

# LIFE



Надеемся, что это самый нормальный отчёт, за который не стыдно)

## 1) Определить тип уязвимости, которую пытались проэксплуатировать злоумышленники (CVE):

Так-как происходит атака, то атакующий должен физически как-то взаимодействовать с жертвой, а значит – отправлять какие-то данные, которые жертва будет обрабатывать.

Отфильтруем пакеты, в которых посылаются запросы с флагом синхронизации (Установки соединения).

`tcp.flags.syn == 1 && tcp.flags.ack == 0`

No.	Time	Source	Destination	Protocol	Length	Info
2	4.283223398	192.168.56.112	192.168.56.114	TCP	74	57386 → 135 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=113413876 TSecr=0 WS=128
11	4.293641282	192.168.56.112	192.168.56.114	TCP	74	33818 → 49670 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=113413886 TSecr=0 WS=128
24	4.301259208	192.168.56.112	192.168.56.114	TCP	74	57398 → 135 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=113413894 TSecr=0 WS=128
33	4.307081287	192.168.56.112	192.168.56.114	TCP	74	33826 → 49670 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=113413900 TSecr=0 WS=128
46	4.313685551	192.168.56.112	192.168.56.114	TCP	74	57410 → 135 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=113413906 TSecr=0 WS=128
55	4.319135335	192.168.56.112	192.168.56.114	TCP	74	33830 → 49670 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=113413912 TSecr=0 WS=128
68	4.325570562	192.168.56.112	192.168.56.114	TCP	74	57414 → 135 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=113413918 TSecr=0 WS=128
80	4.332304527	192.168.56.112	192.168.56.114	TCP	74	33844 → 49670 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=113413925 TSecr=0 WS=128
90	4.339415704	192.168.56.112	192.168.56.114	TCP	74	57418 → 135 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=113413932 TSecr=0 WS=128
117	4.347214156	192.168.56.112	192.168.56.114	TCP	74	33852 → 49670 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=113413940 TSecr=0 WS=128
129	4.354959294	192.168.56.112	192.168.56.114	TCP	74	57430 → 135 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=113413948 TSecr=0 WS=128
138	4.361584044	192.168.56.112	192.168.56.114	TCP	74	33868 → 49670 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=113413954 TSecr=0 WS=128

Наблюдаем стабильные попытки подключения **192.168.56.112** к **192.168.56.114** к портам:

**135, 445, 49670** и **49666** (в самом конце трафика)

Исходя из вышесказанного:

### Злоумышленник:

\* IP - **192.168.56.112**

### Жертва:

\* IP - **192.168.56.114**

\* Порты:

- **135**        **DCE/RPC**
- **445**        **SMB**
- **49670**     **RPC\_NETLOGON**
- **49666**     **???**

Подключение к **445** и **49666** порту произошло в конце трафика, а значит, **атаковать** вероятней всего могли по **135** и **49670** порту.

Начнём разбираться с событиями на **135** порту:

**tcp.port == 135 && ip.dst == 192.168.56.114**

No.	Time	Source	Destination	Protocol	Length	Info
130.	11.574482262	192.168.56.112	192.168.56.114	DCERPC	138	Bind: call_id: 1, Fragment: Single, 1 context items: EPMv4 V3.0 (32bit NDR)
130.	11.590213170	192.168.56.112	192.168.56.114	DCERPC	138	Bind: call_id: 1, Fragment: Single, 1 context items: EPMv4 V3.0 (32bit NDR)
131.	11.606284368	192.168.56.112	192.168.56.114	DCERPC	138	Bind: call_id: 1, Fragment: Single, 1 context items: EPMv4 V3.0 (32bit NDR)
131.	11.623765325	192.168.56.112	192.168.56.114	DCERPC	138	Bind: call_id: 1, Fragment: Single, 1 context items: EPMv4 V3.0 (32bit NDR)
131.	11.637339447	192.168.56.112	192.168.56.114	DCERPC	138	Bind: call_id: 1, Fragment: Single, 1 context items: EPMv4 V3.0 (32bit NDR)
132.	25.269436880	192.168.56.112	192.168.56.114	DCERPC	178	Bind: call_id: 1, Fragment: Single, 1 context items: ISystemActivator V0.0 (32bit NDR), NTLMSSP_NEGO
132.	25.270315440	192.168.56.112	192.168.56.114	DCERPC	436	AUTH3: call_id: 1, Fragment: Single, NTLMSSP_AUTH, User: VULN\Администратор
8	4.286868522	192.168.56.112	192.168.56.114	EPM	222	Map request, RPC_NETLOGON, 32bit NDR
30	4.304970115	192.168.56.112	192.168.56.114	EPM	222	Map request, RPC_NETLOGON, 32bit NDR
52	4.317351502	192.168.56.112	192.168.56.114	EPM	222	Map request, RPC_NETLOGON, 32bit NDR

