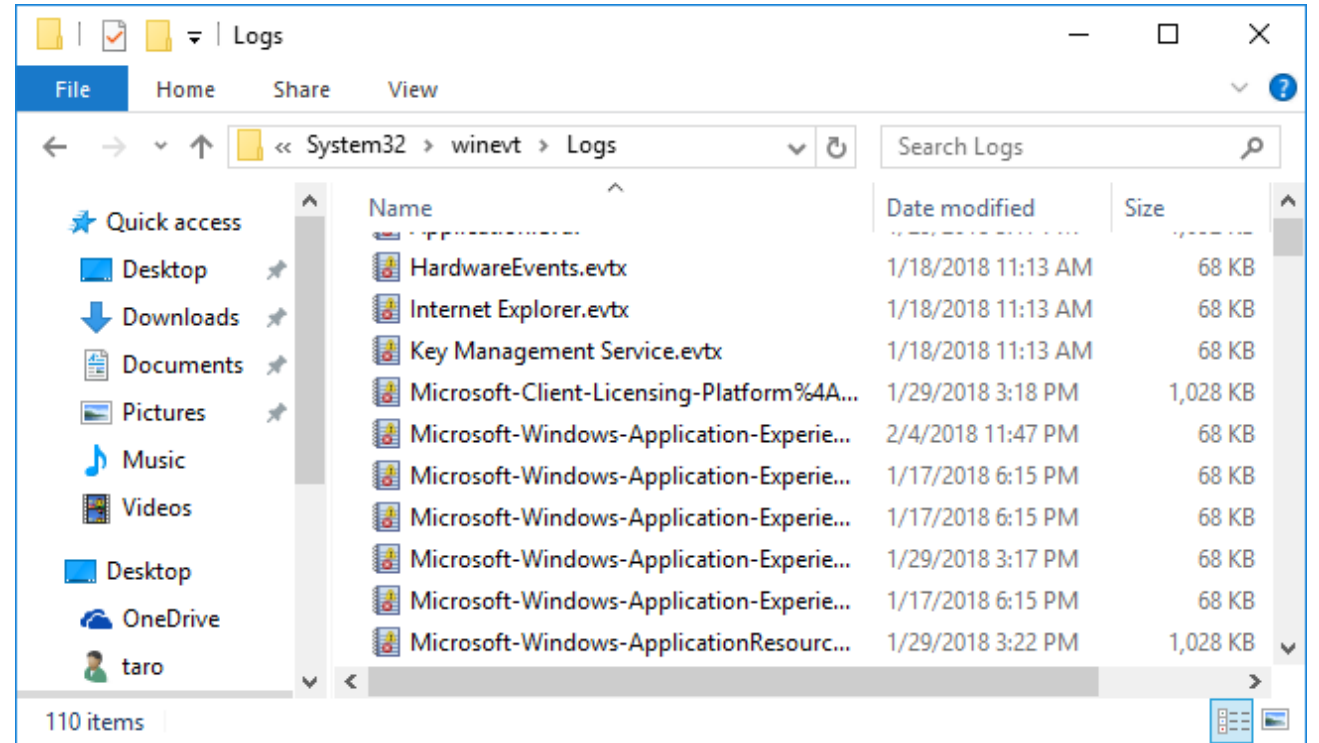


# Event Log Analysis

# Event Log 101

- What is Event Log?
  - Windows version of “syslog”.



- Where are these artifacts located in?
  - %SystemRoot%\System32\winevt\Logs
    - %SystemRoot% is “C:\Windows” typically.

# Event Log 101

- There are three standard logs and lots of custom logs.

## Standard logs

- Security
- System
- Application

## Custom logs (Applications and Services Logs)

- RDP
- PowerShell
- Windows Firewall
- ...

# Event Log 101

- Each log contains following items.

- Source
- Event ID
- Level
  - Information / Warning / Error
- User
  - The target user of a event's message.
- Date and Time
- Computer
  - The target host of a event's message.
- Description
  - The details are described in this un-normalized field!

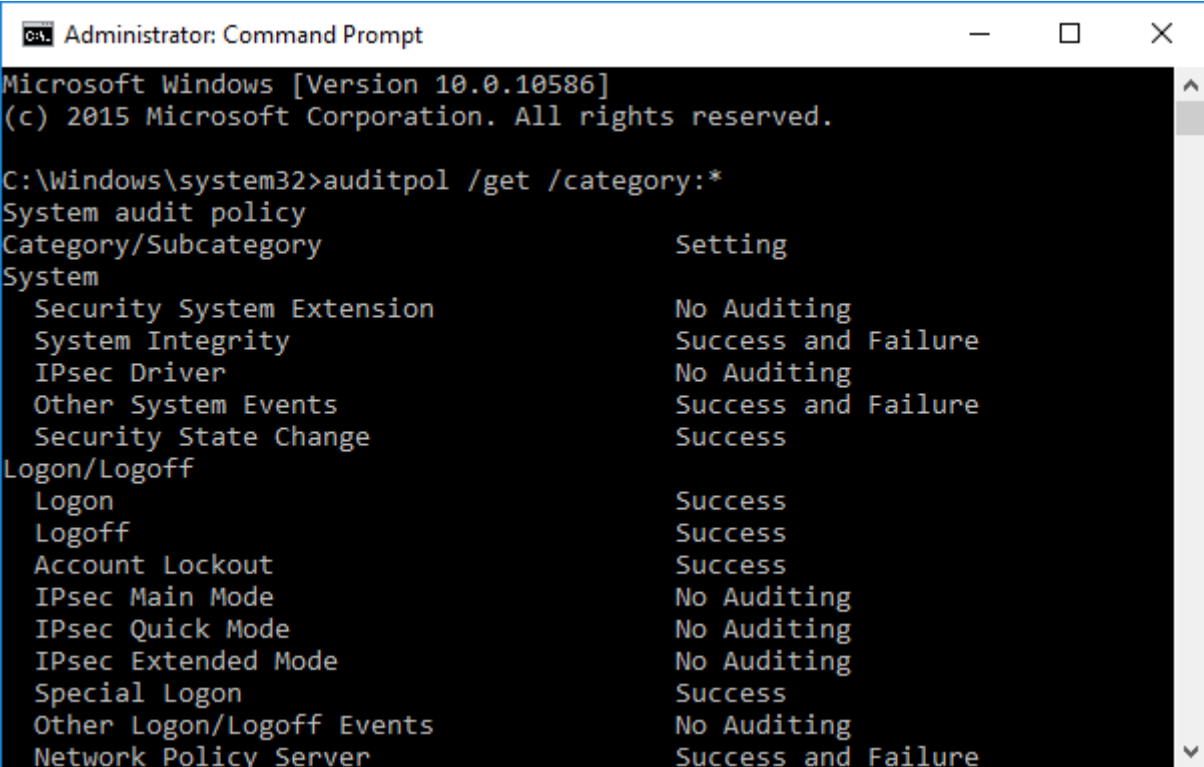
- The event ID number is unique within each log, such as System, Security, Application, and other custom logs. However, the same ID number may be used if the log is different.

The screenshot displays the Windows Event Viewer interface. The 'General' tab is selected, showing a message: 'An account was successfully logged on.' Below this, the 'Subject' section lists: Security ID: SYSTEM, Account Name: DESKTOP-SHCTJ7L\$, and Account Domain: WORKGROUP. The 'Details' tab is also visible, showing a list of event properties: Log Name: Security, Source: Microsoft Windows security, Event ID: 4624, Level: Information, User: N/A, OpCode: Info, Logged: 3/6/2018 5:52:16 PM, Task Category: Logon, Keywords: Audit Success, and Computer: DESKTOP-SHCTJ7L\$. A link for 'More Information: Event Log Online Help' is provided at the bottom.

An account was successfully logged on.			
Subject:			
Security ID:	SYSTEM		
Account Name:	DESKTOP-SHCTJ7L\$		
Account Domain:	WORKGROUP		
Log Name:	Security		
Source:	Microsoft Windows security	Logged:	3/6/2018 5:52:16 PM
Event ID:	4624	Task Category:	Logon
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	DESKTOP-SHCTJ7L
OpCode:	Info		
More Information:	<a href="#">Event Log Online Help</a>		

# Event Log 101

- Audit policy
  - For security log, all logs are not enabled by default. “Audit policy” manages this.
  - You can confirm/edit the current audit policy with these applications/ commands.
    - localpol.msc (online)
    - gpedit.msc (online)
    - auditpol (online)
    - Regripper auditpol plugin (offline)
    - Volatility auditpol plugin (offline)
- Refs
  - <http://www.kazamiya.net/en/PolAdtEv>
  - <https://github.com/keydet89/RegRipper2.8/blob/master/plugins/auditpol.pl>
  - <https://github.com/volatilityfoundation/volatility/blob/master/volatility/plugins/registry/auditpol.py>



