GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Advanced Incident Response, Threat Hunting, and Digital Forensics (Forensics
at http://www.giac.org/registration/gcfa

Windows Logon Forensics

GIAC (GCFA) Gold Certification

Author: Sunil Gupta, sgupta911@gmail.com
Advisor: Hamed Khiabani

Accepted: January 30, 2013

© 2013 SANS Institute Author retains full rights.

Abstract

A compromised Windows® system's forensic analysis may not yield much relevant information about the actual target. Microsoft® Windows Operating System uses a variety of logon and authentication mechanisms to connect to remote systems over the network. Incident Response and Forensic Analysis outcomes are prone to errors without proper understanding of different account types, Windows logons and authentication methods available on a Windows platform. This paper walks thru the logon and authentication and how they are audited for various Windows account types' logons for a successful investigation. In the process it describes common authentication protocols such as Kerberos, NTLM to better understanding of the logon process communications in the Windows environment.

1. Introduction

Digital forensics, also known as computer and network forensics, is the application of science to the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data. The forensic analysis goal is to gain a better understanding of an event of interest by finding and analyzing the facts related to that event. Forensics may be needed in many different situations, such as evidence collection for legal proceedings and internal disciplinary actions, and handling of malware incidents and unusual operational problems (Kent, Chevalier, Grance & Dang, 2006).

According to the NIST Guide to Electronic Authentication Guideline (Burr, Dodson, Newton, Perlner, Polk, Gupta & Nabbus, 2011), the Authentication is a process of establishing confidence in the identity of users or information systems. The Authentication protocol is a defined sequence of messages between a Claimant and a Verifier that demonstrates that the Claimant has possession and control of a valid token to establish his/her identity, and optionally, demonstrates to the Claimant that he or she is communicating with the intended Verifier. The authorization process is different from the authentication process. With authentication, the system proves that you are who you say you are. However with authorization, the system verifies that you have rights to do what you want to do.

Microsoft Windows is a complex operating system with a tempting target due to its pervasiveness and due to perceived insecurities within these systems (Broersma, 2005). Microsoft Windows is still considered the low-hanging fruit. With 92% share of the PC market and a two-thirds share of all Internet-connected devices, Windows is the obvious target for attackers looking to make money or to achieve other goals (Goldman, 2012).The main thesis of this paper is to provide enough details about the Windows logons, authentication and how they can be audited on the Windows system or over the network for forensic analysis. This paper does not cover the authorization methods and the security hardening of a Windows system or Windows network.

© 2013 SANS Institute, Author retains full rights.

1.1. Outline

This paper describes the Windows Logon and Authentication technologies in a Microsoft Windows environment. The paper further explains the auditing and analysis of logon events required for a successful incident investigation. Chapter 2 provides an overview of the Windows Logon and Authentication. Chapter 3 explains the possible Windows Logon types. Chapter 4 goes in further details of the Kerberos and NTLM authentication protocol to better understand the communication common to Microsoft network. Chapter 5 discusses on the Windows account types and the Windows Logon and Authentication events logged for the respective logons. Final chapter 6 elaborates over the filtering and decoding of logon events, and tracking a user for the analysis. There is an illustration of logon traffic and event analysis of the corresponding Windows event ids in the Appendix section.

1.2. Problem Addressed

Microsoft Windows' various technology features, ease of use and GUI approach while easy on outside, implements a complex set of security technologies under the cover. Multiple Operating System versions, types and backward compatibility add further more to this. Windows Logon is one critical and a complex part of Windows security. Windows provides different types of accounts which are managed differently. Windows uses multiple authentication protocols giving multiple ways to access resources. Some of the security log events have changed with the Operating System enhancements. Microsoft has updated the event logging system with many improvements on Windows 2008/Vista onwards which has further increased the level of complexity.

