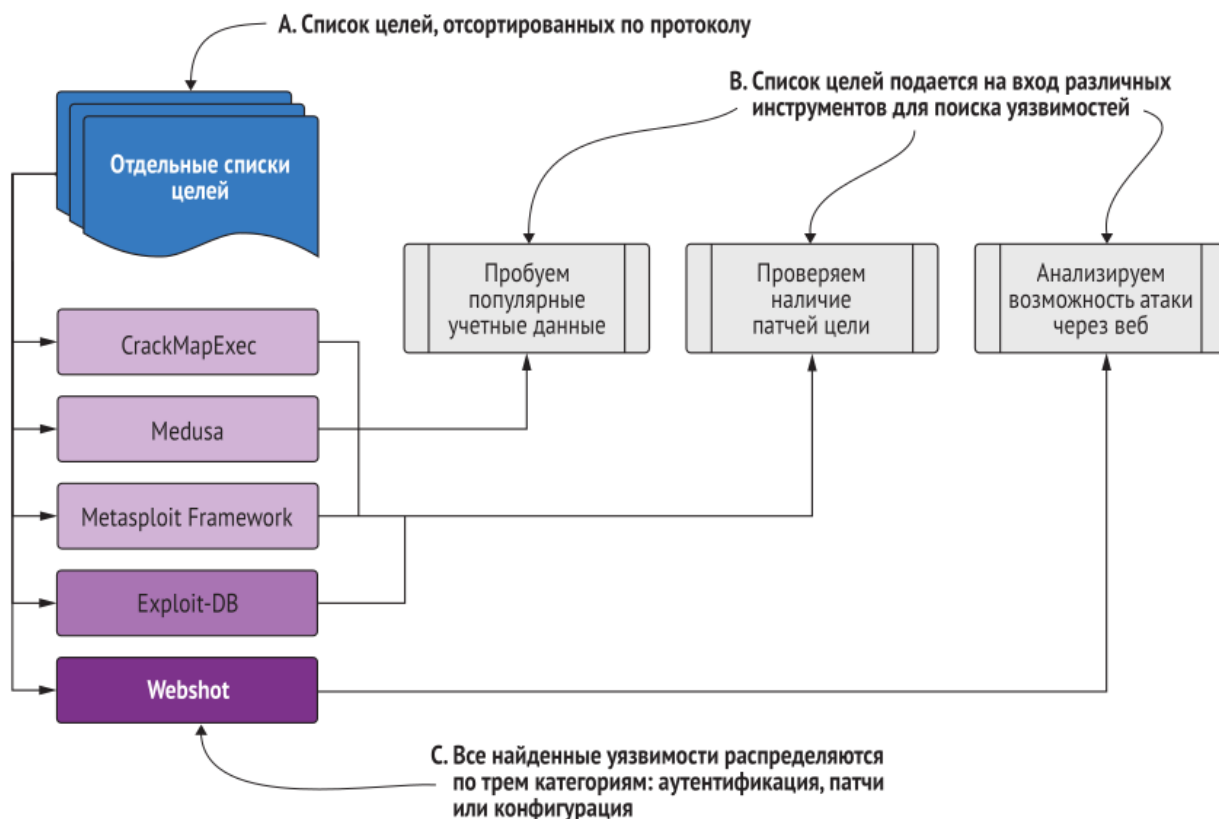
- Применяются ли в сети пароли по умолчанию?
- Установлены ли все последние исправления безопасности и обновления от поставщиков ПО?
- Актуальна ли система?

Способность мыслить как злоумышленник, единственная цель которого – проникнуть внутри любыми доступными средствами, имеет решающее значение для выявления слабых мест в вашей целевой среде.

В результате сбора информации о целевой сети вы должны были создать набор списков для конкретных протоколов, которые представляют собой текстовые файлы с IP-адресами. Файлы сгруппированы по прослушивающим службам, а это значит, что у вас есть один файл для каждого сетевого протокола, который вы хотите оценить, и этот файл должен содержать IP-адрес каждого хоста, найденного на предыдущем этапе, на котором запущена эта конкретная служба. Ниже представлена обобщенная схема процесса обнаружения уязвимостей. Акцент здесь следует сделать на трех действиях:

- Попытка применить общие учетные данные;
- Определение наличия патчей;

– Анализ направлений атаки через веб.



Каждый целевой список вводится в один или несколько инструментов для обнаружения уязвимых мест, таких как отсутствующие, слабые учетные данные или учетные данные по умолчанию; отсутствующие обновления программного обеспечения или небезопасные настройки конфигурации.

Как и настоящие сетевые злоумышленники, мы всегда стремимся найти путь наименьшего сопротивления. Уязвимости и векторы атак различаются по уровню усилий, необходимых для успешной и надежной компрометации пораженной цели. Поэтому в первую очередь мы ищем наиболее очевидные и легко обнаруживаемые векторы атаки. Такие векторы иногда называют уязвимостями с низким уровнем риска, очевидными мишенями или, если использовать жаргон взломщиков, низко висящими фруктами (low hanging fruit, LHF).

