computer emergency response team CERT-EU for the EU institutions, bodies and agencies

CERT-EU Security Whitepaper 17-002

Detecting Lateral Movements in Windows Infrastructure

M.SORIA-MACHADO, D.ABOLINS, C.BOLDEA, K.SOCHA

ver. **2.0**
February 27, 2017

Contents

1 Introduction

Lateral movement techniques are widely used in sophisticated cyber-attacks in particular in *Advanced Persistent Threats* (APTs). The adversary uses these techniques to access other hosts from a compromised system and get access to sensitive resources, such as mailboxes, shared folders, or credentials. These can be used in turn for compromise of additional systems, privilege escalation, or stealing more valuable credentials. This type of attack may ultimately give access to the Domain Controller and provide full control of a Windows-based infrastructure or business-related operator accounts.

This white-paper provides guidelines to detect the lateral movements exploiting NTLM and Kerberos protocols in a Windows Vista / 7 and 2008 based environment. Windows 10 introduces many additional security mechanisms, and hence CERT-EU is planning to release a separate white-paper regarding lateral movement detection on Windows 10.

Microsoft released important guidance about credential theft and how to prevent it[1]. We strongly recommend implementing the proposed protections in addition to the detective controls depicted in the current paper. Note that this type of attack is not only linked to Windows environment, but a similar technique of attack can be applied to other infrastructures, such as UNIX using Kerberos or a single-sign-on solution. While this white-paper focuses specifically on techniques of detecting lateral movements on Windows systems, it may also be an inspiration for other cases, where appropriate logging exists.

We would like to thank the team at Microsoft MSRC in Redmond for their contribution to the quality check and validation of this document.

2 Background

2.1 Windows Lateral Movement Attacks

This paper refers to lateral movement attacks as connections from a *Windows host* to a targeted *Windows host* using valid stolen credentials of an account (i.e., user or service account).

The source host is usually a compromised system in the targeted Windows environment. The first host is compromised in most cases via a spear-phishing attack that contains a malicious attachment or link to a site under attacker's control. Once compromised and in most of the cases, the attacker usually takes control of the host via a call-back to a Command-and-Control server and a (reverse) shell. After elevation of privileges, the adversary can then dump credentials stored in this first compromised host and use them to connect to another host.

Consequently, a lateral movement is a 2-step attack as follows:

1. Capture credentials from a source host.

The attacker can capture any valid credentials. The credentials are usually obtained through specialized tools that access Windows credential storage or memory[2]. This paper is limited to the theft and misuse of NT hash and Kerberos credentials.

The adversary can potentially get any credentials stored in the compromised system, that are still in use or were used in the past (e.g., cached credentials)[3] and that has not been wiped from

[1] http://www.microsoft.com/pth

[2] Key logger can also be used to steal clear-text passwords but this is not in the scope of this paper.

[3] http://technet.microsoft.com/en-us/library/hh994565%28v=ws.10%29.aspx

memory (if no update is installed)[4]. The most interesting credentials are the privileged accounts of the targeted domain, such as help-desk, domain admin, privileged service account, as well as local administrator account, especially if password is re-used or the password generation algorithm is predictable.

2. Use stolen credentials to access another host or resources.

Once the credentials are stolen, the attacker can use them to access another resource, such as a host or a server (e.g., Exchange e-mail accounts). The attacker can use techniques known as pass-the-hash or pass-the-ticket with NT hash or Kerberos ticket accordingly. See [1], [2], [3] for further details on these types of attacks.

There are a few facts that are relevant regarding credentials theft and replay:

- **Any user** connecting to a compromised host **may leave credentials in memory** that can be dumped by the attacker (if appropriate updates are not installed)[5]. Windows caches the credentials in memory to provide features like single-sign-on:
  - Accounts solely using *Network Logon* or RDP in Restricted Admin mode to log into the compromised target host are not exposed.[4]
  - Any other type of logon exposes the credentials, including local, domain users or service accounts. See section 2.3 for more details about credential caching.
- Impacted credentials are not limited to clear-text usernames/passwords, but also **NT hashes**, **Kerberos Tickets** and **Kerberos keys** which can be used to request Kerberos TGTs are valid credentials for lateral movements as well.
- The attacker needs **administrative privileges** to access the credentials in the local Windows credential storage or memory (i.e., Windows Security Accounts Manager, Credential Manager, or Local Security Authority Subsystem Service process)[6]. A local privilege escalation vulnerability can be used for this if the compromised user does not have such privileges yet.
- Lateral movements are not limited to access another workstation, but can be used to connect to other resources such as a mailbox on an Exchange server or a business system.
- Lateral movements use standard protocols, like Kerberos and NTLM protocol, which makes impossible to create a single dedicated Windows event or network IDS rules to detect them.
- One of the advantages of the lateral movement attack is that the attacker can capture credentials and use them later.
- Lateral movements are not Windows specific problems, as any authentication protocol using single-sign-on has the same issue. Any single-sign-on solution requires storing credentials in some valid format so they can be reused to authenticate to other services without re-entering the password each time.

2.2 Typical APT Scenario Using Lateral Movements

Usually, APTs will connect from one workstation to another to obtain higher and higher privileged accounts until they get the credentials of a domain admin account. The next step of the

[4] http://support.microsoft.com/kb/2871997
[5] http://support.microsoft.com/kb/2871997
[6] Refer to [1] http://www.microsoft.com/pth for further details about credential theft in Windows.

attack will usually be to access the Domain Controller and dump all credentials of the Windows domain.