In Windows' world, Logon events, and Account Logon events, also known as Authentication events, are different, and Windows auditing logs these events differently based on Windows Operating System version, Account type, logon type etc. This document tries to make sense of all these factors for an Incident Responder and Forensic Analyst doing an investigation. This paper illustrates the Kerberos and NTLM authentication protocols briefly in this context to understand ongoing activities on the network from the security perspective. Without thorough consideration of the all different Logons to and from the compromised machine to remote system in the Windows network can yield incomplete results and undermine an investigation.

© 2013 SANS Institute, Author retains full rights.

2. Windows Authentication Overview

Microsoft Windows operating systems allow implementing a variety of authentication technologies based on an organization's complexity, the quality of a user's credentials, network access methodologies, and the clients operating systems used for the access. Windows authentication methods range from a simple logon based on something the user knows like a password, to more powerful secure technique using something user has like tokens, public key certificates, and biometrics. Authentication is commonly required to adapt to the more complex business environment having many types of servers in one or more locations and users spread across multiple locations using multiple applications with a variety of access methods (Microsoft TechNet, 2003).

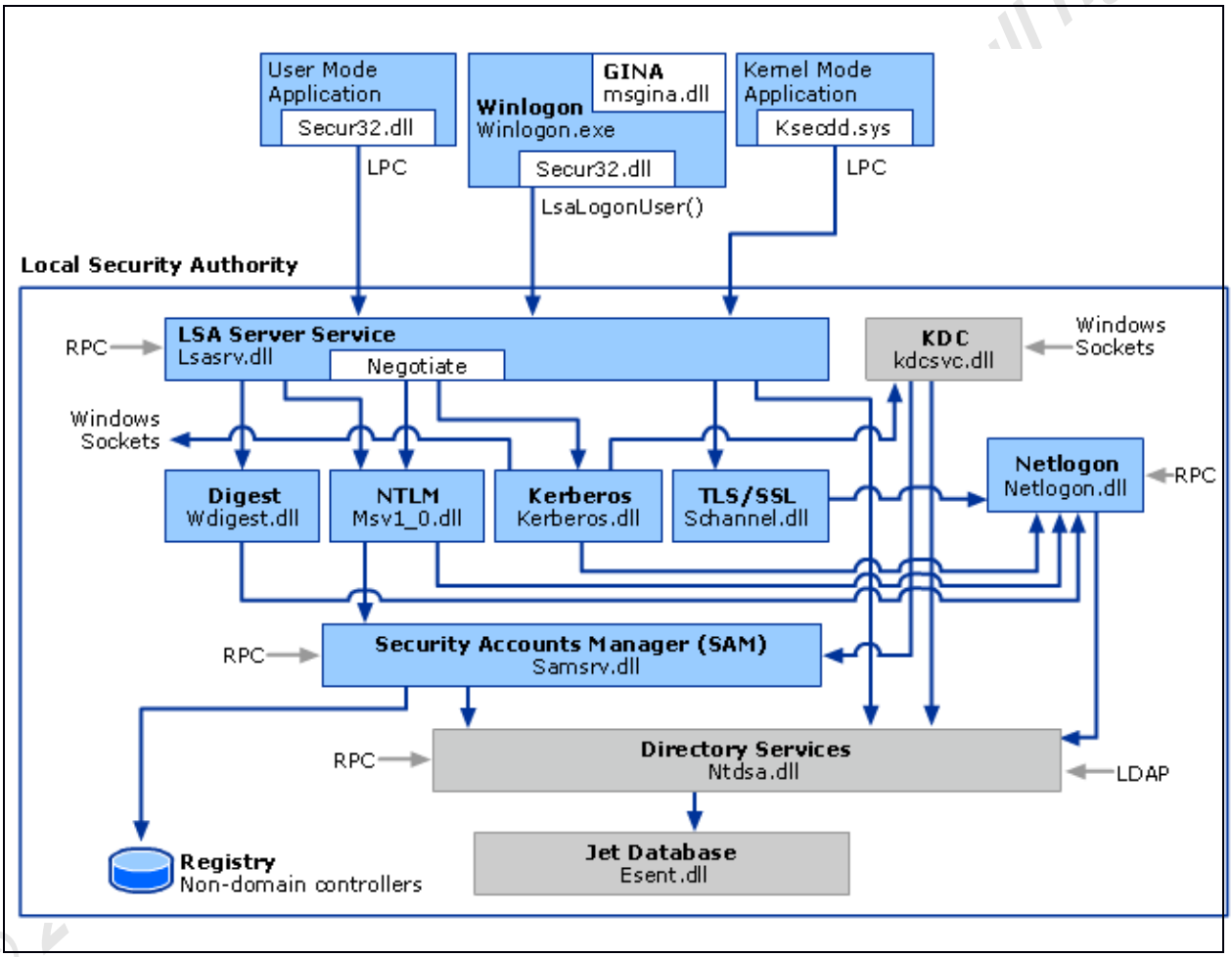
The Microsoft Windows operating system's default set of authentication protocols include Negotiate, Kerberos, NTLM, Schannel (secure channel), and Digest, as part of the Windows security subsystem architecture. These protocols define rules and conventions, and serve the authentication of users, computers, and services. The authentication process allows authorized users and services to access resources in a secure way (Microsoft TechNet, 2003). In a Microsoft Active Directory domain environment, cryptographic keys are stored in a secure central location making the authentication process to be scalable and maintainable.
Active Directory directory service is the default and recommended technology that stores users and computer's credentials and identity information including the cryptographic keys (Microsoft TechNet, 2012).