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Windows\system32>auditpol /get /category:*
System audit policy
Category/Subcategory                Setting
System
  Security System Extension          No Auditing
  System Integrity                   Success and Failure
  IPsec Driver                       No Auditing
  Other System Events                Success and Failure
  Security State Change              Success
Logon/Logoff
  Logon                              Success
  Logoff                             Success
  Account Lockout                    Success
  IPsec Main Mode                    No Auditing
  IPsec Quick Mode                   No Auditing
  IPsec Extended Mode                No Auditing
  Special Logon                      Success
  Other Logon/Logoff Events          No Auditing
  Network Policy Server              Success and Failure
```

# Event Log 101

- There are lots of tools to view and/or parse event logs.
  - Event Viewer (default)
  - PowerShell (default)
  - Event Log Explorer (commercial) [1]
  - python-evtX [2]
  - EvtXtract [3]
  - EvtX Parser [4]
  - LibevtX [5]
  - Log Parser [6]

# Event Log 101

- Before we dive into the event log world, we should discuss two basic authentication protocols for Windows.

## Kerberos

- The default authentication protocol for Windows domain networks.
- But, if a session starts with IP address instead of host name, the NTLM authentication is used.

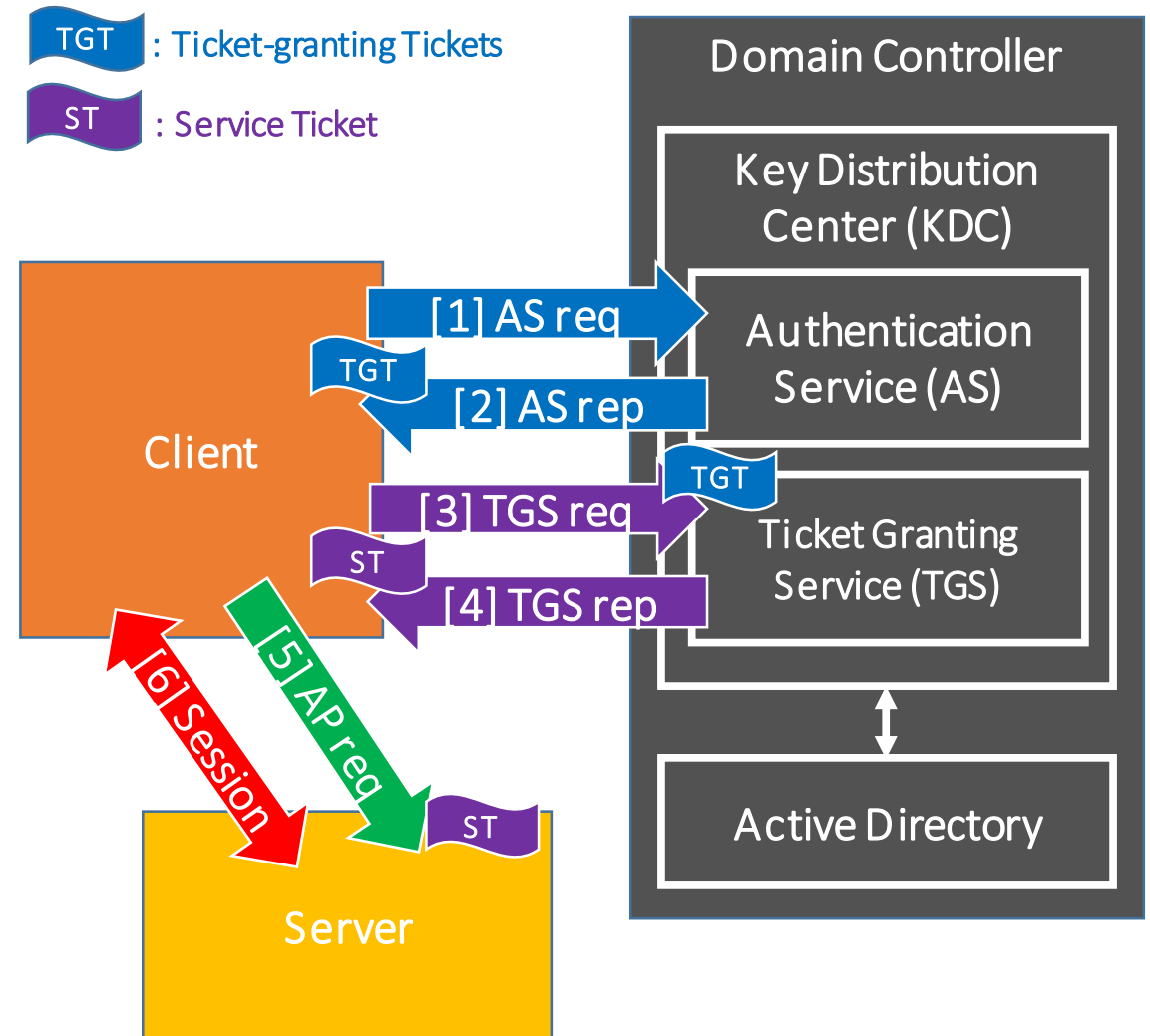
## NTLM

- A traditional authentication protocol.

# Event Log 101

- Kerberos Authentication Mechanism

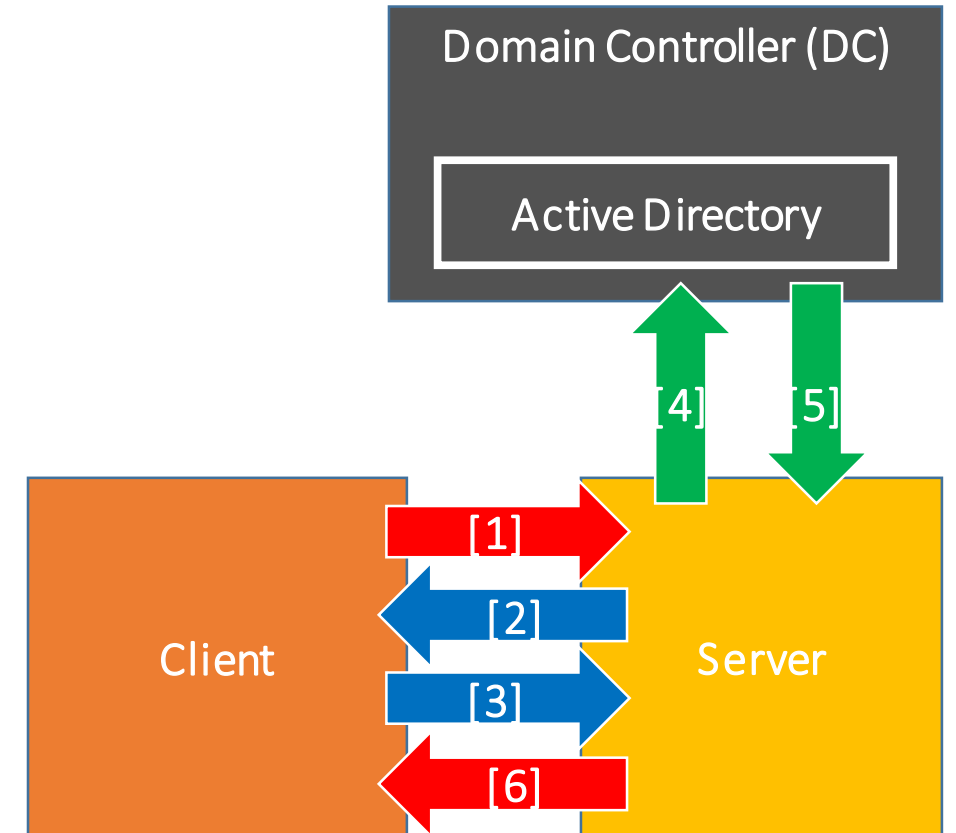
1. A user on client requests a Ticket-granting Tickets (TGT)
2. The Authentication Service (AS) sends a TGT, which is encrypted with password hash of the user.
3. The client decrypt the TGT and send it to Ticket Granting Service (TGS) for a Service Ticket.
4. The TGS sends the Service Ticket to the client.
5. The client send the Service Ticket to the server.
6. Then a service session start.





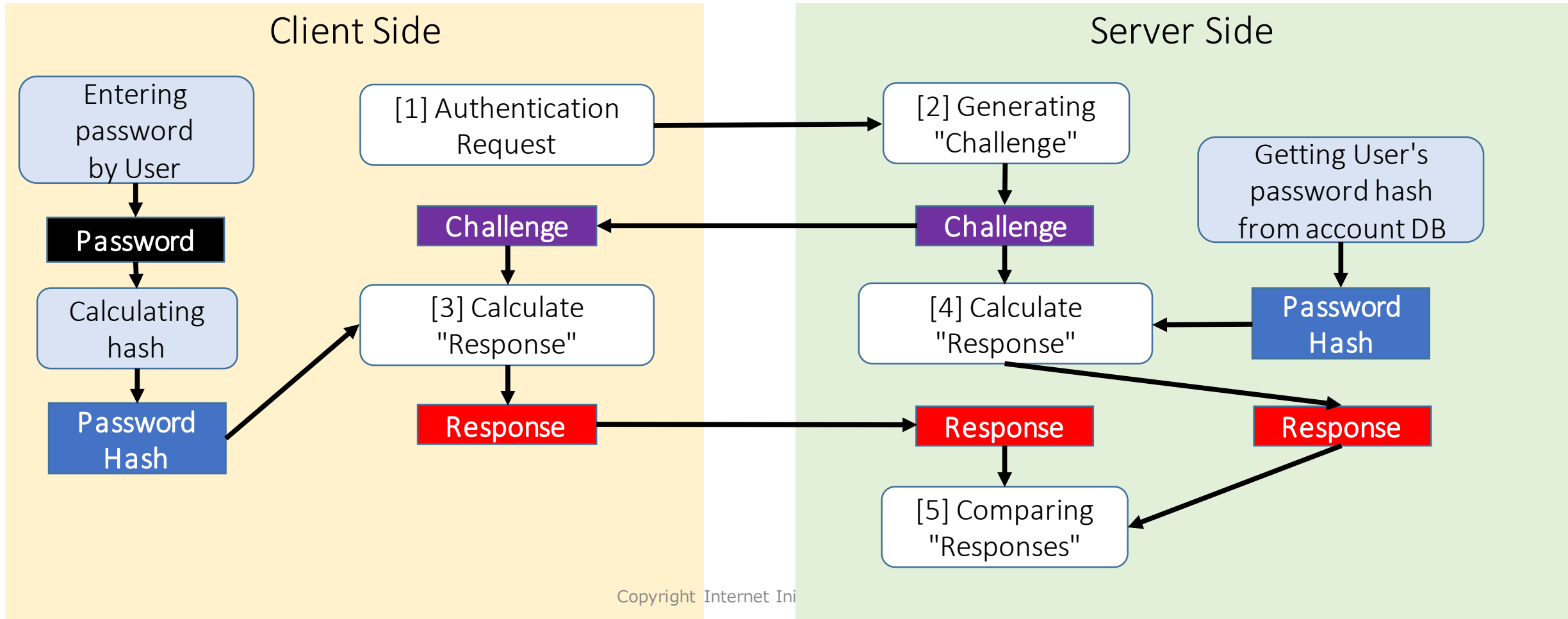
# Event Log 101

- NTLM Authentication Mechanism
  1. A client requests access to a server.
  2. The server respond challenge message to the client.
  3. Clients sends response message to the server.
  4. The server sends challenge and response messages to the Domain Controller (DC).
  5. The DC confirms them to authenticate the user. If the authentication was successful, the DC sends to the server the confirmation that the user was authenticated.
  6. The server respond to the client to start a service.



# Event Log 101

- Challenge Response Authentication Basic



# Event Log 101

- The most important logs for incident response are...
  - Credential validation (Authentication, Account Logon)
    - 4768: requested a TGT
    - 4769: requested a Service Ticket
    - 4776: NTLM authentication
  - Logon (Authorization?)
    - 4624: Logon
    - 4625: Logoff
    - 4634: Logon Failed (not default)
- These all events are logged in the standard "Security" log.

} Kerberos related

# Event Log 101

- 4768: requested a TGT
  - This event logged on the Domain Controller. And both of success and failure requests are logged.

Event Properties - File: C:\Users\ttaro\Desktop\Security.evtx

Standard

Date:	2/8/2018	Source:	Microsoft-Windows-Security-Auditing
Time:	2:27:03 PM	Category:	Kerberos Authentication Service
Type:	Audit Success	Event ID:	4768
User:	N/A		
Computer:	AD-WIN2016.ninja-motors.net		

Description:

A Kerberos authentication ticket (TGT) was requested.

Account Information:

Account Name:	ninja-rdp
Supplied Realm Name:	ninja-motors.net
User ID:	S-1-5-21-3671970501-3975728774-4289435121-3102

Service Information:

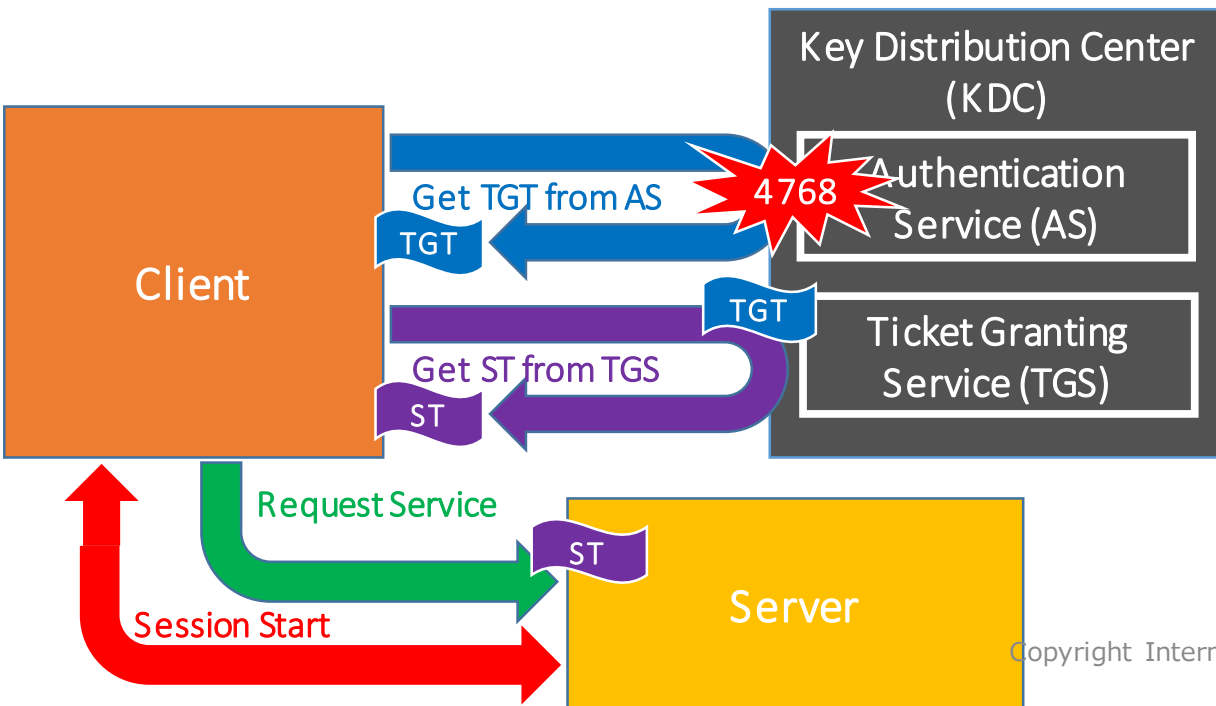
Service Name:	krbtgt
Service ID:	S-1-5-21-3671970501-3975728774-4289435121-502

Network Information:

Client Address:	::ffff:192.168.52.40
-----------------	----------------------

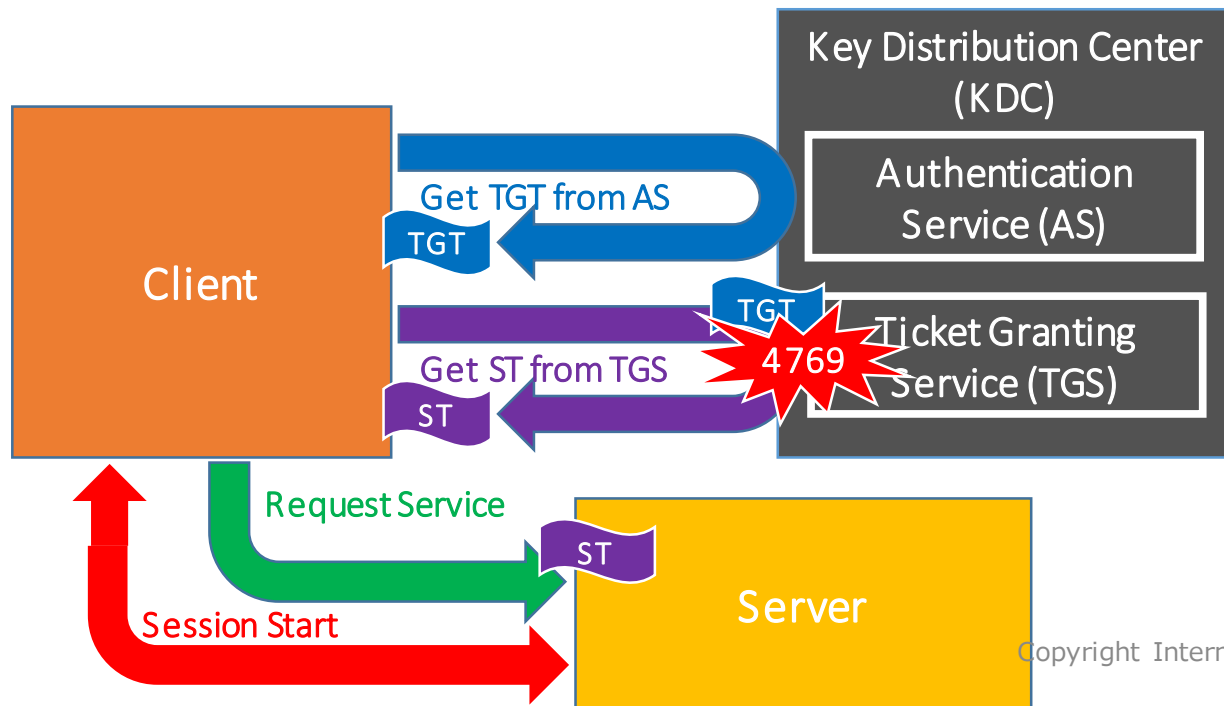
Data:  Bytes  Words  D-Words

Lookup in:



# Event Log 101

- 4769: requested a Service Ticket
  - This event is logged on the Domain Controller. Both succeeded and failed requests are logged.



Event Properties - File: C:\Users\ttaro\Desktop\Security.evtx

Standard

Date:	2/8/2018	Source:	Microsoft-Windows-Security-Auditing
Time:	2:27:03 PM	Category:	Kerberos Service Ticket Operations
Type:	Audit Success	Event ID:	4769
User:	N/A		
Computer:	AD-WIN2016.ninja-motors.net		

Description:

A Kerberos service ticket was requested.

Account Information:

Account Name:	ninja-rdp@NINJA-MOTORS.NET
Account Domain:	NINJA-MOTORS.NET
Logon GUID:	{28CC0EE2-3A76-6B76-DFA1-3C1158C32DF4}

Service Information:

Service Name:	CLIENT-WIN10-1\$
Service ID:	S-1-5-21-3671970501-3975728774-4289435121-2601

Network Information:

Client Address:	::ffff:192.168.52.40
-----------------	----------------------

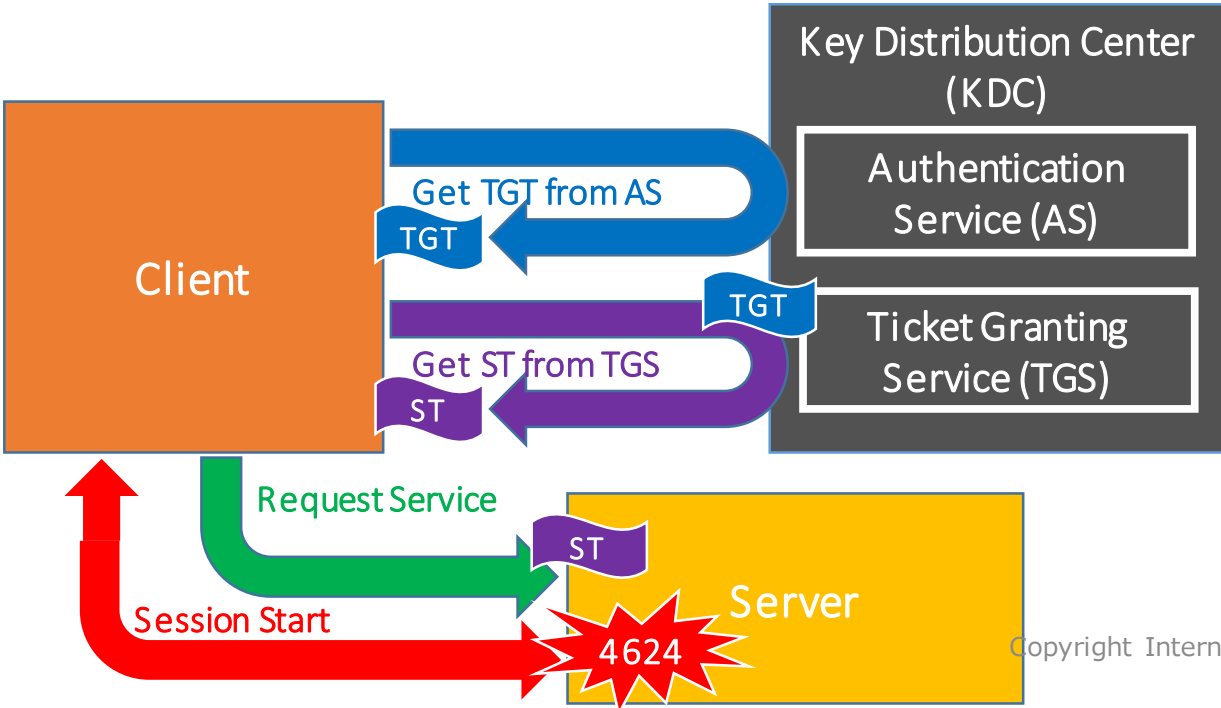
Data:  Bytes  Words  D-Words

Lookup in:

# Event Log 101

- 4624: Logon
  - This event documents successful logon attempt to various components on the local computer.
  - This event also indicates "logon type".

Date:	2/8/2018	Source:	Microsoft-Windows-Security-Auditing
Time:	2:27:03 PM	Category:	Logon
Type:	Audit Success	Event ID:	4624
User:	N/A		
Computer:	client-win10-1.ninja-motors.net		
Description:			
An account was successfully logged on.			
Subject:			
Security ID:	S-1-5-18		
Account Name:	CLIENT-WIN10-1\$		
Account Domain:	NINJA-MOTORS		
Logon ID:	0x3e7		
Logon Information:			
Logon Type:	10		
Restricted Admin Mode:	No		
Virtual Account:	No		
Elevated Token:	No		
Impersonation Level:	Impersonation		
New Logon:			
Security ID:	S-1-5-21-3671970501-3975728774-4289435121-3102		
Account Name:	ninja-rdp		
Account Domain:	NINJA-MOTORS		