The following picture presents the typical scenario of an APT with lateral movement:

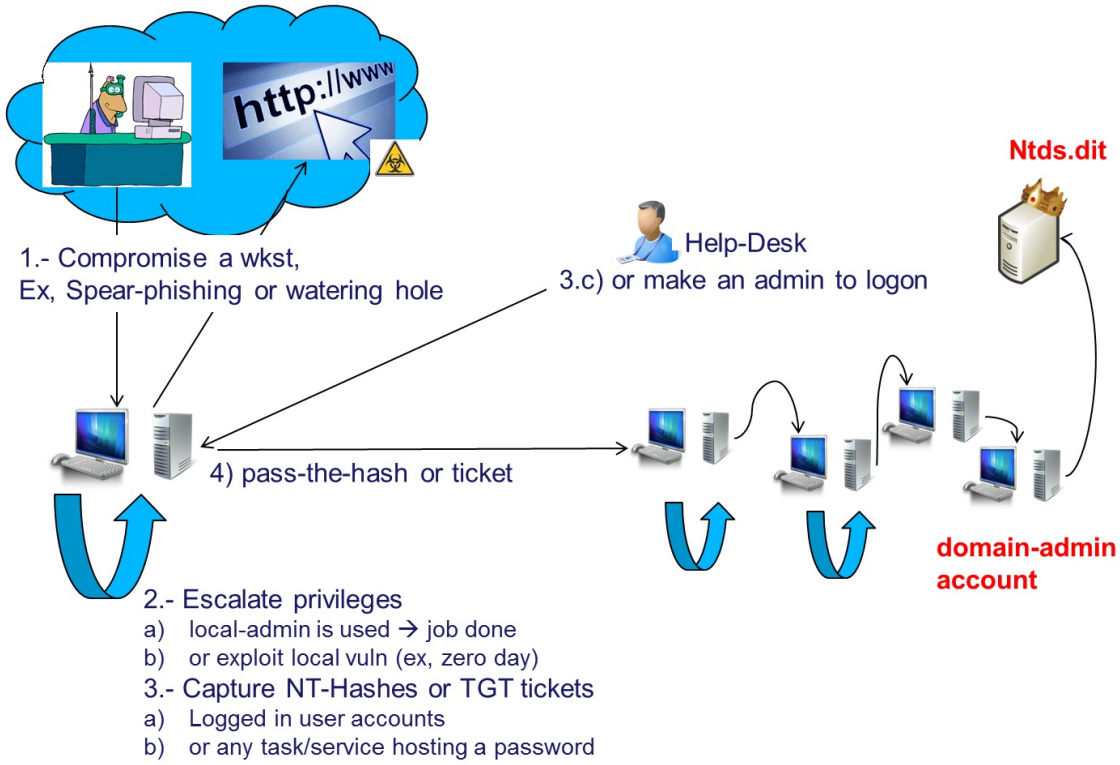

Figure 1: Typical lateral movements in case of APTs

2.3 Credential Caching

As mentioned in the previous section, credentials – including domain users or admins – are cached in memory of the workstation where they connect to or run commands from, for instance when doing RDP (except `RestrictedAdmin` mode) or `runas` commands.

The following table summarizes the caching of Kerberos TGT tickets[7] of a `user2` (e.g., admin user), while logging to a host where another user – `user1` – is already logged on. Any caching of this `user2` tickets is therefore exposed to `user1` and any attacker that would have compromised the workstation.

Note that not all the logon types were tested, but also in some selected scenarios based on the potential behavior of a privileged user, `user2` can access a workstation (for instance for administration purposes). Microsoft's guidance in [1] provides a more exhaustive summary of the exposed reusable credentials on the destination host.

Logon Type	Cached NT Hash	Cached TGT	Log-off & Log-on
remote assistance	NO	NO	N/A
RDP	YES	YES	NO[8] / YES[9]

[7] Windows events (4768, 4769, 4624 and 4625) were monitored to assure that Kerberos authentication was in use instead of NTLM.

[8] The ticket does not stay on the remote host if the user2 logged off properly.

[9] The ticket of `user2` remains if the remote session has not been closed properly.

Logon Type	Cached NT Hash	Cached TGT	Log-off & Log-on
run as admin[10] with interactive	YES	YES	NO
run as admin[11] with interactive + network	YES	YES	NO
run as admin with interactive + network[12]	YES	YES	NO
network to a remote (admin) share[13]	NO	NO[14]	N/A

The use-cases where based on the *run as administrator* Windows feature which grants the full administrator access token (User Account Control). Windows behaves differently when administrator opens an application (ex, `cmd.exe`) with `runas` command:

- when exiting the application, the cached NT hash and ticket remain when opened with `run as administrator` (UAC);
- the credentials are cleaned up from memory when using `runas /user:\\dom\user2`.

Interestingly, the last scenario (cached interactive logon, `run as administrator`, followed by a netlogon) did not require re-entering the password for the netlogon (!).

Some remarks regarding the use-cases:

- All tests were done on a non-privileged interactive session (logon at console of `user1`).
- The Network logons were not persistent.
- The tests were done with delegation switch `on` and `off` (*Account is sensitive and cannot be delegated* feature).
- The logoff tests were done with the target account session was properly closed or left open during the log-off process. The result is still the same.

2.4 Pass-the-Hash versus Pass-the-Ticket

The following table summarizes the main differences between exploiting pass-the-hash and pass-the-ticket. Some interesting conclusions are:

- Administrative privileges are required to steal the credentials but not to use a Kerberos ticket.
- The password change does not make Kerberos tickets invalid.

	Pass-the-Hash	Pass-the-Ticket
privileges to get credentials	administrator	administrator
privileges to reuse credentials	administrator	none
validity	policy based	policy based
resetting password	PtH fails	no impact

[10] A `cmd.exe` was open with a right click to *run as administrator* – user2.

[11] Same as before but using the cached domain password. This scenario might apply to systems like laptops when not connected to the domain.

[12] A `net use` command was run in the command prompt open with run as `user2`.

[13] Commmand: `net use \\target\c$` from `user2` prompt.

[14] Event-id 4768 is logged on DC. Interestingly, there is no TGT ticket cached for `user2` but the local host keeps a [CIFS] Service Ticket in memory for user1 to access the share folder.

3 Detecting Windows Lateral Movements

3.1 General Rules

There is no difference between a legitimate SMB connection and a pass-the-hash or -ticket attack at protocol level. Indeed, there the attack does not exploit a weakness of the protocol. Therefore, there is no predefined rule to detect them.

The attackers however create anomalies at behavior level. For instance, if a domain admin account, `my-admin`, can only be used from a specific workstation, *my-admin's workstation* then any use of that account from another workstation is suspicious and may indicate a potential lateral movement.