© 2013 SANS Institute, Author retains full rights.

2.1. Security Subsystem Architecture

Windows operating systems security model includes a set of security components that ensures that users and applications cannot gain access to resources without proper authentication and authorization. The Local Security Authority (LSA), a protected subsystem, authenticates and logs user access on to the local system. LSA also defines the local security policy to maintain the local security configuration on a computer, and it provides various services for security identifiers (SIDs) name translation. This security subsystem tracks the effective security policies and the accounts used on a computer system (Microsoft TechNet, 2003).

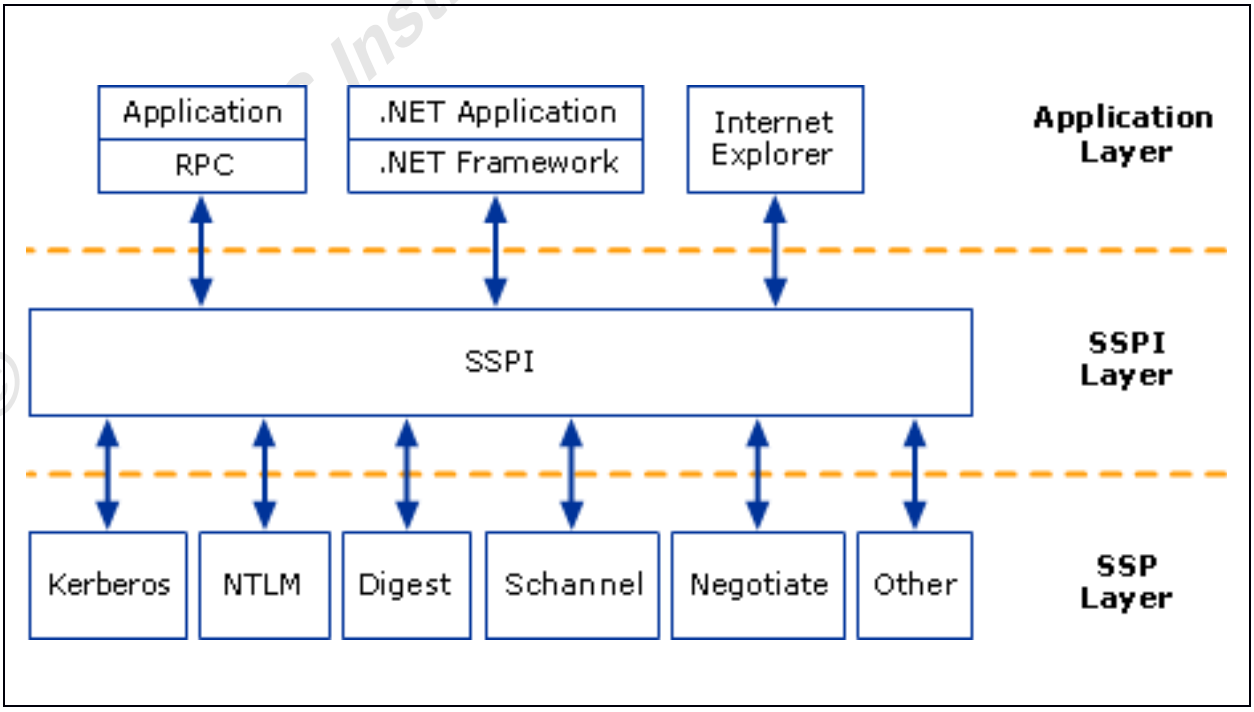
For the domain controller, these are the security policies and accounts effective for the respective domain, and are stored in Active Directory. The local security policy identifies the user logons, user rights, domain trusts, security auditing and pool memory quotas (Microsoft TechNet, 2003). This diagram below displays the LSA architecture security subsystem and it's components on Windows OS.