Logon ID:	0x3a392b		
Linked Logon ID:	0x0		
Network Account Name:	-		
Network Account Domain:	-		
Logon GUID:	{28CC0EE2-3A76-6B76-DFA1-3C1158C32DF4}		
Process Information:			
Process ID:	0x3e8		
Process Name:	C:\Windows\System32\svchost.exe		
Network Information:			
Workstation Name:	CLIENT-WIN10-1		
Source Network Address:	192.168.52.44		



# Event Log 101

- What is “logon type”?
  - Interactive (2)
  - Network (3)
  - Batch (4)
  - Service (5)
  - Proxy (6)
  - Unlock (7)
  - NetworkCleartext (8)
  - NewCredentials (9)
  - RemoteInteractive (10)
  - CachedInteractive (11)
  - CachedRemoteInteractive (12)
  - CachedUnlock (13)

<https://msdn.microsoft.com/en-us/library/aa394189.aspx>

# Event Log 101

- What is “logon type”?
  - Interactive (2)
    - For Local logon with a user credential.
    - For example, if you sit in front of your PC, press Ctrl+Alt+Del keys, and type your user name and password; the log will be produced when the logon is attempted.
  - Network (3)
    - This is the most generic logon type. This type of logon is used for SSO (Single-Sign-On). You don't need to input any additional credentials if you have already had a rights to use services (E.g. connecting to a file server with SMB).
  - Batch (4)
    - For Task Scheduler and AT.
  - Service (5)
    - For Windows Services.



# Event Log 101

- What is “logon type”?
  - Unlock (7)
    - For unlocking the screen lock.
  - RemoteInteractive (10)
    - For RDP.
  - CachedInteractive (11)
    - If the machine cannot communicate with the domain controllers and if you have logged on to the machine in the past, this type is logged when you log on in that situation.
      - E.g. If you take your laptop out with you, and log on to the laptop with a domain account offline.
  - CachedRemoteInteractive (12)
    - A similar situation to 11, but logged for RDP.
  - CachedUnlock (13)
    - A similar situation to 11, but logged for unlocking screen.

# Event Log 101

- There are three "account types" for account/user names logged in Events.
  - User accounts
    - Its just user account. Generally this type of accounts are bind to each person or roll.
  - Computer accounts
    - This account type indicates each host. A name of this account type is terminated with character "\$". For example, "DESKTOP-SHCTJ7L\$" is a name of a computer account.
  - Service accounts
    - Each service account is created to be owner of a certain service. For example, IUSR is the owner of IIS, and krbtgt is the owner of a service that is a part of Key Distribution Center.

# Remote Logon Events

# Remote Logon Events

- There are a lot of remote logon methods that are used by attackers for Windows.
  - RDP
  - Task Scheduler/AT
  - Powershell Remoting
  - WinRS
  - WMIC
  - PsExec
  - Wmiexec
  - ...

RDP

# RDP (1)

- Why this event is important?
  - Attackers sometimes use RDP to logon to remote computers while users are away from clients, or to penetrate servers. So, you should check this event.
- Important event IDs
  - Security.evtx
    - 4624: An account was successfully logged on.
    - 4648: A logon was attempted using explicit credentials.
    - 4778: A session was reconnected to a Window Station. (Not default)
    - 4779: A session was disconnected from a Window Station. (Not default)
  - Microsoft-Windows-TerminalServices-RemoteConnectionManager%4Operational.evtx
    - 1149: User authentication succeeded
    - 21: Remote Desktop Services: Session logon succeeded
    - 24: Remote Desktop Services: Session has been disconnected
    - 25: Remote Desktop Services: Session reconnection succeeded

# RDP (2)

- How can we detect this event?
  - Logon with RDP
    - 4624 (Security.evtx)
      - Description
        - An account was successfully logged on.
      - How can we recognize RDP logon with this ID?
        - Filter with these logon types in this ID.
          - Logon type 10 (RemoteInteractive) or type 12 (CachedRemoteInteractive)
      - Why?
        - RemoteInteractive (10) and CachedRemoteInteractive (12) indicate RDP used clearly because these logon types are dedicated for RDP usage.

# RDP (3)

- How can we detect this event?

- Logon with RDP

- 4648 (Security.evtx)

- Description

- A logon was attempted using explicit credentials.

- How can we recognize RDP logon with this ID?

- Find events with the following conditions.
      - Filter out computer accounts and localhost.
      - Filter out included SPNs or filter with "TERMSERV/".

- Why?

- If a user inputs a credential clearly when the user logs on to remote machines with RDP, then this ID is logged at the source machine.
      - But when "Restricted Admin mode" is used, this ID is not logged for the admin accounts.
    - This event ID logs SPNs (Service Principal Name) that indicates service names which a user wants to use. And SPN for RDP is "TERMSERV" or any SPNs are NOT included for RDP and several cases (E.g. local logon).

Date:	2/8/2018	Source:	Micros
Time:	2:49:52 PM	Category:	Logon
Type:	Audit Success	Event ID:	4648
User:	N/A		
Computer:	client-win10-1.ninja-motors.net		
Description:	A logon was attempted using explicit credentials.		
subject:	Security ID: S-1-5-18		
<b>This message is not related to RDP since its SPN indicates the CIFS service.</b>			
Account Whose Credentials Were Used:			
Account Name:	ninja-master		
Account Domain:	NINJA-MOTORS.NET		
Logon GUID:	{F47280CC-5ADA-C2		
Target Server:	Target Server Name: ad-win2016		
	Additional Information: cifs/ad-win2016		

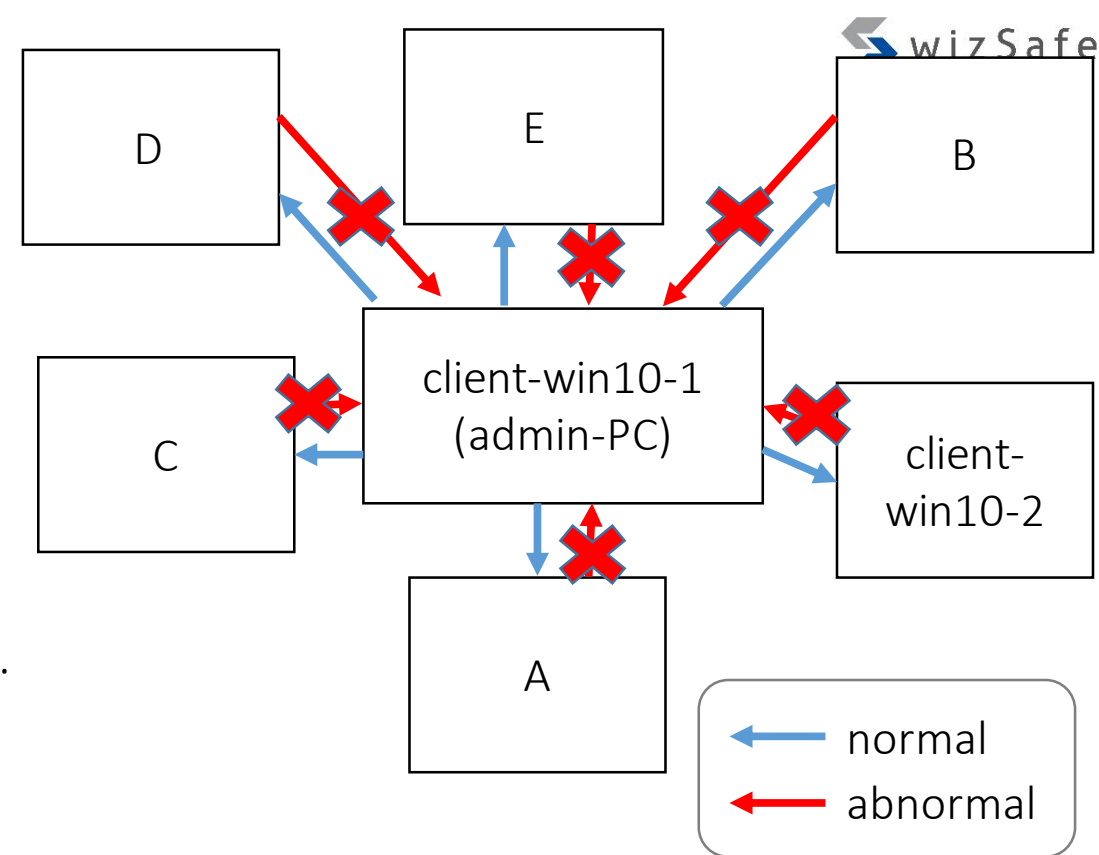


# RDP (4)

- Let's assume these conditions are given.

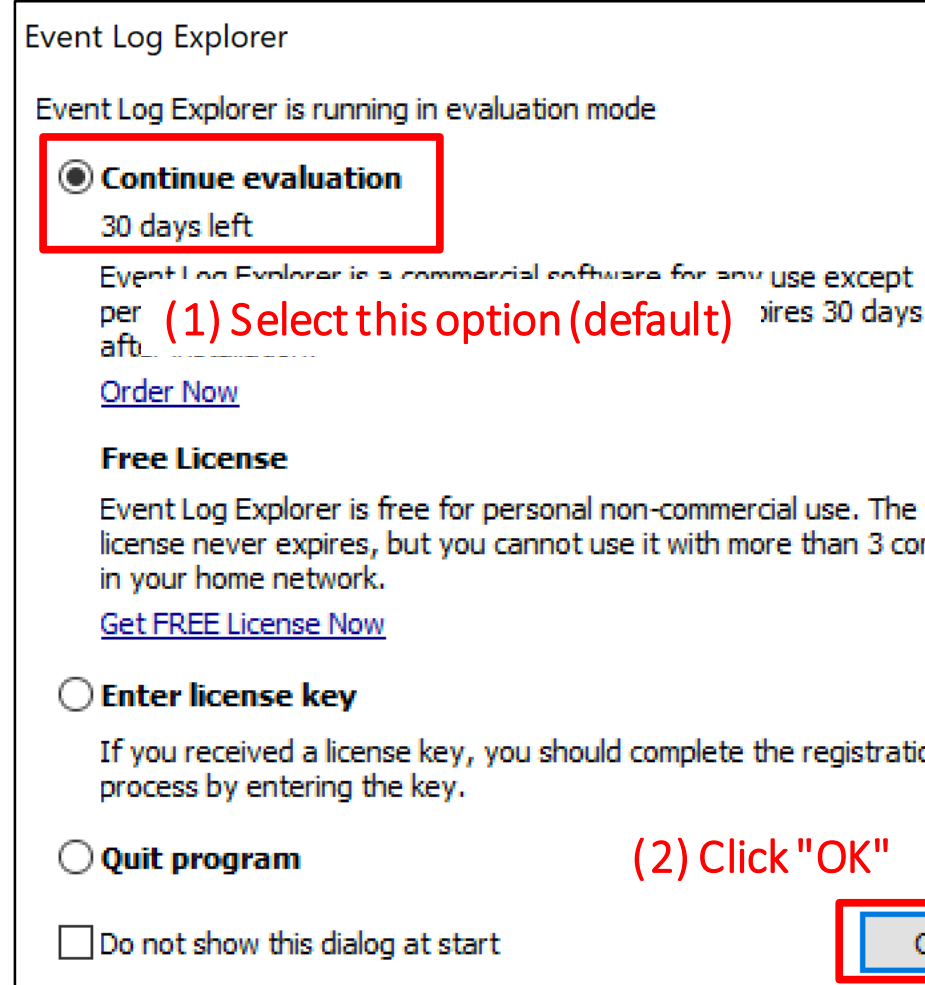
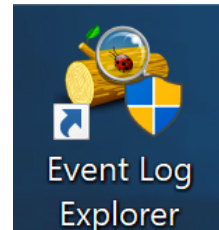
- client-win10-1 (192.168.52.40)
  - Administrator's PC
  - He uses toyoda, ninja-rdp, ninja-master accounts.