Consequently, the detection of lateral movements is possible by monitoring the Windows events. We can define a main rule as follow:

Lateral movements can be detected by identifying the use of accounts from or to unusual or non-authorized systems.

There are some limitations that are important to understand:

- A pragmatic implementation of this rule will limit the detection of lateral movements to privileged accounts. It is very difficult to detect all lateral movements. For this it is necessary to maintain a list of tuples user/workstation/IP addresses and detect any use that is not in line with the expectations. In addition, there are scenarios that cannot be detected with only tuple rules (e.g., access to resources from expected user/workstation but with malicious intentions).
- The feasibility to implement these rules will strongly depend on the defined policy, active directory structure, and the network segregation. Policy should mandate the use of dedicated hosts for the accounts that need to be monitored, e.g., dedicated OU, administrator workstations. An inventory of such workstations must be maintained. **The clearer the policy about these accounts and workstations, the more efficient it will be to detect lateral movements and avoid false positives.** Network segregation will help to identify the lateral movements, especially in case of Kerberos, because Kerberos does not provide hostname information in the related events.
- Detecting lateral movements with local accounts (e.g., local administrator) requires collecting events (4624/4625) from all potential target workstations. This might be in some cases impossible to do. The issue is less relevant when monitoring domain accounts because the main Windows events are stored on the Domain Controller. Microsoft has introduced two SIDs to ease the manipulations with local administrator accounts with GPOs.

The following sections present the events that are generated when performing the pass-the-hash and pass-the-ticket attacks and the main rules that can be setup to detect lateral movements.

3.2 Conventions and Assumptions

This paper focuses on the detection of lateral movements with administrator accounts, named as `ADMIN`, initiated from a workstation other than their own `ADMIN-WS`. The same rules can be fine-tuned to detect other cases, such as **service accounts** or other privileged accounts.

In the example given below, we assume that:

- Domain Admin accounts can be easily identified by querying Active Directory (command: `net group "Domain Admins" /domain`),

- `ADMIN` will refer to this group of Administrator, attackers familiar with environment can opt for naming convention;
- The administrative workstations can be easily identified:
  - Through their hostname, for instance:
  - Maintaining a OU or list
  - Or via a naming convention, example `admin-ws-1`, `admin-ws-2`, etc.
  - And through the IP addresses:
  - Having a dedicated (V)LAN for these workstations
  - Using or enforcing the use of a *jump-server*[15]
- `ADMIN-WS` will refer to the `ADMIN`'s workstation or jump-servers.

3.3 Detecting NTLM Lateral Movements (PtH)

3.3.1 Summary of the Generated Events

The following figure summarizes events generated in all entities of an NTLM credentials use scenario and on the Domain Controllers if a domain user is used. The detailed events are presented in section 6.1.

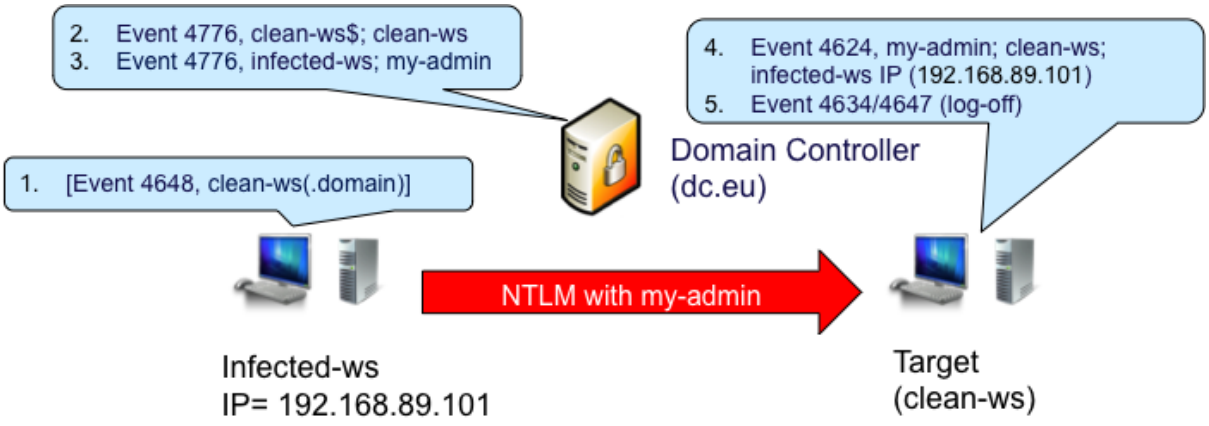

Figure 2: Events related to NTLM credential use

Event 4648 logged on infected workstation (`infected-ws`): A logon was attempted using explicit credentials

The events generated here depend on the *modus operandi* of the attacker. In this scenario, the attacker runs a `psexec.exe \\Target cmd.exe` that opens a command prompt on the target host using the NT hash previously injected. See Annex C for more details.

The events on the infected workstation are useful for forensics purposes, but not efficient to proactively detect a pass-the-hash attempt. In this scenario, the event provides the destination of the lateral movement, `clean-ws`.

Two events 4776 logged on the Domain Controller: The domain controller attempted to validate the credentials for an account

The first event 4776 is generated during the authentication of the machine, `clean-ws$`, to the domain controller. This event is not useful to detect a pass-the-hash.

[15] Administrator would login to this server before connecting to any other system.

The second event 4776 indicates the validation of the account, `my-admin`, when accessing the target workstation, `clean-ws`. **This event can indicate a lateral movement and is the key element to monitor the environment for.**

Event 4624 logged on target host (`clean-ws`): An account was successfully logged on

This event indicates the successful logon of the target user, `my-admin`, on the target workstation, `clean-ws`. This event can be used to detect lateral movements, but requires collection of the specific logs from all workstations. It might still be useful for a limited number of workstations or servers.

In any case, this event and the failed logon event, 4625, are very useful for forensic purposes as they provide the type of logon (Network logon in this case) and more interestingly, the source from where the attacker initiated the connection (`infected-ws`).

Event 4634/4647 logged on the target host: An account was/initiated logged off.

This event indicates the log off of the attacker. This is useful for forensics purposes to determine the full session of the attack via the Logon ID value of the event 4624 and this event.