LSA Architecture (Microsoft TechNet, 2003).

2.2. Microsoft Security Support Provider Interface (SSPI)

The Microsoft Security Support Provider Interface (SSPI) provides the base for the authentication in Windows Operating System. SSPI provides authentication services to applications and infrastructure services on Windows computer or network. The SSPI mechanism allows carrying authentication tokens between the two parties over the existing communication channel. With the SSPI an application can use various security models available on a computer or network for authentication without changing the security system interface. The security support providers (SSPs) are the implementation of the authentication protocols installed in the form of dynamic link libraries (DLLs). The default SSPs are Negotiate (SPNEGO), Kerberos, NTLM, Schannel, and Digest authentication protocols plugged into the SSPI. SSPI provides custom plug-in approach for additional SSPs for interoperability. When one party authenticates with another, authentication requests are routed to the SSPI, which in turn, transferred to one of the SSP, completing the authentication process, regardless of the network protocol currently in use (Microsoft TechNet, 2003). This diagram below depicts the basic SSPI architecture and it's components on Windows OS.



SSPI Architecture (Microsoft TechNet, 2003).

© SANS Institute. Author retains full rights.

2.3. Security Support Providers (SSP)

Here are the SSPs, the authentications protocols that are plugged into the SSPI. These protocols are used in different ways to provide secure authentication.

Kerberos

The Kerberos version 5 (v5) is an industry standard protocol used for logon authentication. The Kerberos authentication protocol provides a mechanism for authentication, and mutual authentication between the two parties such as client and server or server and server. Beginning with Windows Server 2000, Kerberos is the preferred authentication method for services and is the authentication protocol of choice for Active Directory authentication requests. Microsoft's default Kerberos implementations require Active Directory domain service infrastructure set up. Kerberos v5 protocol is implemented as an SSP, which is accessible through the SSPI discussed earlier. Windows also includes extensions to this standard protocol that permit initial authentication using public key certificates on smart cards. (Microsoft TechNet, 2011).

NTLM

NTLM, NT LAN Manager, has been around since Windows has had networking support dating back to the LAN Manager days, thus this name. The NTLM protocol is the default network authentication protocol used in the Windows NT 4.0 operating system. It is a challenge-response protocol that is now used to provide compatibility with versions of Windows earlier than Windows 2000.The NTLM authentication protocols include LAN Manager version 1 and 2, and NTLM version 1 and 2. They all follow the same authentication process, but they differ in the level of encryption hence the level of security (Northup & Thomas, 2004).The NTLM authentication protocols authenticate client based on a challenge-response mechanism that proves to a server that the client knows the password associated with that account. NTLM protocol also optionally provides for session security, specifically message integrity and message confidentiality through signing and sealing functions (Microsoft TechNet, 2012).

© 2013 SANS Institute, Author retains full rights.