Замечаем пакет аутентификации под учётной записью **Администратор** к нашей жертве. Посмотрим, что следовало дальше за этим пакетом:

13234	25.266313559	192.168.56.114	192.168.56.114	DCERPC	326 Bind ACK: call_id: 1, Fragment: Single, max_xmit: 4280 max_recv: 4280, 1 results: Acceptance, Ntl
13235	25.266332064	192.168.56.112	192.168.56.114	TCP	66 59302 → 135 [ACK] Seq=113 Ack=261 Win=64128 Len=0 TSval=113434859 TSecr=332601
13236	25.270315440	192.168.56.112	192.168.56.114	DCERPC	436 AUTH3: call_id: 1, Fragment: Single, NTLMSSP_AUTH, User: VULN\Администратор
13237	25.304010949	192.168.56.112	192.168.56.114	TCP	66 52474 → 445 [ACK] Seq=792 Ack=889 Win=64128 Len=0 TSval=113434897 TSecr=332597
13238	25.320707785	192.168.56.114	192.168.56.112	TCP	66 135 → 59302 [ACK] Seq=261 Ack=483 Win=66048 Len=0 TSval=332656 TSecr=113434863
13239	25.320721807	192.168.56.112	192.168.56.114	ISystemActivator	578 RemoteCreateInstance request
13240	25.338744637	192.168.56.114	192.168.56.112	ISystemActivator	10.. RemoteCreateInstance response
13241	25.345254721	192.168.56.112	192.168.56.114	TCP	74 35454 → 49666 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=113434938 TSecr=0 WS=128
13242	25.345441102	192.168.56.114	192.168.56.112	TCP	74 49666 → 35454 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM TSval=332681 TSecr=

Заметим, что после него появился пакет по протоколу **ISystemActivator** и происходит первое и последнее подключение к порту **49666**.

**ISystemActivator::RemoteCreateInstance** отвечает за вызов и загрузку объектов, а также за авторизацию клиента. Возвращается идентификатор процесса и номер порта, на котором будет происходить взаимодействие. Отсюда следует, что у злоумышленника **получилось зайти под учётной записью Администратор** и всё дальнейшее взаимодействие с жертвой велось по **49666** порту.

Атака прошла успешно, остаётся понять, за счёт чего злоумышленник получил доступ к жертве. Вернёмся к нашим портам и проанализируем передаваемые данные на **49670** порт.

`tcp.port == 49670 && ip.dst == 192.168.56.114`

No.	Time	Source	Destination	Protocol	Length	Info
13162	11.633234032	192.168.56.112	192.168.56.114	RPC_NETLOGON	198	NetrServerAuthenticate3 request
13182	11.646276209	192.168.56.112	192.168.56.114	RPC_NETLOGON	162	NetrServerReqChallenge request, VULN-DC
13184	11.647823012	192.168.56.112	192.168.56.114	RPC_NETLOGON	198	NetrServerAuthenticate3 request
13187	11.657770829	192.168.56.112	192.168.56.114	RPC_NETLOGON	682	NetrServerPasswordSet2 request [Malformed Packet]
11	4.293641282	192.168.56.112	192.168.56.114	TCP	74	33818 → 49670 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA

Замечаем помимо множества попыток авторизации **NetrServerAuthenticate3** и провалов, пакет с методом **NetrServerPasswordSet2**. Данный метод отвечает за установку пароля в службе **Active Directory**.

Рассмотрим данный пакет подробнее:

13187	11.657770829	192.168.56.112	192.168.56.114	RPC_NETLOGON	682 NetrServerPasswordSet2 request[Malformed Packet]
11	4.293641282	192.168.56.112	192.168.56.114	TCP	74 33818 → 49670 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=113413886 TSecr=0 M
16	4.293814289	192.168.56.112	192.168.56.114	TCP	66 33818 → 49670 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=113413886 TSecr=311629

  