3.3.2 Generic Detection Rules

This section provides the events to collect from each source, and the values that can be used to detect a NTLM lateral movement. As mentioned above, the main event – 4776 – to monitor is on the Domain Controller (DC). The event 4624 and 4625 (failed attempt) is optional but recommended to be collected from critical systems.

Log	Event	Field	Value to Monitor
DC	4776	Authentication Package	MICROSOFT_AUTHENTICATION_PACKAGE
		Logon Account	`ADMIN`
		Source Workstation	**any other than** `ADMIN-WS`
		Error Code	any
WS	4624	Authentication Package	MICROSOFT_AUTHENTICATION_PACKAGE or NTLM
	4625	Logon Account	`ADMIN`
		Workstation Name	**any other than** `ADMIN-WS`
		Source Network Address	**any other than** `ADMIN-WS` **'s IP**
		Logon Type	3 or any

NOTE: do not ignore the importance of event logs on workstations, especially ones that are used for sensitive and/or privileged accounts.

3.4 Detecting Kerberos Lateral Movements (Pass-the-Ticket)

3.4.1 Summary of the Generated Event-IDs

The following figure presents a summary of the events generated in each end when doing a Kerberos authentication. The detailed events are in section 6.2.

This scenario did not generate an event 4648 as for the pass-the-hash.

Event 4768 logged on the Domain Controller: A Kerberos authentication ticket (TGT) was requested.

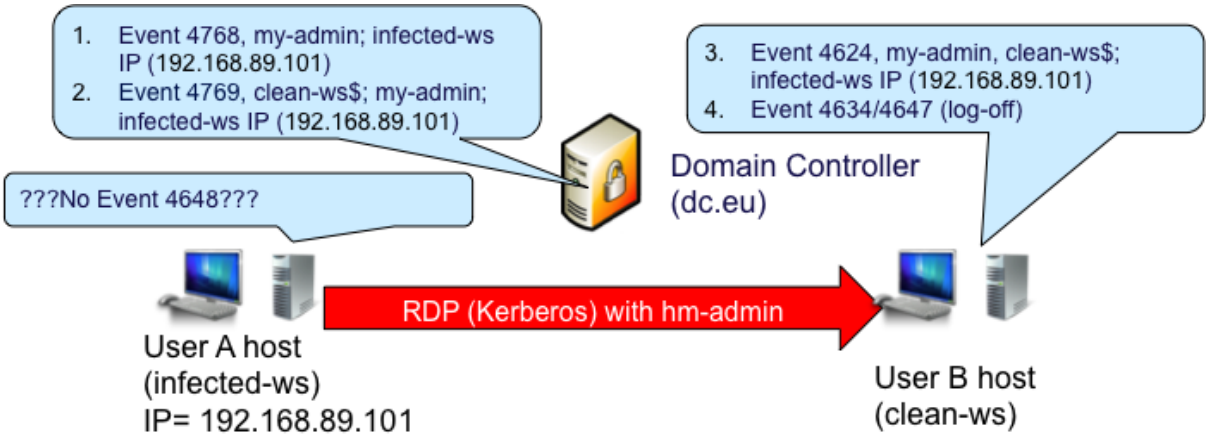

Figure 3: Events related to NTLM credential use

The first event 4768 is generated to request the Kerberos TGT ticket to the Domain Controller. This event might not be seen during a pass-the-ticket as the TGT ticket is previously stolen and directly injected in the attack instead of requesting a new one to the Kerberos Distribution Center/Domain Controller.

Event 4769 logged on the Domain Controller: A Kerberos service ticket was requested.

This event is generated to request access to the target system or resource, `clean-ws$` in the above example.

This event can indicate a lateral movement and is the main event to be used to monitor your environment.

Event 4624 logged on Target host (`clean-ws`): An account was successfully logged on

This event indicates the actual logon of the user – `my-admin` – on the target – `clean-ws`. This event can potentially be used to proactively detect lateral movements, but required collecting logs from all workstations. It might still be useful for a limited number of workstations or servers.

In any case, this event and failed logon, 4625, is very useful for forensic purposes as it provides the type of logon (Network logon in this case) and more interestingly, the source from where the attacker initiated the connection, ie. the infected workstation (`infected-ws`).

Event 4634/4647 An account was/initiated logged off.

This event indicates the log off of the attacker. This is useful for forensics purpose to determine the full session of the attack via the Logon ID value of the event 4624 and this event.

3.4.2 Generic Detection Rule

This section provides the events to collect from each source and the values that can be used to proactively detect a lateral movement with pass-the-ticket.

As mentioned above, the main events to monitor are on the Domain Controller (DC), 4769 and potentially 4768. Note that this time only the IP address can be verified, as Kerberos event does not provide the hostname. This is a problem with DHCP-enabled environments that can be a challenge in dynamic environments or environments with short DHCP lease time.

The event 4624 and 4625 (failed attempts) are also optional but recommended to be collected from critical systems.

Log	Event	Field	Value to Monitor
DC	4769	Service Name	any - any other than `ADMIN-WS`
	4768	Account Name	`ADMIN`
		Client Address	**any other than** `ADMIN-WS` **'s IP**
		Failure Code	any
WS	4624	Authentication Package	optional - [NEGOTIATE] or [KERBEROS]
	4625	Logon Account	`ADMIN`
		Workstation Name	empty
		Source Network Address	**any other than** `ADMIN-WS` **'s IP**
		Logon Type	optional - any

Potential false positives:

Note that if an administrator – e.g., help desk – is opening applications on the remote hosts (e.g., doing a Remote Access followed by a `cmd.exe` with `runas administrator`), this might generate events 4768.

3.4.3 Detecting the Golden Ticket

CERT-EU released a white-paper about the Kerberos golden ticket. See [8] for more details.

3.5 Main Accounts to Monitor

The monitoring rules depicted in this document are based on the Domain Administrator account. Other important accounts can be monitored and be quick wins to detect attacks:

- service accounts (e.g., a backup account),
- rarely used accounts,
- emergency accounts,
- business-critical accounts.

3.6 Additional Events to Monitor

We recommend the reference from NSA [7] that provides additional events that might be useful to monitor to detect potential attacks. The paper covers a wide range of event and type of attack, not only lateral movements.