Negotiate

Microsoft Negotiate SSP acts as an application layer between the Security Support Provider Interface (SSPI) and the other SSPs. This SSP is used to negotiate a specific authentication protocol. Application specifies the SSP such as Kerberos, NTLM to process the logon request when making calls into SSPI for authentication. If the application specifies Negotiate SSP, Negotiate analyzes the request and handles it to the best SSP based on system's security policy configuration. Negotiate SSP currently selects from either the Kerberos or NTLM protocol. Negotiate selects the Kerberos as the preferred default protocol unless it cannot be used by one of the systems involved in the authentication or other restrictions apply which doesn't make Kerberos authentication possible such as incomplete a user principal name (UPN), service principal name (SPN), or a NetBIOS account name in the request.

Digest authentication

The Digest authentication is an industry standards based authentication protocol that is used for Lightweight Directory Access Protocol (LDAP) and web authentication. Digest protocol is a challenge-response protocol that transmits credentials across the network using secret keys such as an MD5 hash or message digest.

Schannel

The Schannel, secure channel, SSP implements the Secure Sockets Layer/Transport Layer Security (SSL/TLS) internet standard authentication protocols. Schannel is used for Web based server authentication such as user accessing a secure Web server. The SSL/TLS protocols are used to provide mutual authentication between the two parties in a client server fashion, and also to encrypt messages providing message confidentiality between them. The SSL/TLS protocols, versions 2.0 and 3.0 are based on public key cryptography.

2.4. Windows Security Terms

This section describes some Windows important terms for a security investigator to know.

Active Directory

Active Directory, first released with Windows 2000, is an implementation of LDAP directory service designed to handle a very large number of read and search, and significantly low number of write and modify operations. Active directory gets installed on the Windows

© 2013 SANS Institute, Author retains full rights.

server when it is promoted to become a domain controller. Active Directory is required for default NTLM and Kerberos implementations. Active Directory maintains a shared account database for the domain environment which allows for the Windows domain authentication, group memberships, group policy assignments and other services. Active Directory data is replicated among the domain controllers. The Active Directory database consists of many different types of objects such as users, groups etc, and attributes such as user's last name, logon name. Active Directory Schema defines the objects and attributes used to store data. Active Directory data is hierarchical and extensible which allows for the Active directory schema to be extended (MSDN, 2012).

Security identifier (SID)

A security identifier (SID) is a unique value that identifies a security principal or security group in Windows operating systems. Well known generic users or generic groups such as default Administrator or Guest account have defined well known SIDs which remains constant across all Windows operating systems. Users' account names are referred by the operating system internally by their SIDs. Domain account SID is created by concatenating the SID of the domain with a relative identifier (RID) for the account. SIDs are unique within their scope such as domain or local, and are never reused. Account SID is created at the time of a particular account creation. Local account or group SID is generated by the Local Security Authority (LSA) on the computer and is stored in a secure area of the registry also known as Security Account Manager (SAM). Domain account or group SID is generated by the domain security authority and is stored as an attribute of that User or Group object in Active Directory (Microsoft TechNet, 2003). Sometimes, an Investigator might see SID instead of the respective user or group name in the GUI due to GUI display or SID resolving problems.

Security Access Token (SAT)

An access token object describes the security context of a process or thread. Access token is created for the user after the user is logged on and authenticated successfully. It includes the identity and privileges of the user account associated with the process or thread. Thereafter, every process executed for this user has a copy of this access token. The system uses an access token to verify the user's identity and privileges when a thread interacts with a securable object. Access tokens contain the information such as user's account SID, SIDs for the user's groups,

© 2013 SANS Institute, Author retains full rights.

logon SID identifying the current logon session, a list of the privileges held by either the user or the user's groups etc (MSDN, 2012).