- client-win10-2 (192.168.52.44)
  - Honda's PC
  - He is a general employee and he don't have any admin rights.
  - He uses only this PC and "honda" account.

- The owner of the "client-win10-1" often use RDP to logon to remote hosts. But not vise versa.
- Since event ID 4624 is recorded on the target host, which is the destination host when it was logged on from a remote host, let's check "client-win10-1" first to see if there are any logons from a remote host is recorded.



# RDP (5)

- Open the below log with Event Log Explorer.
  - Training\_Materials\EventLogAnalysis\RDP\Win10-1\_Security.evtx
    - Original log file name : Security.evtx
- Notice:
  - You should **drag the log file and drop it to** the Event Log Explorer.
  - If you double-click the log file, Event Viewer, which is the Windows' default log viewer, starts instead. The viewer is not capable of complex filtering.



# RDP (6)

- Click the “Filter Events” button.



# RDP (7)

Filter

Apply filter to:

Active event log view (File: E:\first\_tc\_2018\evtx\win10-1\Logs\Security.evtx)

Event log view(s) on your choice

Event types

Information

Warning

Error

Critical

Audit Success

Audit Failure

Source:   Exclude

Category:   Exclude

User:   Exclude

Computer:   Exclude

Event ID(s):

4624  Exclude

Enter ID numbers and/or ID ranges, separated by commas, use exclamation mark to exclude criteria (e.g. 1-19,100,250-450!10,255)

Text in description:

Logon Type:[\t\s]\*10[\r\n\s]\*|Logon Type:[\t\s]\*12[\r\n\s]  RegExp  Exclude

Filter by description params (for security event logs, e.g. Object\Object Name contains elcx.exe)

New condition Delete condition Clear list

Name	Operator	Value

Date  Time  Separately

From: 2/25/2018 12:00:00 AM To: 2/25/2018 12:00:00 AM  Exclude

Display event  hours  Exclude

Clear **Load...** Save... OK Cancel

(2) Choose "Training\_Materials\EventLogAnalysis\RDP\Sec4624\_rdp.elc", then click "Open" button.

(1) Click "Load" button.

# RDP (8)

Filter

Apply filter to:

Active event log view (File: E:\first\_tc\_2018\evtx\win10-1\Logs\Security.evtx)

Event log view(s) on your choice

Event types

Information

Warning

Error

Critical

Audit Success

Source:   Exclude

Category:   Exclude

User:   Exclude

Computer:   Exclude

Event ID(s):

Exclude

Enter ID numbers:  Mark to exclude criteria (e.g. 1-19,100,250-450!10,255)

Text in description:

RegExp  Exclude

Filter by description params (for security event logs, e.g. Object\Object Name contains elx.exe)

New condition Delete condition Clear list

Name	Operator	Value

Date  Time  Separately

From:   To:    Exclude

Display event for the last  days  hours  Exclude

Clear Load... Save... OK Cancel

Filter with Event ID 4624.

Filter with logon type 10 or 12.

# RDP (9)

- How To Analyze
  - Logon with RDP

Event ID	Log Location	Logged Host	Where You Should Look	What You Get
4624	Security.evtx	Destination (remote host)	Date, Time	Date/Time around RDP used
			Computer Name	Destination computer name
			New Logon\Security ID	Logon user's SID
			New Logon\Account Name	Logon user's account name
			New Logon\Logon ID	An ID to combine with 4648 and others
			New Logon\Logon GUID	An ID to combine with 4769
			Network Information\Source Network Address	Source IP address

R

Event Log Explorer

File Tree View Event Advanced Window Help

Security.evtx

Filtered: showing 1 of 20634 event(s) NT

Type	Date	Time	Event	Source	Category	User
Audit Success	2/8/2018	2:27:03 PM	4624	Microsoft-Windows-Se	Logon	N/A

Description

Logon Information:

- Logon Type: 10
- Restricted Admin Mode: No
- Virtual Account: No
- Elevated Token: No

Impersonation Level: Impersonation

New Logon:

- Security ID: S-1-5-21-3671970501-3975728774-4289435121-3102
- Account Name: ninja-rdp
- Account Domain: NINJA-MOTORS
- Logon ID: 0x3a392b
- Linked Logon ID: 0x0
- Network Account Name: -
- Network Account Domain: -
- Logon GUID: {28CC0EE2-3A76-61

Process Information:

- Process ID: 0x3e8
- Process Name: C:\Windows\System

Network Information:

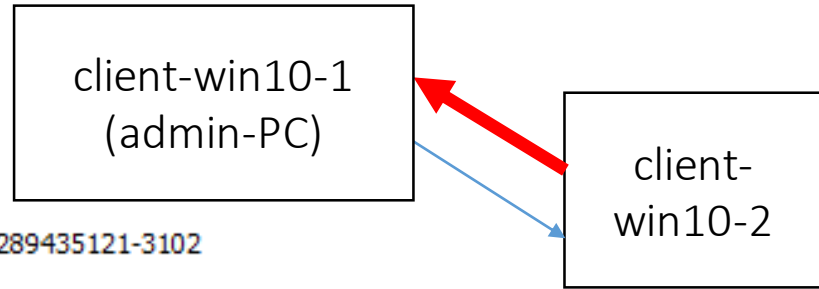
- Workstation Name: CLIENT-WIN10-1
- Source Network Address: 192.168.52.44
- Source Port: 0

Detailed Authentication Information:

Description Data

Events: 20634 Displayed: 1 Selected: 1

This message logged on client-win-10-1 which is the destination of this RDP Session.



ninja-rdp account logged on to "client-win10-1" which is the administrator's PC from 192.168.52.44 with RDP.

It's suspicious logon!

The destination host

ID 4624 is always logged on the destination host.

# RDP (11)

- If the attackers do not use RestrictedAdmin mode when they logon to remote servers, event ID 4648 is logged on the both source and destination hosts because they need to input a credential to use RDP. Let's check this.
- Open the below log with Event Log Explorer, and click "Filter Events" button.
  - Training\_Materials\EventLogAnalysis\RDP\Win10-2\_Security.evtx
    - Original log file name : Security.evtx

Notice:

You should **drag the log file and drop it to** the Event Log Explorer.





RDP (

Filter

Apply filter to:

Active event log view (File: C:\Users\taro\Desktop\Artifacts\evtx\remote\_logon\RDP\W

Event log view(s) on your choice

Event types

Information

Warning

Error

Critical

Audit Success

Audit Failure

Source:   Exclude

Category:   Exclude

User:   Exclude

Computer:   Exclude

Event ID(s):

4648  Exclude

Enter ID numbers and/or ID ranges, separated by comas, use exclamation mark to exclude criteria (e.g. 1-19,100,250-450! 10,255)

Text in description:

RegExp  Exclude

Filter by description params (for security event logs, e.g. Object\Object Name contains elcx.exe)

New condition Delete condition Clear list

Name	Operator	Value