4 Annex A - Definitions

Pass-the-hash: is a hacking technique that allows an attacker to authenticate to a remote server/service by using the previously stolen underlying NTLM and/or LanMan hash of a user's password, instead of requiring the associated plaintext password as is normally the case.

Pass-the-ticket: similar to Pass-the-hash but with Kerberos tickets instead of NT hashes;

Credentials: the identity and the related secret (authenticator) that can be used to proof someone identity. Consequently, a type of credential is not limited to plaintext passwords but it can be a Windows NTLM hash or a Kerberos Ticket depending on the Windows Authentication protocol that is used. In some circumstances, Windows caches the credentials to provide the single-sign-on feature. This paper will focus on Kerberos ticket called Ticket-Granting-Tickets (TGT). See [1] for more details about Windows Credential types (table 4) and caching.

TGT and ST Kerberos tickets: Ticket-Granting-Tickets (TGT) and Service Tickets are part of the Kerberos protocol. For more details about Kerberos and related tickets see [2].

KDC: Key distribution Center.

5 Annex B – References

[1] Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft Techniques http://www.microsoft.com/pth

[2] Kerberos Authentication Technical Reference http://technet.microsoft.com/en-us/library/cc739058(v=ws.10).aspx

[3] Chapter 3 - Recovering from Active Directory Attacks http://technet.microsoft.com/en-us/library/bb727066.aspx#ECAA

[4] Credential Protection and Management http://technet.microsoft.com/en-us/library/dn408190.aspx

[5] Windows events https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/Default.aspx

[6] Windows 7 and 2008 Security events http://www.microsoft.com/download/details.aspx?id=50034

[7] Techniques for spotting an adversary https://www.iad.gov/iad/library/reports/spotting-the-adversary-with-windows-event-log-monitoring.cfm

[8] Protection from Kerberos Golden Ticket http://cert.europa.eu/static/WhitePapers/UPDATED%20-%20CERT-EU_Security_Whitepaper_2014-007_Kerberos_Golden_Ticket_Protection_v1_4.pdf

6 Annex C - Detailed Events

This sections detail the events generated by a pass-the-hash and pass-the-ticket scenarios and reported with log2timeline.

- Infected workstation: `USER-WS (192.168.89.101)`
- Target user: `my-admin`
- Target host: `admin-ws (192.168.89.102)`
- Domain name: `corp.pass.thehash`

6.1 Network Logon and Pass-the-Hash Events

6.1.1 Domain Controller Events

```
Time: 06:32:56
Event: 4776
Event content:
- PackageName = MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
- TargetUserName = my-admin
- Workstation = USER-WS
- Status = 0x00000000
Command: `psexec.exe \\admin-ws cmd.exe`
Comment: The domain controller attempted to validate the credentials for an account

Time: 06:33:37
Event: 4776
Event content:
- PackageName = MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
- TargetUserName = my-admin
- Workstation = USER-WS
- Status = 0x00000000
Command: robocopy.exe c:\goodies\sch \\admin-ws\c$
Comment: The domain controller attempted to validate the credentials for an account

Time: 06:34:16
Event: 4776
Event content:
- PackageName = MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
- TargetUserName = my-admin
- Workstation = USER-WS
- Status = 0x00000000
Command: at.exe \\admin-ws 06:35 c:\schedule.bat
Comment: The domain controller attempted to validate the credentials for an account
```

6.1.2 Source/Infected Host Events (`user-ws`)

```
Time: 06:32:44
Event: 4624
Event content:
- SubjectUserSid = S-1-5-18 SubjectUserName = USER-WS$
- SubjectDomainName = CORP
- SubjectLogonId = 0x00000000000003e7 TargetUserSid = S-1-5-18 TargetUserName = SYSTEM
  TargetDomainName = NT AUTHORITY TargetLogonId = 0x00000000001046e9
- LogonType = 9
- LogonProcessName = seclogo
- AuthenticationPackageName = Negotiate
- WorkstationName =  LogonGuid = {00000000-0000-0000-0000-000000000000}
- TransmittedServices = - LmPackageName = - KeyLength = 0 ProcessId = 0x00000000000003b4
- ProcessName = C:/Windows/System32/svchost.exe IpAddress = ::1 IpPort = 0
Command: sekurlsa::pth /user:my-admin /domain:corp /ntlm:[nt hash] /run:cmd.exe
Comment: Succesful logon, TargetLogonId = 0x00000000001046e9

Time: 06:32:44
Event: 4672
Event content:
- SubjectUserSid = S-1-5-18 SubjectUserName = SYSTEM SubjectDomainName = NT AUTHORITY
- SubjectLogonId = 0x00000000001046e9
```

```
- PrivilegeList = SeCreateTokenPrivilege   SeAssignPrimaryTokenPrivilege   SeTcbPrivilege
  SeSecurityPrivilege   SeTakeOwnershipPrivilege   SeLoadDriverPrivilege   SeBackupPrivilege
     SeRestorePrivilege   SeDebugPrivilege   SeAuditPrivilege   SeSystemEnvironmentPrivilege
     SeImpersonatePrivilege
Comment: Special privileges assigned to new logon, as above. LogonId = 0x00000000001046e9

Time: 06:32:55
Event: 4648
Event content:
- SubjectUserSid = S-1-5-18 SubjectUserName = SYSTEM SubjectDomainName = NT AUTHORITY
- SubjectLogonId = 0x00000000001046e9 LogonGuid = {00000000-0000-0000-0000-000000000000}
- TargetUserName = -------- TargetDomainName = ---- TargetLogonGuid =
  {00000000-0000-0000-0000-000000000000}
- TargetServerName = admin-ws.corp.pass.thehash TargetInfo = admin-ws.corp.pass.thehash
- ProcessId = 0x0000000000000004 ProcessName =
- IpAddress = - IpPort = -
Command: psexec.exe \\admin-ws cmd.exe
Comment: A logon was attempted using explicit credentials. This event is generated when a
  process attempts to log on an account by explicitly specifying that accounts credentials.
  This most commonly occurs in batch-type configurations such as scheduled tasks, or when
  using the RUNAS command. SubjectLogonId = 0x00000000001046e9

Time: 06:32:55
Event: 4648
Event content:
- SubjectUserSid = S-1-5-18 SubjectUserName = SYSTEM SubjectDomainName = NT AUTHORITY
- SubjectLogonId = 0x00000000001046e9 LogonGuid = {00000000-0000-0000-0000-000000000000}
- TargetUserName = -------- TargetDomainName = ---- TargetLogonGuid =
  {00000000-0000-0000-0000-000000000000}
- TargetServerName = admin-ws.corp.pass.thehash TargetInfo = admin-ws.corp.pass.thehash
  ProcessId = 0x0000000000000998
- ProcessName = C:/goodies/PsExec.exe
- IpAddress = - IpPort = -
Comment: LogonId = 0x00000000001046e9

Time: 06:33:35
Event: 4648
Event content:
- SubjectUserSid = S-1-5-18 SubjectUserName = SYSTEM SubjectDomainName = NT AUTHORITY
- SubjectLogonId = 0x00000000001046e9 LogonGuid = {00000000-0000-0000-0000-000000000000}
- TargetUserName = -------- TargetDomainName = ---- TargetLogonGuid =
  {00000000-0000-0000-0000-000000000000}
- TargetServerName = admin-ws.corp.pass.thehash TargetInfo = admin-ws.corp.pass.thehash
- ProcessId = 0x0000000000000004 ProcessName =
- IpAddress = - IpPort = -
Command: robocopy.exe c:\goodies\sch \\admin-ws\c$
Comment: A logon was attempted using explicit credentials. LogonId = 0x00000000001046e9

Time: 06:34:15
Event: 4648
Event content:
- SubjectUserSid = S-1-5-18 SubjectUserName = SYSTEM SubjectDomainName = NT AUTHORITY
- SubjectLogonId = 0x00000000001046e9 LogonGuid = {00000000-0000-0000-0000-000000000000}
- TargetUserName = -------- TargetDomainName = ---- TargetLogonGuid =
  {00000000-0000-0000-0000-000000000000}
- TargetServerName = admin-ws.corp.pass.thehash TargetInfo = admin-ws.corp.pass.thehash
- ProcessId = 0x0000000000000004 ProcessName =
- IpAddress = - IpPort = -
Command: at.exe \\admin-ws 08:00 c:\schedule.bat
Comment: A logon was attempted using explicit credentials.LogonId = 0x00000000001046e9
```