Access Control List (ACL)

The access control list (ACL) is a list of access control entries (ACE). Each ACE in an ACL identifies an account and specifies that account's the access rights such as allowed, denied, or audited. There are two types of ACLs: a DACL and a SACL. A discretionary access control list (DACL) identifies a set of permissions on a securable object such as files, folder, registry entry etc. The system checks the ACEs in the object's DACL to determine the access when a process tries to access that securable. A system access control list (SACL) configures the auditing for the secured object access. Each ACE is SACL specifies the types of access attempts by specified accounts to log in the security event log (MSDN, 2012).

© 2013 SANS Institute, Author retains full rights.

3. Logon Process Scenarios

This section describes the different logon scenarios permitted on the Windows system.

3.1. Interactive Logon

In an Interactive logon, user enters credentials into the Log On to Windows dialog box or user inserts a smart card into the smart card reader. User's authentication is then checked against the security database on the user's local computer or to an Active Directory domain. User can perform an interactive logon in two different ways:

1. Locally, when the user has direct access to the console.
2. Remotely, through Terminal Services.

`Logon type 2` is logged when a user logs on at the console whether it is domain or a local user account. Logons through Terminal Services, Remote Desktop or Remote Assistance are qualified as `remote interactive` and logs the logon attempt with `logon type 10`. Prior to Windows XP, Windows 2000 only used logon type 2 for all the interactive logons (Microsoft TechNet, 2003).

Local Logon

In a local logon, user logs on using the user account in the Security Accounts Manager (SAM) on that local computer. A local logon grants access only to that computer's resources. Local user and group membership from SAM is used to manage access to local resources (Microsoft TechNet, 2003).

Domain Logon

In a domain user logon, user specifies the domain for which user is logging on. A domain logon requires that the user as well as computer have accounts in the corresponding Active Directory domain(s). User needs to have the user rights to log on to a local computer or a domain. Domain user account and group membership information are used to manage user's access to local and domain resources (Microsoft TechNet, 2003).

Smart Card Logon

Smart card logon does not require pressing CTRL+ALT+DEL to enter credentials into the Log On to Windows dialog box. For logon, the smart card is inserted into the smart card reader of the computer and it then prompts for the user's personal identification number (PIN) instead of the user name and password. A Smart card logon provides stronger form of authentication because users need to possess the card as well as remember the PIN making it a two factor authentication, and it also utilizes cryptography-based identification.

3.2. Network Logon

Network logon are very common to Windows environment. They are only used after an account authentication such as user, computer, service has already taken place. For network logon, the process does not use the initial logon dialog box to enter the credentials. Instead, already established credentials for the account are used, or credentials are collected using in a different way. This is typically invisible to the user unless alternate credentials are used. Network logon confirms the users' identification to the network service such as mapped drive on another server that the user is attempting to access (Microsoft TechNet, 2003). Windows logs `logon type 3` for network logons such as accessing shared folders, printers, GPOs, and most logons to IIS.

© 2013 SANS Institute, Author retains full rights.

3.3. Batch

For a scheduled task execution in Windows, the Scheduled Task service first creates a new logon session for the task so that it can run under the user account specified for that task. Windows logs this logon attempt as `logon type 4`. Some job scheduling systems or other application, depending on their design, may also generate logon events with `logon type 4` (Smith, 2005).

3.4. Service

Windows services are configured to run under specified user accounts individually. Starting of a service first creates a logon session for the specified user account which results in a Logon/Logoff event with `logon type 5` (Smith, 2005).

3.5. Unlock

This occurs when a user returns to the console and unlocks the password protected screen. Windows treats this as a logon and logs the appropriate Logon/Logoff event using `logon type 7` identifying the event as an unlock attempt.

3.6. NetworkCleartext

This is a kind of network logon where the password is sent over the network in the clear text. This is logged as `logon type 8`. Windows server doesn't allow connection to shared file or printers with clear text authentication. It is possible with logons from within an ASP script using the ADVAPI or when a user logs on to IIS using IIS's basic authentication mode. In both cases the logon process in the event's description will list `advapi` (Smith, 2005).