> Frame 13187: 682 bytes on wire (5456 bits), 682 bytes captured (5456 bits) on interface eth0	0000	08 00 27 80 4d 7a 08 00	27 22 46 4f 08 00 45 00	..'.Mz...'FO..E..
> Ethernet II, Src: PcsCompu_22:46:4f (08:00:27:22:46:4f), Dst: PcsCompu_80:4d:7a (08:00:27:80:4d:7a)	0010	02 9c 3d e6 40 00 40 06	08 43 c0 a8 38 70 c0 a8	..=@.@..C..8p..
> Internet Protocol Version 4, Src: 192.168.56.112, Dst: 192.168.56.114	0020	38 72 b3 d2 c2 06 b4 ff	2d 9f 1c a7 40 b2 80 18	8r.....@....
> Transmission Control Protocol, Src Port: 46034, Dst Port: 49670, Seq: 301, Ack: 141, Len: 616	0030	01 f6 f4 c1 00 00 01 01	08 0a 06 c2 ab c2 00 04	.....h.....
> Distributed Computing Environment / Remote Procedure Call (DCE/RPC) Request, Fragment: Single	0040	de 08 05 00 00 03 10 00	00 00 68 02 00 00 03 00	.....h.....
> Microsoft Network Logon, NetrServerPasswordSet2	0050	00 00 50 02 00 00 00 00	1e 00 00 00 00 00 09 00	..p.....h.....
Operation: NetrServerPasswordSet2 (30)	0060	00 00 00 00 00 00 09 00	00 00 56 00 55 00 4c 00	.....V-U-L..
[Response in frame: 13188]	0070	4e 00 2d 00 44 00 43 00	24 00 00 00 06 00 08 00	N...D-C-\$. ..
NULL Pointer: Server Handle	0080	00 00 00 00 00 00 08 00	00 00 56 00 55 00 4c 00	.....V-U-L..
> unknown string	0090	4e 00 2d 00 44 00 43 00	00 00 00 00 00 00 00 00	N...D-C-.....
[Malformed Packet: RPC_NETLOGON]	00a0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	.....
	00b0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	.....
	00c0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	.....
	00d0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	.....
	00e0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	.....

Видно предупреждение **Malformed Packet: RPC NETLOGON** которое может быть связано с уязвимостью **ZeroLogon**. Убедимся, она ли была использована:

Посмотрим пакет аутентификации:

13184	11.647823012	192.168.56.112	192.168.56.114	RPC_NETLOGON	198 NetrServerAuthenticate3 request
13186	11.655661336	192.168.56.112	192.168.56.114	RPC_NETLOGON	110 NetrServerAuthenticate3 response
13187	11.657770829	192.168.56.112	192.168.56.114	RPC_NETLOGON	682 NetrServerPasswordSet2 request[Malformed Packet]
13188	11.658723510	192.168.56.112	192.168.56.114	RPC_NETLOGON	106 NetrServerPasswordSet2 response[Malformed Packet]
13221	25.247533084	192.168.56.112	192.168.56.114	SMB	139 Negotiate Protocol Request

  

> Internet Protocol Version 4, Src: 192.168.56.112, Dst: 192.168.56.114	0000	08 00 27 80 4d 7a 08 00	27 22 46 4f 08 00 45 00	..'.Mz...'FO..E..
> Transmission Control Protocol, Src Port: 46034, Dst Port: 49670, Seq: 169, Ack: 97, Len: 110	0010	00 b8 3d e5 40 00 40 06	0a 28 c0 00 00 00 00 00	.....
> Distributed Computing Environment / Remote Procedure Call (DCE/RPC) Request, Fragment: Single	0020	38 72 b3 d2 c2 06 b4 ff	2d 1b 1c 00 00 00 00 00	.....
> Microsoft Network Logon, NetrServerAuthenticate3	0030	01 f6 f2 dd 00 00 01 01	08 0a 06 c2 ab c2 00 04	.....h.....
Operation: NetrServerAuthenticate3 (26)	0040	de 06 05 00 00 03 10 00	00 00 68 02 00 00 03 00	.....h.....
[Response in frame: 13186]	0050	00 00 6c 00 00 00 00 00	1a 00 be 00 00 00 00 00	.....
> Server Handle: \\VULN-DC	0060	00 00 00 00 00 00 00 00	0a 00 00 00 00 00 5c	.....
> Acct Name: VULN-DC\$	0070	55 00 4c 00 4e 00 2d 00	44 00 43 00 00 00 00 00	.....
Sec Chan Type: SEC_CHAN_BDC (6)	0080	00 00 00 00 00 00 09 00	00 00 56 00 00 00 00 00	.....
> Computer Name: VULN-DC	0090	4e 00 2d 00 44 00 43 00	24 00 00 00 00 00 08 00	.....
Client Credential: 0000000000000000	00a0	00 00 00 00 00 00 08 00	00 00 56 00 00 00 00 00	.....
> Negotiation options: 0x212fffff	00b0	4e 00 2d 00 44 00 43 00	00 00 00 00 00 00 00 00	.....
	00c0	00 00 ff ff 2f 21		.....