6.1.3 Target host events (`admin-ws`)

```
Time: 06:32:55
Event: 4672
Event content:
- SubjectUserSid = S-1-5-21-2976932740-3244455291-537790045-1105
- SubjectUserName = my-admin
- SubjectDomainName = CORP SubjectLogonId = 0x00000000000f133c PrivilegeList =
  SeSecurityPrivilege   SeBackupPrivilege   SeRestorePrivilege   SeTakeOwnershipPrivilege
  SeDebugPrivilege   SeSystemEnvironmentPrivilege   SeLoadDriverPrivilege
  SeImpersonatePrivilege
Comment: Special privileges assigned to new logon.


Time: 06:32:55
Event: 4624
Event content:
- SubjectUserSid = S-1-0-0 SubjectUserName = - SubjectDomainName = - SubjectLogonId =
  0x0000000000000000 TargetUserSid = S-1-5-21-2976932740-3244455291-537790045-1105
- TargetUserName = my-admin
- TargetDomainName = CORP
- TargetLogonId = 0x00000000000f133c
- LogonType = 3
- LogonProcessName = NtLmSsp
- AuthenticationPackageName = NTLM WorkstationName = USER-WS
- LogonGuid = {00000000-0000-0000-0000-000000000000} TransmittedServices = - LmPackageName =
  NTLM V1 KeyLength = 128 ProcessId = 0x0000000000000000 ProcessName = - IpAddress =
  192.168.89.101 IpPort = 49286
Command: psexec.exe \\admin-ws cmd.exe
Comment: Succesful logon. TargetLogonId = 0x00000000000f133c


Time: 06:33:32
Event: 4634
Event content:
- TargetUserSid = S-1-5-21-2976932740-3244455291-537790045-1105
- TargetUserName = my-admin
- TargetDomainName = CORP
- TargetLogonId = 0x00000000000f133c
- LogonType = 3
Comment: TargetLogonId = 0x00000000000f133c

Time: 06:33:35
Event: 4672
Event content:
- SubjectUserSid = S-1-5-21-2976932740-3244455291-537790045-1105
- SubjectUserName = my-admin
- SubjectDomainName = CORP
- SubjectLogonId = 0x00000000000f2736
- PrivilegeList = SeSecurityPrivilege   SeBackupPrivilege   SeRestorePrivilege
  SeTakeOwnershipPrivilege   SeDebugPrivilege   SeSystemEnvironmentPrivilege
  SeLoadDriverPrivilege   SeImpersonatePrivilege

Time: 06:33:35
Event: 4624
Event content:
- SubjectUserSid = S-1-0-0 SubjectUserName = - SubjectDomainName = - SubjectLogonId =
  0x0000000000000000 TargetUserSid = S-1-5-21-2976932740-3244455291-537790045-1105
- TargetUserName = my-admin
- TargetDomainName = CORP
- TargetLogonId = 0x00000000000f2736
```

```
- LogonType = 3
- LogonProcessName = NtLmSsp
- AuthenticationPackageName = NTLM
- WorkstationName = USER-WS
- LogonGuid = {00000000-0000-0000-0000-000000000000} TransmittedServices = - LmPackageName =
  NTLM V1 KeyLength = 128 ProcessId = 0x0000000000000000 ProcessName = -
- IpAddress = 192.168.89.101 IpPort = 49298
Command: robocopy.exe c:\goodies\sch \\admin-ws\c$

Time: 06:34:02
Event: 4634
Event content:
- TargetUserSid = S-1-5-21-2976932740-3244455291-537790045-1105
- TargetUserName = my-admin
- TargetDomainName = CORP
- TargetLogonId = 0x00000000000f2736
- LogonType = 3

Time: 06:34:15
Event: 4672
Event content:
- SubjectUserSid = S-1-5-21-2976932740-3244455291-537790045-1105
- SubjectUserName = my-admin SubjectDomainName = CORP
- SubjectLogonId = 0x00000000000f309b
- PrivilegeList = SeSecurityPrivilege   SeBackupPrivilege   SeRestorePrivilege
  SeTakeOwnershipPrivilege   SeDebugPrivilege   SeSystemEnvironmentPrivilege
  SeLoadDriverPrivilege   SeImpersonatePrivilege  LogonId = 0x00000000000f309b

Time: 06:34:15
Event: 4624
Event content:
- SubjectUserSid = S-1-0-0 SubjectUserName = - SubjectDomainName = - SubjectLogonId =
  0x0000000000000000 TargetUserSid = S-1-5-21-2976932740-3244455291-537790045-1105
- TargetUserName = my-admin
- TargetDomainName = CORP
- TargetLogonId = 0x00000000000f309b
- LogonType = 3
- LogonProcessName = NtLmSsp
- AuthenticationPackageName = NTLM
- WorkstationName = USER-WS
- LogonGuid = {00000000-0000-0000-0000-000000000000} TransmittedServices = - LmPackageName =
  NTLM V1 KeyLength = 128 ProcessId = 0x0000000000000000 ProcessName = -
- IpAddress = 192.168.89.101 IpPort = 49299
Command: at.exe \\admin-ws 08:00 c:\schedule.bat
Comment: LogonId = 0x00000000000f309b

Time: 06:34:26
Event: 4634
Event content:
- TargetUserSid = S-1-5-21-2976932740-3244455291-537790045-1105
- TargetUserName = my-admin
- TargetDomainName = CORP
- TargetLogonId = 0x00000000000f309b
- LogonType = 3
Comment: LogonId = 0x00000000000f309b
```