3.7. NewCredentials

Using `RunAs` command to start a program under a different user account with the /netonly switch, Windows records a logon/logoff event with `logon type 9`. When starting a program with `RunAs` using `/netonly`, the program executes on the local computer as the user currently logged on as but for any connections to other computers on the network, Windows connects to those computers using the account specified on the `RunAs` command. Without `/netonly` Windows runs the program on the local computer and on the network as the specified user and records the logon event with `logon type 2` (Smith, 2005).

© 2015 SANS Institute, Author retains full rights.

3.8. CachedInteractive

Windows Cached Logons feature facilitates mobile users that allow caching credentials hashes of the last 10 interactive domain logons by default. When client is off the network or when no domain controller is available, Windows uses these hashes to verify the identity of the logon with a domain account. It is logged with `logon type 11` (Smith, 2005).

4. Accessing Resources

Kerberos version 5 is the default authentication protocol and protocol of choice for Active Directory authentication access requests for the Windows environment. NTLM is used in Active Directory domains to process network authentication for compatibility reasons. NTLM authentication protocol is also used for computers that are not participating in a domain, such as stand-alone servers and workgroups. When the NTLM protocol is used between a client and a server in a domain, the server forwards the client credentials to a domain controller in the client account domain to verify the client credentials. In the case of Kerberos protocol, the client gets a ticket for a server by requesting one from a domain controller in the server account domain and then the server validates the ticket. The resource server does not have to contact the domain controller or any other authority for access in this case. Resource access is further explained using these protocols in this section.

4.1. Kerberos Authentication and Resource Access

Kerberos authentication is designed to work with specially formatted data packets known as `tickets`. These `tickets` pass through the network instead of passwords which makes the authentication process more resistant to attackers who can intercept the network traffic (Northup & Thomas, 2004). Active Directory Domain Services is required for default Kerberos implementations in the domain or forest. The Kerberos Key Distribution Center (KDC) is integrated to work with other Windows Server security services running on the domain controller. The KDC utilizes the Active Directory Domain Services database as its security account database (Microsoft TechNet, 2012). The Kerberos ticket request flow is described in the picture below and is broken into three main exchanges such as The Authentication Service Exchange, The Ticket-Granting Service Exchange and The Client/Server Exchange as described afterwards:

© 2013 SANS Institute, Author retains full rights.

Kerberos authentication and resource access

1. Kerberos authentication service request (KRB_AS_REQ): When trying to logon, the client contacts the KDC's authentication service for a short-lived ticket, a message containing the client's identity such as SIDs, called a ticket granting ticket (TGT).

2. Kerberos authentication service response (KRB_AS_REP): The authentication service (AS) constructs a limited lifetime TGT and creates a session key that the client uses to encrypt communication with the ticket granting service (TGS). Client has not been granted access to any local or domain resources at this point.

3. Kerberos ticket granting service request (KRB_TGS_REQ): When the client wants access to a resource, the client sends a request to the TGS for a ticket for that resource such as local or network server or service. This ticket is also called as the service ticket (ST) or session ticket. The client submits the TGT, an authenticator, and the name of the target resource using the Server Principal Name (SPN) to TGS to receive the service ticket.

4. Kerberos ticket granting service response (KRB_TGS_REP): The TGS examines the TGT and the authenticator and creates a service ticket if the TGT is acceptable. The client's identity is copied from the TGT to the service ticket and then service ticket is sent to the client.

5. Kerberos application server request (KRB_AP_REQ): After receiving the service ticket client sends the ticket and a new authenticator to the target resource server, requesting access. The server decrypts the service ticket, validate the authenticator, and for Windows services, create an access token for the user provided user has access based on the SIDs in the ticket.

6. Kerberos application server response (KRB_AP_REP): This step is optional. The client might request that the target server verify its own identity for mutual authentication. If requested, the target server takes the client's timestamp from the authenticator, encrypts it with the session key the TGS provided, and send it to the client (Microsoft TechNet, 2009).

© 2013 SANS Institute, Author retains full rights.