Target Server\Target Server Name	Not equal	localhost
Account Whose Credentials Were Used\Account Name	Does not contain	\$
Target Server\Additional Information	Does not contain	/

Display event for the last 14 days  Exclude

Clear **Load...** Save... OK Cancel

(2) Choose "Training\_Materials\EventLogAnalysis\RDP\Sec4648\_rdp\_src.elc", then click "Open" button.

(1) Click "Load" button.

# RDP (

Filter

Apply filter to:

Active event log view (File: C:\Users\taro\Desktop\Artifacts\evtx\remote\_logon\RDP\W)

Event log view(s) on your choice

Event types

Information

Warning

Error

Critical

Audit Success

Source:   Exclude

Category:   Exclude

User:   Exclude

Computer:   Exclude

Event ID(s):

Exclude

Enter ID numbers and/or ID ranges, separated by comas, use exclamation mark to exclude criteria (e.g. 1-19,100,250-450! 10,255)

Text in description:

RegExp  Exclude

Filter by description params (for s...)

New condition Delete cond

Name	Operator	Value
Target Server\Target Server Name	Not equal	localhost
Account Whose Credentials Were Used\Account Name	Does not contain	\$
Target Server\Additional Information	Does not contain	/

Da

From: "TERMSRV". You should tweak the last condition to filter with that.

Display event for the last  days  hours  Exclude

Clear Load... Save... OK Cancel

Filter with the event ID 4648.

Filter out localhost, computer accounts and SPNs.

Some kinds of rdp sessions are logged with a SPN for terminal server "TERMSRV". You should tweak the last condition to filter with that.

# RDP (14)

- How To Analyze

Event ID	Log Location	Logged Host	Where You Should Look	What You Get
4648	Security.evtx	Source	Date, Time	Date/Time around RDP used
			Computer Name	Source computer name
			Subject\Security ID	SID of RDP used
			Subject\Account Name	User name of RDP used
			Target Server\Target Server Name	Destination computer name
			Account Whose Credentials Were Used\Account Name	Logon user name of the remote host
		Destination	Date, Time	Date/Time around RDP used
			Computer Name	Destination computer name
			Account Whose Credentials Were Used\Account Name	Logon user name of the remote host
			Network Information\Source Network Address	Source IP address

Type	Date	Time	Event	Source	Category	User
Audit Success	2/8/2018	2:27:00 PM	4648	Microsoft-Windows-Se	Logon	N/A
Audit Success	2/8/2018	2:26:56 PM	4648	Microsoft-Windows-Se	Logon	N/A

Description

A logon was attempted using explicit credentials.  
Subject:  
Security ID: S-1-5-21-3671970501-397572877  
Account Name: honda  
Account Domain: NINJA-MOTORS  
Logon ID: 0x2c206c  
Logon GUID: {00000000-0000-0000-0000-000000000000}  
Account Whose Credentials Were Used:  
Account Name: ninja-rdp  
Account Domain: NINJA-MOTORS  
Logon GUID: {00000000-0000-0000-0000-000000000000}  
Target Server:  
Target Server Name: client-win10-1.ninja-motors.net  
Additional Information: client-win10-1.ninja-motors.net  
Process Information:  
Process ID: 0x2a0  
Process Name: C:\Window  
Network Information:  
Network Address: -

client-win10-1  
(admin-PC)

client-win10-2

This message logged on client-win-10-2 which is the source of this RDP Session.

The attackers have already had honda's credential and ninja-rdp's credential. And they moved laterally to "client-win10-1" with RDP.

# RDP (16)

- We found “honda” account logged on to ninja-rdp@client-win10-1 (192.168.52.40) from client-win10-2 (192.168.52.44) with RDP.
- It is a suspicious logon because 192.168.52.40 is the system administrator’s PC, and Honda, who is a general employee, does not own that PC. And, he cannot know the credential of the “ninja-rdp” account, which is an administrative account.

# Task Scheduler/AT Events

# Task Scheduler/AT Events (1)

- Why is this event important?
  - Attackers often use Task Scheduler and AT to execute commands on remote computers in lateral movement phase. So you should check this event.
- Important event IDs
  - Security.evtx
    - 4624: An account was successfully logged on.
  - Microsoft-Windows-TaskScheduler%4Operational.evtx
    - 100: Task started
    - 102: Task completed
    - 106: Task registered
    - 107: Task triggered on scheduler
    - 110: Task triggered by user
    - 129: Created Task Process (Launched)
    - 140: Task updated
    - 141: Task deleted
    - 200: Action Started
    - 325: Launch request queued

# Task Scheduler/AT Events (2)

- How can we detect this event?
  - 106 (Microsoft-Windows-TaskScheduler%4Operational.evtx)
    - Description
      - Task registered
    - How can we recognize Task Scheduler/AT with this ID?
      - This ID is dedicated for task registration.
      - And 4624 with logon type 3 (Security.evtx) is logged at the same time if the task is registered from remote hosts. You can get the source address information by combining with date/time and the user name of these logs.
  - 4624 (Secuirty.evtx)
    - How can we recognize Task Scheduler/AT with this ID?
      - We can filter with logon type 4 with this ID to get tasks triggered and those dates.



# Task Scheduler/AT Events (3)

- Let's assume this condition is given.
  - We have already known attackers moved laterally around 25<sup>th</sup> February 2018 from forensic analysis so far.
  - So we should look for registrations of tasks around that time at first.
- Open the below log with Event Log Explorer, and click "Filter Events" button.
  - Training\_Materials\EventLogAnalysis\TaskSched\Win10-2\_TaskSchedOpe.evtx
    - Original log name: Microsoft-Windows-TaskScheduler%4Operational.evtx

Notice:

You should **drag the log file and drop it** to the Event Log Explorer.



# Task Scheduler

Filter

Apply filter to:

Active event log view (File: C:\Users\taro\Desktop\Artifacts\evtx\TaskSched\Microsoft-)