Видим учётные данные клиента **0000000000000000**

13187	11.657770829	192.168.56.112	192.168.56.114	RPC_NETLOGON	682 NetrServerPasswordSet2 request[Malformed Packet]
11	4.293641282	192.168.56.112	192.168.56.114	TCP	74 33818 → 49670 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=113413886 TSecr=0 W
16	4.293814289	192.168.56.112	192.168.56.114	TCP	66 33818 → 49670 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=113413886 TSecr=311629

  

> Frame 13187: 682 bytes on wire (5456 bits), 682 bytes captured (5456 bits) on interface eth0	0000	08 00 27 80 d4 7a 08 00	27 22 46 4f 08 00 45 00	..Mz.. "FO..E..
> Ethernet II, Src: PcsCompu_22:46:4f (08:00:27:22:46:4f), Dst: PcsCompu_80:4d:7a (08:00:27:80:4d:7a)	0010	02 9c 3d e6 40 00 40 06	08 43 c0 a8 38 70 c0 a8	..=@..C..8p..
> Internet Protocol Version 4, Src: 192.168.56.112, Dst: 192.168.56.114	0020	38 72 b3 d2 c2 06 b4 ff	2d 9f 1c a7 40 b2 80 18	8r.....@....
> Transmission Control Protocol, Src Port: 46034, Dst Port: 49670, Seq: 301, Ack: 141, Len: 616	0030	01 f6 f4 c1 00 00 01 01	08 0a 06 c2 ab c2 00 04	.....h.....
> Distributed Computing Environment / Remote Procedure Call (DCE/RPC) Request, Fragment: Single	0040	de 08 05 00 00 03 10 00	00 00 68 02 00 00 03 00	.....h.....
> Microsoft Network Logon, NetrServerPasswordSet2	0050	00 00 50 02 00 00 00 00	1e 00 00 00 00 00 09 00	..P.....
Operation: NetrServerPasswordSet2 (30)	0060	00 00 00 00 00 00 09 00	00 00 56 00 55 00 4c 00	.....V-U-L..
[Response in frame: 13188]	0070	4e 00 2d 00 44 00 43 00	24 00 00 00 06 00 08 00	N...D-C..\$. ..
NULL Pointer: Server Handle	0080	00 00 00 00 00 00 08 00	00 00 56 00 55 00 4c 00	.....V-U-L..
> unknown string	0090	4e 00 2d 00 44 00 43 00	00 00 00 00 00 00 00 00	N...D-C.....
> [Malformed Packet: RPC_NETLOGON]	00a0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	.....
	00b0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	.....
	00c0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	.....
	00d0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	.....
	00e0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	.....

Видим, что методу **NetrServerPasswordSet2** передаются данные, в которых 516 байт – пустые, а остальные 8 – тоже.

Всё это характерно для **уязвимости Zerologon (CVE-2020-1472)**. Она позволила получить доступ к учётной записи **Администратор**

Ответ: **Zerologon (CVE-2020-1472)**

Наглядный KillChain всей атаки:

(слева – направо и заново)



## 2) Определить предполагаемый хактул который пытались использовать злоумышленники:

Zerologon можно эксплуатировать с помощью **эксплоитов**, например ([risksense/zerologon: Exploit for zerologon cve-2020-1472 \(github.com\)](https://github.com/risksense/zerologon-exploit)), либо с помощью готовых сборок решений, на подобии **impacket + mimikatz**. Также для подключения к жертве с помощью хэша могло использоваться **Evil-WinRM** ([Hackplayers/evil-winrm: The ultimate WinRM shell for hacking/pentesting \(github.com\)](https://github.com/Hackplayers/evil-winrm)) и подобные решения.

**Ответ:**     **Exploit | Impacket и Evil-WinRM** (возможно другое, но подобное этому)

## 3) Описать контрмеры, позволяющие исключить возможность использования уязвимости в будущем

**Microsoft** пропатчили эту уязвимость - [How to manage the changes in Netlogon secure channel connections associated with CVE-2020-1472 - Microsoft Support](https://support.microsoft.com/en-us/topic/how-to-manage-the-changes-in-netlogon-secure-channel-connections-associated-with-cve-2020-1472-2021-02-02)

И если верить описанию, то после февраля 2021 года протокол был переработан проблема с несовместимостью была устранена.

Создатели протокола рекомендуют:

- Обновить контроллеры домена
- Включить принудительный режим обращения к данной уязвимости
- Устранить несоответствующие устройства

**Ответ: Обновить контроллер домена, устранить несоответствующие устройства и включить принудительный режим.**