6.2 Kerberos authentication and Pass-the-Ticket events

6.2.1 Domain Controller events

We see, on the Domain Controller, that a Kerberos service ticket was requested to access the `admin-ws` host from the IP address of the `user-ws` machine (`192.168.86.101` , event-id 4769).

Notice that there is no event-id 4768 (Kerberos TGT request). This is in line to the fact that the ticket was stolen and re-injected in the attack.

```
Time: 14:11:12
Event: 4769
Event content:
- TargetUserName = myadmin@corp
- TargetDomainName = corp
- ServiceName = ADMIN-WS$
- ServiceSid = S-1-5-21-2976932740-3244455291-537790045-1107
- TicketOptions = 0x40810000
- TicketEncryptionType = 0x00000012
- IpAddress = ::ffff:192.168.89.101 IpPort = 49407
- Status = 0x00000000
- LogonGuid = {B757831E-D810-CDCC-C1C2-804BB3A2FB2C}
- TransmittedServices = -
Command: net use \\admin-ws
```

6.2.2 Target host events (`admin-ws`)

We see two events related to accounts successfully logged on the target machine (event-id 4624). As on the DC, none of them indicate it is a golden ticket.

```
Time: 14:11:12
Event: 4624
Event content:
- SubjectUserSid = S-1-0-0 SubjectUserName = - SubjectDomainName = - SubjectLogonId =
  0x0000000000000000
- TargetUserSid = S-1-5-21-2976932740-3244455291-537790045-500 TargetUserName = myadmin
  TargetDomainName = corp
- TargetLogonId = 0x000000000051f916
- LogonType = 3 LogonProcessName = Kerberos AuthenticationPackageName = Kerberos
- WorkstationName =
- LogonGuid = {A0706C8D-9BC6-F4D5-1226-FA2A48BB58D9} TransmittedServices = - LmPackageName = -
   KeyLength = 0 ProcessId = 0x0000000000000000 ProcessName = -
- IpAddress = 192.168.89.101 IpPort = 49406
Command: net use \\admin-ws

Time: 14:11:12
Event: 4672
Event content:
- SubjectUserSid = S-1-5-21-2976932740-3244455291-537790045-500 SubjectUserName = myadmin
- SubjectDomainName =
- SubjectLogonId = 0x000000000051f916
- PrivilegeList = SeSecurityPrivilege SeBackupPrivilege SeRestorePrivilege
  SeTakeOwnershipPrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeLoadDriverPrivilege
   SeImpersonatePrivilege
Command: net use \\admin-ws

Time: 14:11:39
```

```
Event: 4624
Event content:
- SubjectUserSid = S-1-0-0 SubjectUserName = - SubjectDomainName = - SubjectLogonId =
  0x0000000000000000
- TargetUserSid = S-1-5-21-2976932740-3244455291-537790045-500 TargetUserName = myadmin
  TargetDomainName = corp
- TargetLogonId = 0x00000000005204ad
- LogonType = 3 LogonProcessName = Kerberos AuthenticationPackageName = Kerberos
- WorkstationName =
- LogonGuid = {B504E2E8-3007-1C03-F480-011559C08D34} TransmittedServices = - LmPackageName = -
   KeyLength = 0 ProcessId = 0x0000000000000000 ProcessName = -
- IpAddress = 192.168.89.101 IpPort = 49409
Command: psexec.exe \\admin-ws cmd.exe

Time: 14:11:39
Event: 4672
Event content:
- SubjectUserSid = S-1-5-21-2976932740-3244455291-537790045-500 SubjectUserName = myadmin
  SubjectDomainName =
- SubjectLogonId = 0x00000000005204ad
- PrivilegeList = SeSecurityPrivilege SeBackupPrivilege SeRestorePrivilege
  SeTakeOwnershipPrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeLoadDriverPrivilege
   SeImpersonatePrivilege
Command: psexec.exe \\admin-ws cmd.exe
```

6.3 Annex D – Security Windows events

This section depicts the main security events discussed in this paper. Extracted from Microsoft definition [5],[6].