Event log view(s) on your choice

Event types

Information

Warning

Error

Critical

Audit Success

Source:   Exclude

Category:   Exclude

User:   Exclude

Computer:   Exclude

Event ID(s):

Exclude

Enter ID numbers and/or ID ranges, separated by comas, use exclamation mark to exclude criteria (e.g. 1-19,100,250-450!10,255)

Text in description:

RegExp  Exclude

Filter by description params (for security event logs, e.g. Object\Object Name contains elx.exe)

Name	Operator	Value

Date  Time  Separately

From:   To:    Exclude

Display event for the last  days  hours  Exclude

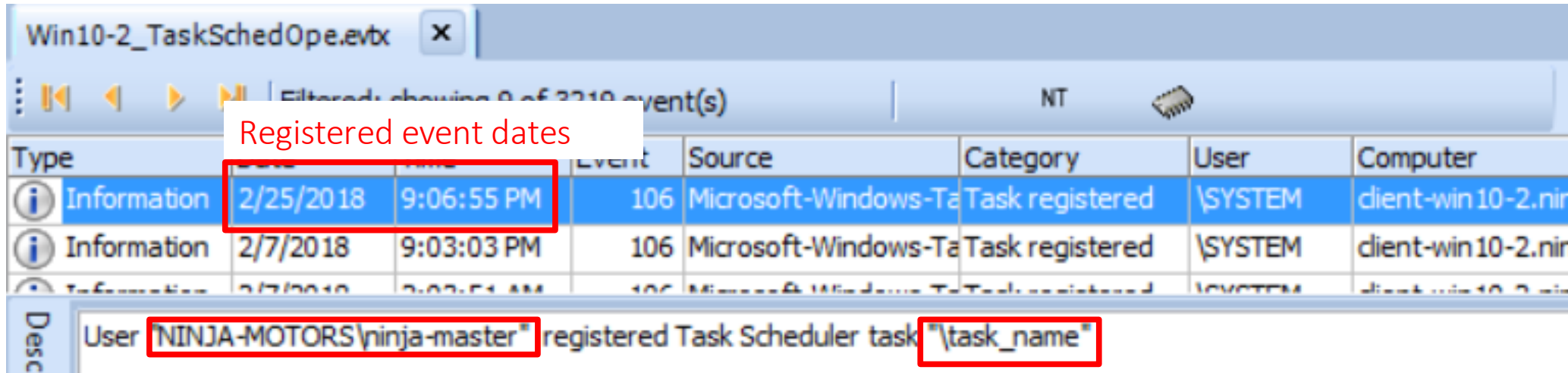
Filter with Event ID 106.

# Task Scheduler/AT Events (5)

Event ID	Log Location	Logged Host	Where You Should Look	What You Get
106	*1	Destination (remote host)	Date, Time	Date/Time around Task Scheduler used
			Computer Name	Destination computer name
			User	User name or SID of task registered
			Task	Task name
4624	Security.evtx	Destination (remote host)	Date, Time	Date/Time around Task Scheduler used
			Computer Name	Destination computer name
			New Logon\Security ID	Logon user's SID
			New Logon\Account Name	Logon user's account name
			New Logon\Logon ID	An ID to combine with 4648 and others
			New Logon\Logon GUID	An ID to combine with 4769
			Network Information\Source Network Address	Source IP address

\*1 : Microsoft-Windows-TaskScheduler%4Operational.evtx

# Task Scheduler/AT Events (6)



Type	Date and Time	Event	Source	Category	User	Computer
Information	2/25/2018 9:06:55 PM	106	Microsoft-Windows-Ta	Task registered	\SYSTEM	client-win10-2.nir
Information	2/7/2018 9:03:03 PM	106	Microsoft-Windows-Ta	Task registered	\SYSTEM	client-win10-2.nir
Information	2/7/2018 9:03:51 AM	106	Microsoft-Windows-Ta	Task registered	\SYSTEM	client-win10-2.nir

Desc: User "NINJA-MOTORS\ninja-master" registered Task Scheduler task "\task\_name"

User's name or SID

Task name

If the AT is used, task name is always "\At\*".

"\*" means a number.

Now, you can check whether legitimate tasks or not.

# Task Scheduler/AT Events (7)

- We got date/time, task name and registered user name from 106.
  - But where did this user register this task from?
    - If the task is registered from the remote host, then you can find 4624 type 3 log.
    - If the task is registered locally, 4624 type 3 message is not logged at the same time.

# Task Scheduler/AT Events (8)

- Let's find the ID 4624 with logon type 3 logs, which is logged at the same time with the ID 106 we confirmed before.
- Open the log below with Event Log Explorer, and click “Filter Events” button.
  - Training\_Materials\EventLogAnalysis\TaskSched\Win10-2\_Security.evtx
    - Original log name: Security.evtx

Notice:

You should **drag the log file and drop it to** the Event Log Explorer.



## Task S

Filter

Apply filter to:

Active event log view (File: C:\Users\ttaro\Desktop\EventLogAnalysis\RDP\Win10-2\_Se

Event log view(s) on your choice

Event types

Information

Warning

Error

Critical

Audit Success

Audit Failure

Source:   Exclude

Category:   Exclude

User:   Exclude

Computer:   Exclude

Event ID(s):

Exclude

Enter ID numbers and/or ID ranges, separated by comas, use exclamation mark to exclude criteria (e.g. 1-19,100,250-450!10,255)

Text in description:

RegExp  Exclude

Filter by description params (for security event logs, e.g. Object\Object Name contains elcx.exe)

(2) Choose "Training\_Materials\EventLogAnalysis\TaskSched\Sec4624\_type3\_Feb25\_9PM.elc", then click "Open" button.

Date  Time  Separately

From:   To:    Exclude

Display event for the   Exclude

Copyright Internet Initiative Japan Inc.

(1) Click "Load" button.

# Task 9

Filter

Apply filter to:

Active event log view (File: C:\Users\ttaro\Desktop\EventLogAnalysis\RDP\Win10-2\_Ser  
 Event log view(s) on your choice

Event types

Information  
 Warning  
 Error  
 Critical  
 Audit Success

Source:   Exclude

Category:   Exclude

User:   Exclude

Computer:   Exclude

Event ID(s):  
  Exclude

Enter ID numbers and/or ID ranges, separated by commas, use exclamation mark to exclude criteria (e.g. 1-19, 100, 250-450! 10, 255)

Text in description:  
  RegExp  Exclude

Filter by description params (for security event logs, e.g. Object\ObjectName contains elex.exe)

New condition Delete condition Clear list

Name	Operator	Value

Date  Time  Separately

From:   To:    Exclude

Display event for the last  days  hours  Exclude

Clear Load... Save... OK Cancel

Copyright Internet Initiative Japan Inc.

Filter with the event ID 4624.

Filter with logon type 3

Filter with Feb/25/2018 9 PM to 10 PM



Win10-2\_TaskSchedOpe.evtx

Filtered: showing 9 of 3219 event(s)

Type	Date	Time	Event	Source	Category	User	Computer
Information	2/25/2018	9:06:55 PM	106	Microsoft Windows Ta	Task registered	\SYSTEM	client-win10-2.nir

Win10-2\_Security.evtx

Filtered: showing 8 of 14232 event(s)

Type	Date	Time	Event	Source	Category	User	Computer
Audit Success	2/25/2018	9:06:55 PM	4624	Microsoft-Windows-Se	Logon	N/A	client-win10-2.

Description

Logon Information:

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

Impersonation Level: Impersonation

New Logon:

- Security ID: S-1-5-21-3671970501-3975728774-4289435121-3101
- Account Name: **ninja-master**
- Account Domain: NINJA-MOTORS.NET

50a805

0x0

Network Account Domain: -

Logon GUID: {AC0DAB8C-3425-EA6A-3C79-50AF2E0962D5}

Process Information:

- Process ID: 0x0
- Process Name: -

Network Information:

- Workstation Name: -
- Source Network Address: **192.168.52.40**
- Source Port: -

ID 4624 is always logged on destination host.

You can see the same time and the same user name between 106 and 4624.

We got the remote IP (source) address!