При нацеливании на LHF-уязвимости основная идея состоит в том, что если мы сможем попасть куда-нибудь быстро и тихо, то сможем избежать лишнего шума в сети, что полезно, когда требуется повышенная скрытность. Фреймворк Metasploit содержит множество эксплоитов и модулей для таких уязвимостей, например полезный модуль для быстрого и надежного определения MS17-010 (кодовое название: Eternal Blue) – LHF-уязвимости Windows, часто используемой злоумышленниками.

```

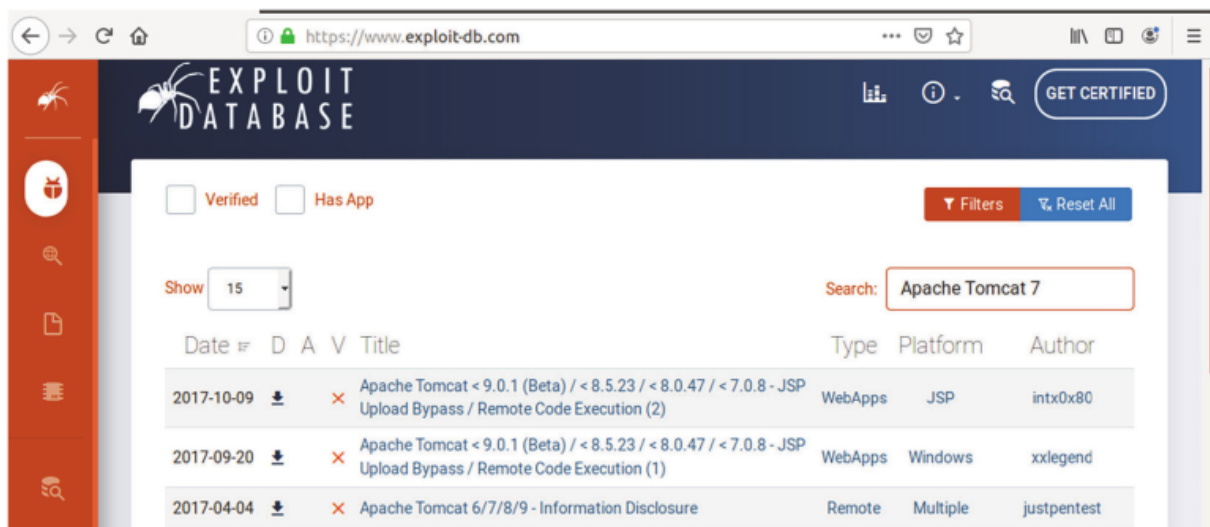
msf6 > use auxiliary/scanner/smb/smb_ms17_010
msf6 auxiliary(scanner/smb/smb_ms17_010) > set rhost 192.168.23.129
rhost => 192.168.23.129
msf6 auxiliary(scanner/smb/smb_ms17_010) > run

[-] 192.168.23.129:445 - Rex::ConnectionTimeout: The connection with (192.168.23.129:445) timed out.
[*] 192.168.23.129:445 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_ms17_010) > run

[+] 192.168.23.129:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7600 x64 (64-bit)
[*] 192.168.23.129:445 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_ms17_010) >