Event ID: 4624 An account was successfully logged on.

```
Subject:
 Security ID:  %1
 Account Name:  %2
 Account Domain:  %3
 Logon ID:  %4

Logon Type:   %9

New Logon:
 Security ID:  %5
 Account Name:  %6
 Account Domain:  %7
 Logon ID:  %8
 Logon GUID:  %13

Process Information:
 Process ID:  %17
 Process Name:  %18

Network Information:
 Workstation Name: %12
 Source Network Address: %19
 Source Port:  %20

Detailed Authentication Information:
 Logon Process:  %10
```

```
 Authentication Package: %11
 Transited Services: %14
 Package Name (NTLM only): %15
 Key Length:  %16

This event is generated when a logon session is created. It is generated on the computer that
  was accessed.
The subject fields indicate the account on the local system which requested the logon. This is
   most commonly a service such as the Server service, or a local process such as Winlogon.exe
   or Services.exe.
The logon type field indicates the kind of logon that occurred. The most common types are 2
  (interactive) and 3 (network).
The New Logon fields indicate the account for whom the new logon was created, i.e. the account
   that was logged on.
The network fields indicate where a remote logon request originated. Workstation name is not
  always available and may be left blank in some cases.
The authentication information fields provide detailed information about this specific logon
  request.
 - Logon GUID is a unique identifier that can be used to correlate this event with a KDC
  event.
 - Transited services indicate which intermediate services have participated in this logon
  request.
 - Package name indicates which sub-protocol was used among the NTLM protocols.
 - Key length indicates the length of the generated session key. This will be 0 if no session
  key was requested.
```

Event ID: 4625 An account failed to log on.

```
Subject:
 Security ID:  %1
 Account Name:  %2
 Account Domain:  %3
 Logon ID:  %4

Logon Type:   %11

Account For Which Logon Failed:
 Security ID:  %5
 Account Name:  %6
 Account Domain:  %7

Failure Information:
 Failure Reason:  %9
 Status:   %8
 Sub Status:  %10

Process Information:
 Caller Process ID: %18
 Caller Process Name: %19

Network Information:
 Workstation Name: %14
 Source Network Address: %20
 Source Port:  %21

Detailed Authentication Information:
 Logon Process:  %12
 Authentication Package: %13
 Transited Services: %15
 Package Name (NTLM only): %16
```

```
 Key Length:  %17

This event is generated when a logon request fails. It is generated on the computer where
  access was attempted.

The Subject fields indicate the account on the local system which requested the logon. This is
   most commonly a service such as the Server service, or a local process such as Winlogon.exe
   or Services.exe.

The Logon Type field indicates the kind of logon that was requested. The most common types are
   2 (interactive) and 3 (network).

The Process Information fields indicate which account and process on the system requested the
  logon.

The Network Information fields indicate where a remote logon request originated. Workstation
  name is not always available and may be left blank in some cases.

The authentication information fields provide detailed information about this specific logon
  request.
 - Transited services indicate which intermediate services have participated in this logon
  request.
 - Package name indicates which sub-protocol was used among the NTLM protocols.
 - Key length indicates the length of the generated session key. This will be 0 if no session
  key was requested.
```

Event ID: 4634 An account was logged off.

```
Subject:
 Security ID:  %1
 Account Name:  %2
 Account Domain:  %3
 Logon ID:  %4

Logon Type:   %5

This event is generated when a logon session is destroyed. It may be positively correlated
  with a logon event using the Logon ID value. Logon IDs are only unique between reboots on
  the same computer.

Event ID: 4647
User initiated logoff.

Subject:
 Security ID:  %1
 Account Name:  %2
 Account Domain:  %3
 Logon ID:  %4

This event is generated when a logoff is initiated but the token reference count is not zero
  and the logon session cannot be destroyed.  No further user-initiated activity can occur.
  This event can be interpreted as a logoff event.
```

Event ID: 4648 A logon was attempted using explicit credentials.

```
Subject:
 Security ID:  %1
 Account Name:  %2
 Account Domain:  %3
```

```
 Logon ID:  %4
 Logon GUID:  %5

Account Whose Credentials Were Used:
 Account Name:  %6
 Account Domain:  %7
 Logon GUID:  %8

Target Server:
 Target Server Name: %9
 Additional Information: %10

Process Information:
 Process ID:  %11
 Process Name:  %12

Network Information:
 Network Address: %13
 Port:   %14

This event is generated when a process attempts to log on an account by explicitly specifying
  that accounts credentials. This most commonly occurs in batch-type configurations such as
  scheduled tasks, or when using the RUNAS command.
```

Event ID: 4672 Special privileges assigned to new logon.

```
Subject:
 Security ID:  %1
 Account Name:  %2
 Account Domain:  %3
 Logon ID:  %4

Privileges:  %5
```

Event ID: 4768 A Kerberos authentication ticket (TGT) was requested.

```
Account Information:
 Account Name:  %1
 Supplied Realm Name: %2
 User ID:   %3

Service Information:
 Service Name:  %4
 Service ID:  %5

Network Information:
 Client Address:  %10
 Client Port:  %11

Additional Information:
 Ticket Options:  %6
 Result Code:  %7
 Ticket Encryption Type: %8
 Pre-Authentication Type: %9

Certificate Information:
 Certificate Issuer Name:  %12
 Certificate Serial Number: %13
 Certificate Thumbprint:  %14
```

```
Certificate information is only provided if a certificate was used for pre-authentication.

Pre-authentication types, ticket options, encryption types and result codes are defined in RFC
   4120.
```

Event ID: 4769 A Kerberos service ticket was requested.

```
Account Information:
 Account Name:  %1
 Account Domain:  %2
 Logon GUID:  %10

Service Information:
 Service Name:  %3
 Service ID:  %4

Network Information:
 Client Address:  %7
 Client Port:  %8

Additional Information:
 Ticket Options:  %5
 Ticket Encryption Type: %6
 Failure Code:  %9
 Transited Services: %11

This event is generated every time access is requested to a resource such as a computer or a
  Windows service.  The service name indicates the resource to which access was requested.

This event can be correlated with Windows logon events by comparing the Logon GUID fields in
  each event.  The logon event occurs on the machine that was accessed, which is often a
  different machine than the domain controller which issued the service ticket.

Ticket options, encryption types, and failure codes are defined in RFC 4120.
```

Event ID: 4776 The domain controller attempted to validate the credentials for an account.

```
Authentication Package: %1
Logon Account: %2
Source Workstation: %3
Error Code: %4
```