# Task Scheduler/AT Events (12)

- We confirmed “ninja-master” registered the task named “task\_name” from 192.168.52.40 at 9:06:55 PM on 25th Feb.
- What process is executed?
- And how many times were this command executed?
- You should see the below log again!
  - Artifacts\evtx\remote\_logon\TaskSched\Win10-2\_TaskSchedOpe.evtx

# Task Scheduler/AT Events (13)

- We should see the IDs below.
  - 107: Task triggered on scheduler
    - We can get execution times by counting this logs.
  - 110: Task triggered by user
    - We can get execution times by counting this logs.
  - 200: Action Started
    - We can see the execution file name.

# Task Sc

Filter

Apply filter to:

Active event log view (File: C:\Users\taro\Desktop\Artifacts\evtx\remote\_logon\TaskScd  
 Event log view(s) on your choice

Event types

Information  
 Warning  
 Error  
 Critical  
 Audit Success

Source:   Exclude

Category:   Exclude

User:   Exclude

Computer:   Exclude

Event ID(s):

Exclude

Enter ID numbers and/or ID ranges, separated by commas, use exclamation mark to exclude criteria (e.g. 1-19,100,250-450!10,255)

Text in description:

RegExp  Exclude

Filter by description params (for security event logs, e.g. Object\Object Name contains elcx.exe)

New condition Delete condition Clear list

Name	Operator	Value

Date  Time  Separately

From:   To:    Exclude

Display event for the last  days  hours  Exclude

Clear Load... Save... OK Cancel

Filter with Event ID 107, 110 and 200.

Filter with the task name "\task\_name".

# Task Scheduler/AT Events (15)

Event ID	Log Location	Logged Host	Where You Should Look	What You Get
200	*1	Destination (remote host)	Date, Time	Date/Time around Task Scheduler used
			Computer Name	Destination computer name
			action	Execution file name
			task	Task name
107	*1	Destination (remote host)	Date, Time	Date/Time around Task Scheduler used
			Computer Name	Destination computer name
			This event ID	Task triggered on scheduler
110	*1	Destination (remote host)	Date, Time	Date/Time around Task Scheduler used
			Computer Name	Destination computer name
			This event ID	Task triggered by user
			user	User name which task triggered

\*1 : Microsoft-Windows-TaskScheduler%4Operational.evtx

Type	Date	Time	Event	Source	Category	User	Computer
Information	2/25/2018	9:06:01 PM	107	Microsoft-Windows-Ta	Task triggered on scheduler	\SYSTEM	client-win10-2.ninja-mo
		:16 PM	110	Microsoft-Windows-Ta	Task triggered by user	\SYSTEM	client-win10-2.ninja-mo
		:02 PM	200	Microsoft-Windows-Ta	Action started	\SYSTEM	client-win10-2.ninja-mo
Information	2/25/2018	9:07:02 PM	107	Microsoft-Windows-Ta	Task triggered on scheduler	\SYSTEM	client-win10-2.ninja-mo

The task was executed three times.

Task Scheduler launched action "C:\Windows\system32\cmd.EXE" in instance "{E5E840A2-B80E-49E1-8AC9-131E3D85CAE9}" of task "\task\_name".

Execution file was found in the ID 200!

# Task Scheduler/AT Events (17)

- We confirmed “ninja-master” registered the “task\_name” task from 192.168.52.40 on February 25, 2018 at 21:06:55.
  - “cmd.exe” was executed three times in the task.

# Task Scheduler/AT Events (18)

- We can also find Task Scheduler/AT events with 4624, logon type 4 in “Security.evtx”.
  - Type 4 means “Batch”.
  - This logon type is dedicated for Task Scheduler/AT.
  - It logs every task trigger and launch requests.



# Task Scheduler/AT Events (19)

Event ID	Log Location	Logged Host	Where You Should Look	What You Get
4624	Security.evtx	Destination (remote host)	Date, Time	Date/Time around Task Scheduler used
			Computer Name	Destination computer name
			New Logon\Security ID	Logon user's SID
			New Logon\Account Name	Logon user's account name
			New Logon\Logon ID	An ID to combine with 4648 and others
			New Logon\Logon GUID	An ID to combine with 4769

# Task S

Win10-2\_Security.evtx x

Filtered: showing 4 of 14232 event(s) NT

Type	Date	Time	Event	Source	Category	User	Computer
Audit Success	2/25/2018	9:08:00 PM	4624	Microsoft-Windows-Se	Logon	N/A	client-win10-2.ninja-motors.r
Audit Success	2/25/2018	9:07:16 PM	4624	Microsoft-Windows-Se	Logon	N/A	client-win10-2.ninja-motors.r
Audit Success	2/25/2018	9:07:16 PM	4624	Microsoft-Windows-Se	Logon	N/A	client-win10-2.ninja-motors.r
Audit Success	2/25/2018	9:07:02 PM	4624	Microsoft-Windows-Se	Logon	N/A	client-win10-2.ninja-motors.r

Description

An account was successfully logged on.

Subject:

- Security ID: S-1-5-18
- Account Name: CLIENT-WIN10-2\$
- Account Domain: NINJA-MOTORS
- Logon ID: 0x3e7

Logon Information:

- Logon Type: 4
- Restricted Admin Mode: -
- Virtual Account: No
- Elevated Token: Yes

Impersonation Level: Impersonation

New Logon:

- Security ID: S-1-5-21-3671970501-3975728774-4289435121-3101
- Account Name: ninja-master
- Account Domain: NINJA-MOTORS
- Logon ID: 0x50c34e
- Linked Logon ID: 0x0
- Network Account Name: -
- Network Account Domain: -
- Logon GUID: {2F85E608-D6C5-46CE-7553-FACC5589FCE6}

Process Information:

- Process ID: 0x3c8
- Process Name: C:\Windows\System32\svchost.exe

Network Information:

- Workstation Name: CLIENT-WIN10-2
- Source Network Address: -
- Source Port: -

Detailed Authentication Information:

- Logon Process: .UBPM

x Description Data

# Task Scheduler/AT Events (21)

- Unified Background Process Manager (UBPM)
  - Service Control Manager – manages Windows Services
  - **Task Scheduler – manages Windows Tasks**
  - Windows Management Instrumentation – manages WMI providers
  - DCOM Server Process Launcher – manages out-of-process COM applications.

<https://blogs.technet.microsoft.com/askperf/2009/10/04/windows-7-windows-server-2008-r2-unified-background-process-manager-ubpm/>

# Task Scheduler/AT Events (22)

- You should also check the “Tasks” folders below.
  - C:\Windows\System32\Tasks
  - C:\Windows\SysWOW64\Tasks