```

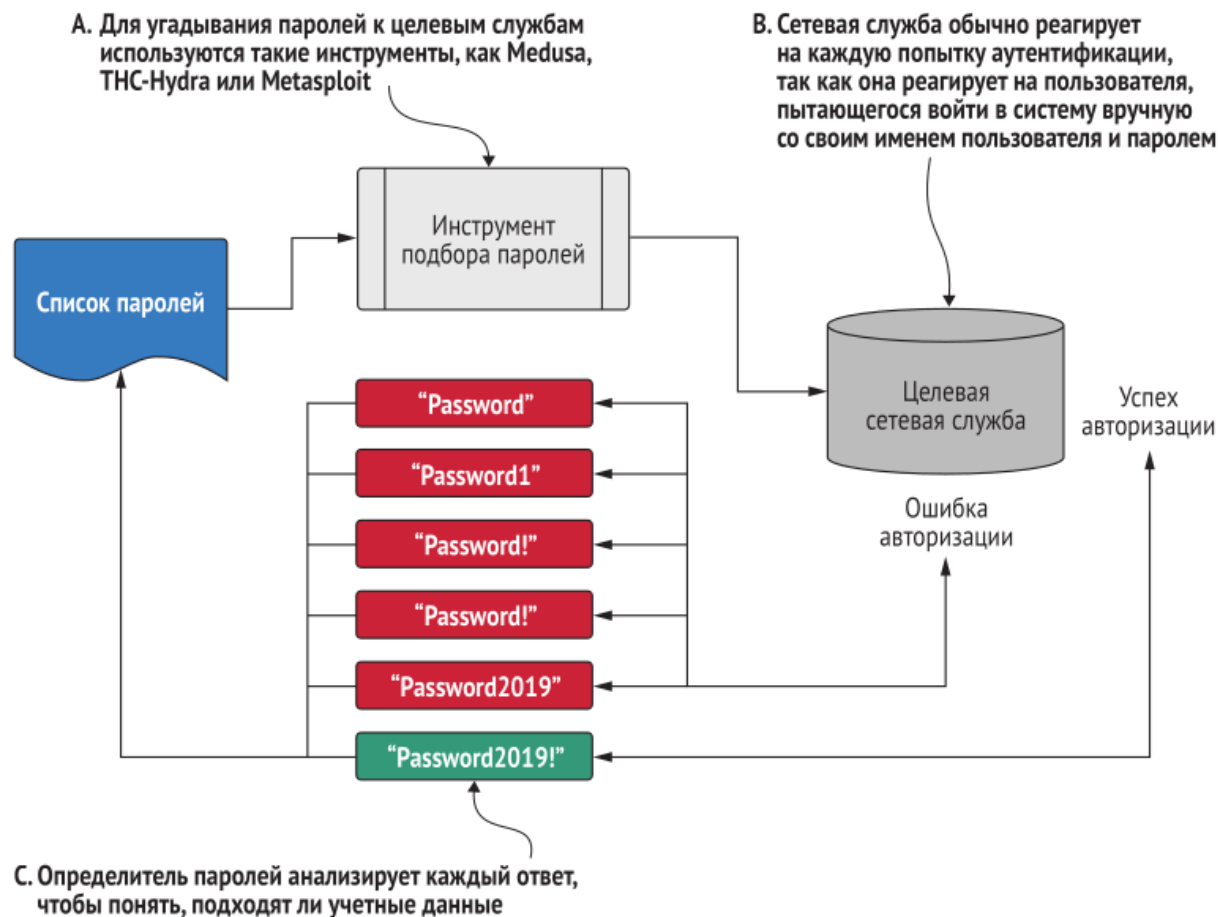
Обнаружение уязвимостей, связанных с отсутствием своевременных исправлений безопасности, заключается в определении того, какая именно версия конкретного программного обеспечения работает на вашей цели, а затем сравнении этой версии с последней стабильной версией, доступной от поставщика программного обеспечения. Если ваша цель использует программное обеспечение более старых версий, вы можете проверить общедоступные базы эксплойтов, чтобы узнать, исправлены ли в новейшем выпуске какие-либо ошибки удаленного выполнения кода, к которым может быть уязвима более старая версия.



The screenshot shows the Exploit-DB website interface. The search bar contains 'Apache Tomcat 7'. The results table lists three exploits:

Date	Download	Verified	Title	Type	Platform	Author
2017-10-09			Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code Execution (2)	WebApps	JSP	intx0x80
2017-09-20			Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code Execution (1)	WebApps	Windows	xxlegend
2017-04-04			Apache Tomcat 6/7/8/9 - Information Disclosure	Remote	Multiple	justpentest

Уязвимость аутентификации – это любое проявление пустого или легко угадываемого пароля по умолчанию. Самый простой способ обнаружить уязвимости аутентификации – выполнить атаку методом подбора пароля. Ниже показана упрощенная схема, демонстрирующая процесс подбора пароля с точки зрения сетевых злоумышленников.



Пример успешного подбора с помощью инструмента CrackMapExec:

```
root@JEFFLAB-DEB02:~/CrackMapExec# cme smb 192.168.29.38 -u ~/users.txt -p ~/passwords.txt -d jefflab.local
SMB 192.168.29.38 445 JEFFLAB-DC01 [*] Windows Server 2016 Standard 14393 x64 (name:JEFFLAB-DC01)
(domain:jefflab.local) (signing:True) (SMBv1:True)
SMB 192.168.29.38 445 JEFFLAB-DC01 [-] jefflab.local\Tony.Wonder:Winter2017 STATUS_LOGON_FAILURE
SMB 192.168.29.38 445 JEFFLAB-DC01 [-] jefflab.local\Tony.Wonder:Password123 STATUS_LOGON_FAILURE
SMB 192.168.29.38 445 JEFFLAB-DC01 [-] jefflab.local\Tony.Wonder:P@ssword STATUS_LOGON_FAILURE
SMB 192.168.29.38 445 JEFFLAB-DC01 [-] jefflab.local\Bob.Loblaw:Winter2017 STATUS_LOGON_FAILURE
SMB 192.168.29.38 445 JEFFLAB-DC01 [-] jefflab.local\Bob.Loblaw:Password123 STATUS_LOGON_FAILURE
SMB 192.168.29.38 445 JEFFLAB-DC01 [-] jefflab.local\Bob.Loblaw:P@ssword STATUS_LOGON_FAILURE
SMB 192.168.29.38 445 JEFFLAB-DC01 [-] jefflab.local\Gene.Parmesan:Winter2017 STATUS_LOGON_FAILURE
SMB 192.168.29.38 445 JEFFLAB-DC01 [-] jefflab.local\Gene.Parmesan:Password123 STATUS_LOGON_FAILURE
SMB 192.168.29.38 445 JEFFLAB-DC01 [-] jefflab.local\Gene.Parmesan:P@ssword STATUS_LOGON_FAILURE
SMB 192.168.29.38 445 JEFFLAB-DC01 [+] jefflab.local\Gene.Parmesan:P@ssword (Pwn3d!)
root@JEFFLAB-DEB02:~/CrackMapExec#
```