```
</Hidden>false</Hidden>
<RunOnlyIfIdle>>false</RunOnlyIfIdle>
<WakeToRun>>false</WakeToRun>
<ExecutionTimeLimit>PT72H</ExecutionTimeLimit>
<DeleteExpiredTaskAfter>PT1S</DeleteExpiredTaskAfter>
<Priority>7</Priority>
</Settings>
<Actions Context="Author">
  <Exec>
    <Command>cmd</Command>
    <Arguments>/c ipconfig /all &gt; C:%windir%\temp\cccc.txt</Arguments>
  </Exec>
</Actions>
</Task>
```

- For AT command, you should look this folder.
  - c:\windows\tasks
  - \*.job

# Task Scheduler/AT Events (23)

- You might also need to check these logs below.
  - Microsoft-Windows-TaskScheduler%4Operational.evtx
    - 100: Task started
    - 102: Task completed
    - 140: Task updated
    - 141: Task deleted

PsExec

# PsExec Detection (1)

- PSEXec is a remote command execution tool for system administrators that is included in “Sysinternals Suite” tools, but this is often used for lateral movement in targeted attacks as well.
- Typical behavior of PsExec
  - It copies the PsExec service execution file (default: PSEXESVC.exe) to %SystemRoot% on remote computers with network logon (type 3).
  - It copies a file to execute command to %SystemRoot% through \$Admin share if -c option is used.
  - It registers the service (default: PSEXESVC), and starts the service to execute the command on the remote computer.
  - It stops the service (default: PSEXESVC), and removes the service on the remote computer after execution.

# PsExec Detection (2)

- Important behaviors of PSEXec options
  - -r
    - To change the copied file name and the service name for remote computers (default: %SystemRoot%\PSEXESVC.exe and PSEXESVC)
  - -s
    - To be executed by SYSTEM account.
  - -c
    - To copy a program to remote computers
    - It is copied to Admin\$ (%SystemRoot%)
  - -u
    - To use a specific credential to log on to remote computers.
    - Logon type 2 & logon type 3 is occurred.



# PsExec Detection (3)

- Important event IDs
  - Security.evtx
    - 4624: An account was successfully logged on.
  - System.evtx
    - 7045: A service was installed in the system.
- How can we find PsExec?
  - You can find PsExec execution by finding service registration logs.
    - Event ID 7045 in “System.evtx”
  - There are two methods.
    - Method 1: Finding default service name
    - Method 2: Finding changed service name

# PsExec Detection Method 1

# PsExec Detection Method 1 (1)

- How can we detect this event?
  - PsExec creates a service on remote hosts when it executes a command.
    - The default service name is “PSEXESVC”.
    - We can detect this service name.
  - System.evtx
    - 7045
      - Description
        - A service was installed in the system.
      - How can we recognize PsExec execution with this ID?
        - Filter with “PSEXE” string in this ID.
      - Why?
        - PsExec creates a service including this string by default.

# PsExec Detection Method 1 (2)

- Open the below log with Event Log Explorer, and click “Filter Events” button.
  - Training\_Materials\EventLogAnalysis\PSExec\win7\_system\_psexec\_en.evtx

Notice:

You should **drag the log file and drop it to** the Event Log Explorer.



# PsExec

Filter

Apply filter to:

Active event log view (File: C:\Users\taro\Desktop\win7\_system\_psexec\_en.evtx)

Event log view(s) on your choice

Event types

- Information
- Warning
- Error
- Critical
- Audit Success
- Audit Failure

Source:   Exclude

Category:   Exclude

User:   Exclude

Computer:   Exclude

Event ID(s):   Exclude

Text in description:

RegExp  Exclude

Filter by description params (for security event logs, e.g. Object\Object Name contains elex.exe)

New condition Delete condition Clear list

Name	Operator	Value

Date  Time  Separately

From:   To:    Exclude

Display event for the last  days  hours  Exclude

Clear Load... Save... OK Cancel

Filter with a part of default service and execution name. (e.g. 1-19,100,250-450! 10,255)

# PsExec Detection Method 1(4)

- How To Analyze

Event ID	Log Location	Logged Host	Where You Should Look	What You Get
7045	System.evtx	Destination (remote host)	Date, Time	Date/Time around Task Scheduler used
			Computer Name	Destination computer name
			User	Actual user name or SID for execution
			Service Name	Installed service name
			Service File Name	Copied execution file name
			Service Type	Whether user or kernel mode service

P

Event Log Explorer

File Tree View Event Advanced Window Help

<Load filter>

Computers Tree

You can find 7045 (Service registration) and 7036 (Change service state). Note that 7036 could not be not logged on Windows 8/10 hosts.

Type	Date	Time	Event	Source	Ca	User	Comput
Information	2/20/2018	8:11:18 PM	7036	Service Control	No	N/A	client-w
Information	2/20/2018	8:11:18 PM	7036	Service Control	No	N/A	client-w
Information	2/20/2018	8:11:18 PM	7045	Service Control	No	\S-1-5-21-3671970501-3975728774-4289435121-3101	client-w
Information	2/20/2018	8:10:43 PM	7036	Service Control	No	N/A	client-w
Information	2/20/2018	8:10:43 PM	7036	Service Control	No	N/A	client-w

You can also get the SID or the user name of the actual user even if the -s option is used.

Description

A service was installed in the system.  
 Service Name: PSEXESVC  
 Service File Name: %SystemRoot%\PSEXESVC.exe  
 Service Type: user mode service  
 Service Start Type: demand start  
 Service Account: LocalSystem

Description    Data

PSEXESVC is found in "Service Name" and PSEXESVC.exe is found in "Service File Name".

# PsExec Detection Method 1 (6)

- If you look for the ID 4624 logs in the “Security” log around the time when the ID 7045 is logged, you can get the same user name/SID and the source address of the remote computer.

2/20/2018	8:11:18 PM	7045	Service Cor No	\S-1-5-21-3671970501-3975728774-4289435121-3101
-----------	------------	------	----------------	---



# PsExec Detection Method 1 (7)

- Open the below log with Event Log Explorer, and click “Filter Events” button.
  - Artifacts\evtx\remote\_logon\PSExec\win7\_**security**\_psexec\_en.evtx



Notice:

You should **drag the log file and drop it to** the Event Log Explorer.

# PsExec

Filter

Apply filter to:

Active event log view (File: C:\Users\taro\Desktop\Artifacts\evtx\psexec\win7\_security)

Event log view(s) on your choice

Event types

Information

Warning

Error

Critical

Audit Success

Audit Failure

Source:   Exclude

Category:   Exclude

User:   Exclude

Computer:   Exclude

Event ID(s):

Exclude

Enter ID numbers and/or ID ranges, separated by commas, use exclamation mark to exclude criteria (e.g. 1-19,100,250-450!10,255)

Text in description:

RegExp  Exclude

Filter by description params (for security event logs, e.g. Object\Object Name contains elx.exe)

Name	Operator	Value
Network Information\Source Network Address	Not equal	:::1
Network Information\Source Network Address	Not equal	-
Network Information\Source Network Address	Not equal	127.0.0.1

(2) Choose "Training\_Materials\EventLogAnalysis\PSExec\Sec4624\_remote\_logon\_type3.elc", then click "Open" button.

Display event for the   Exclude

(1) Click "Load" button.

PsExec

Filter

Apply filter to:

Active event log view (File: C:\Users\taro\Desktop\Artifacts\evtx\psexec\win7\_security)

Event log view(s) on your choice

Event types

Information

Warning

Error

Critical

Audit Success

Source:   Exclude

Category:   Exclude

User:   Exclude

Computer:   Exclude

Event ID(s):

Exclude

Enter ID numbers and/or ID ranges, separated by commas, use exclamation mark to exclude criteria (e.g. 1-19,100,250-450!10,255)

Text in description:

RegExp  Exclude

Filter by description params (for security event logs, e.g. Object\Object Name contains elx.exe)

New condition Delete condition Clear list

Name	Operator	Value
Network Information\Source Network Address	Not equal	:::1
Network Information\Source Network Address	Not equal	-
Network Information\Source Network Address	Not equal	127.0.0.1

Date  Time  Separately

From:   To:

Display event for the last  days  hours  Exclude

Clear Load... Save... OK Cancel

Filter with event ID 4624.

Filter out :

- localhost
- computer accounts
- system account
- anonymous account

Filter with logon type 3.

# PsExec Detection Method 1 (10)

Event ID	Log Location	Logged Host	Where You Should Look	What You Get
7045	System.evtx	Destination (remote host)	Date, Time	Date/Time around Task Scheduler used
			Computer Name	Destination computer name
			User	Actual user name or SID for execution
			Service Name	Installed service name
			Service File Name	Copied execution file name
			Service Type	Whether user or kernel mode service
4624	Security.evtx	Destination (remote host)	Date, Time	Date/Time around Task Scheduler used
			Computer Name	Destination computer name
			New Logon\Security ID	Logon user's SID
			New Logon\Account Name	Logon user's account name
			New Logon\Logon ID	An ID to combine with 4648 and others
			New Logon\Logon GUID	An ID to combine with 4769
			Network Information\Source Network Address	Source IP address

2/20/2018	8:11:18 PM	7045	Service Cor No	S-1-5-21-3671970501-3975728774-4289435121-3101
-----------	------------	------	----------------	--

Type	Date	Time	Event	Source	Category
Audit Success	2/20/2018	8:11:46 PM	4624	Microsoft-Windows-Se	Logon
Audit Success	2/20/2018	8:11:45 PM	4624	Microsoft-Windows-Se	Logon
Audit Success	2/20/2018	8:11:18 PM	4624	Microsoft-Windows-Se	Logon
Audit Success	2/20/2018	8:11:18 PM	4624	Microsoft-Windows-Se	Logon
Audit Success	2/20/2018	8:11:47 PM	4624	Microsoft-Windows-Se	Logon

**Description**

**New Logon:**

- Security ID: S-1-5-21-3671970501-3975728774-4289435121-3101
- Account Name: ninja-master
- Account Domain: NINJA-MOTORS
- Logon ID: 0xc2e8a
- Linked Logon ID: (null)
- Network Account Name: (null)
- Network Account Domain: (null)

**Process Information:**

- Process ID: 0x0
- Process Name: -

**Network Information:**

- Workstation Name: -
- Source Network Address: 192.168.52.40
- Source Port: 64216

**Detailed Authentication Information:**

- Logon Process: Kerberos

*You can get the actual account name and the source address.*

# PsExec Detection Method 1 (12)

- We found PsExec execution from ninja-master@192.168.52.40 at 8:11:18 PM on February 20, 2018.
- We can find another PsExec execution in this log.
  - 2/20/2018 8:10:42 PM
  - 2/20/2018 8:08:09 PM
  - 2/20/2018 8:07:56 PM

# PsExec Detection Method 2

# PsExec Detection Method 2 (1)

- If the attackers change the execution name and the service name of PSEXec with -r option, we can still detect PSEXec execution because of the following characteristics.
  - The PSEXec service execution file (default: PSEXESVC.exe) is copied to “%SystemRoot%” directory on the remote computer.
  - The service name is the same as the execution name without the “.exe” extension.
  - The service is executed in “user mode”, not “kernel mode”.
  - “LocalSystem” account is used for the service account.
  - The actual account is used to execute the service execution file, not “SYSTEM”.



# PsExec Detection Method 2 (2)

- We use the same log as the previous exercise's one. Click "Filter Events" button.
  - Training\_Materials\EventLogAnalysis\PSExec\win7\_system\_psexec\_en.evtx



# PsExec

Filter

Apply filter to:

Active event log view (File: C:\Users\taro\Desktop\win7\_system\_psexec\_en.evtx)

Event log view(s) on your choice

Event types

- Information
- Warning
- Error
- Critical
- Audit Success
- Audit Failure

Source:   Exclude

Category:   Exclude

User:   Exclude

Computer:   Exclude

Event ID(s):

Exclude

Enter ID numbers and/or ID ranges, separated by commas, use exclamation mark to exclude criteria (e.g. 1-19,100,250-450!10,255)

Text in description:

RegExp  Exclude

Filter by description params (for security event logs, e.g. Object\Object Name contains elx.exe)

New condition Delete condition Clear list

Name	Operator	Value
Service File Name	Contains	.exe
Service File Name	Contains	%SystemRoot%
Service Type	Equal	user mode service

Display event for t... (1) Click "Load" button. ...  Exclude

Clear **Load...** Save... OK Cancel

(2) Choose "Training\_Materials\EventLogAnalysis\PSExec\Sys7045\_psexec.elc", then click "Open" button.

# PsExec

Filter

Apply filter to:

Active event log view (File: C:\Users\taro\Desktop\win7\_system\_psexec\_en.evtx)

Event log view(s) on your choice

Event types

- Information
- Warning
- Error
- Critical
- Audit Success

Source:   Exclude

Category:   Exclude

User:   Exclude

Computer:   Exclude

Event ID(s):

Enter ID numbers and/or ID ranges, separated by commas

Text in description:

Filter by description params (for security events)

New condition Delete condition

Name	Operator	Value
Service File Name	Contains	.exe
Service File Name	Contains	%SystemRoot%
Service Type	Equal	user mode service

Date  Time  Separately

From:   To:    Exclude

Display event for the last  days  hours  Exclude

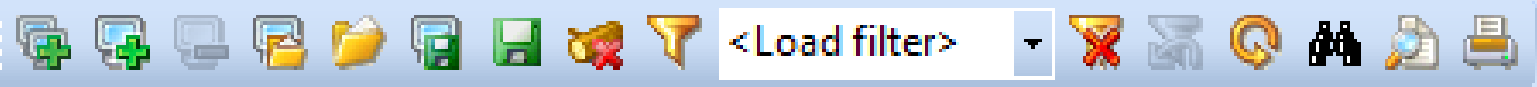
Clear Load... Save... OK Cancel

Filter out the "SYSTEM" account.

Filter with the event ID 7045.

Filter with:

- containing .exe in the file name
- containing %SystemRoot% in the file name
- user mode service for service type
- LocalSystem as service account
- demand start as service start type



Computers Tree

win7\_system\_psexec\_en.evbx

Filtered: showing 5 of 174 event(s) NT

Type	Date	Time	Event	Source	Category
Information	2/20/2018	8:11:46 PM	7045	Service Control Manag	None
Information	2/20/2018	8:11:18 PM	7045	Service Control Manag	None
Information	The file name is not the default PSEXec name, but...			Service Control Manag	None
Information	2/20/2018	8:08:09 PM	7045	Service Control Manag	None
Information	2/20/2018	8:07:55 PM	7045	Service Control Manag	None

This execution file is directly under the %SystemRoot% directory.

Description

A service was installed in the system.  
 Service Name: **WindowsWMIService**  
 Service File Name: **%SystemRoot%\WindowsWMIService.exe**  
 Service Type: **user mode service**  
 Service Start Type: demand start  
 Service Account: **LocalSystem**

The same name

This is a user mode service, not kernel mode.

The service account is "LocalSystem"

It seems this entry is a PsExec used with -r option!

# PsExec Detection Method 2 (6)

- We found PsExec execution with -r option at 8:11:46 PM on 20<sup>th</sup> Feb.
  - The temporary service name is “WindowsWMIService”.

To be continued...