4.2. NTLM Authentication and Resource Access

NTLM provides a basic three way handshake mechanism for granting access to a server for a client. It provides a way for the server to prove the identity of the client without having to send clear text credentials across over a network. When user accesses a client computer and provides domain credentials, the client computes a cryptographic hash of the password and discards the actual password (GuyTe, 2010). NTLM protocol is quite chatty with the domain accounts resources accesses. With NTLM, a resource server must contact a domain authentication service on the domain controller for the domain accounts or look up the account in the local account database for local account to verify the identity of a computer or user whenever a new access token is needed (Microsoft TechNet, 2012). A typical resource access using NTLM authentication handshake is shown in the picture below and is described thereafter:

NTLM authentication and resource access

First, the user from the client machine tries to connect to the resource server to access a resource and sends the user account name to the server in plaintext. Next, the server generates a 16 byte random number, called a challenge, and sends it back to client machine. In third step, the client encrypts the challenge received with the hash of the user's password and returns this result to the server, called a response. Now, the server sends the user name, the challenge sent to the client, and the response received from the client to the domain controller for account authentication in fourth step. Next, domain controller uses the user name to retrieve the hash of the user's password from the SAM database. It uses this password hash to encrypt the challenge. The domain controller compares the encrypted challenge it computed to the response computed by the client in step three. If they are both identical, user account authentication is successful and the server is notified by the domain controller. The server notifies the client of the authentication and creates an access token for the user based on the SIDs, if the access is authorized (GuyTe, 2010).

© 2015 SANS Institute, Author retains full rights.

5. Logon Auditing and Logon Events

5.1. Logon Auditing

The audit security settings determine whether to audit each instance of a user logging on to or logging off from a computer. Enforcing audit settings helps in security incidents to be

detected and in collecting enough evidences for analysis of those incidents. Certain regulations such as SOX, HIPAA also require the auditing of certain events and activities. Domain member servers and workstations auditing settings for the event categories are undefined by default while domain controllers have auditing turned on by default. An appropriate audit policy that meets the security needs of an organization is created by defining auditing settings for desired event categories (Microsoft TechNet, 2005).

The security audit policy settings under `Computer Configuration\Windows Settings Security Settings\Local Policies\Audit Policy` provide broad security audit capabilities for client workstations and servers that cannot use advanced security audit policy settings. Windows workstations and servers such as Windows XP and Windows Server 2003, releases prior to Windows Vista and Windows 2008, does not allow advanced security audit policy settings configured for granularity. (Microsoft TechNet, 2009). These broad legacy audit security setting for `account logon` and `logon/logoff` events are configured by setting the appropriate `Success` and `Failure` check boxes.

```
# Account Logon audit GPO setting

Computer Configuration\Windows Settings\Security Settings\Local
Policies\Audit Policy\Audit account logon events

# Logon/Logff audit GPO setting

Computer Configuration\Windows Settings\Security Settings\Local
Policies\Audit Policy\Audit logon events
```

The Windows Server 2008 has detailed audit facilities that allow administrators to tune their audit policy with greater specificity. The client computers running Windows Vista and servers running Windows Server 2008 require logon scripts using `auditpol.exe` to apply these advanced security audit policy settings, else, only the basic local audit policy settings are applied as above. Microsoft made further improvements with Windows 7 and Windows Server 2008 R2 onwards that allow these advanced security audit policy settings to be configured using Group Policy (GPO) audit policy subcategory settings. This requires `Force audit policy subcategory settings` security setting to be enabled to favor the audit subcategories over the legacy audit policies.

According to the Center for Internet Security (CIS, 2012), enabling the legacy audit facilities outlined above in this section, it is probable that the performance of the system may be

© 2013 SANS Institute, Author retains full rights.

reduced and that the security event log may realize very high event volumes. Given this, it is recommended that Detailed Audit Policies be leveraged in favor over the legacy policies represented above. The CIS Guidance is provided for establishing the recommended state via GPO and `auditpol.exe`. For the Specialized Security Limited Functionality (SSLF) Member Server and SSLF Domain Controller profile(s), the Audit Logon and Audit Account Logon policy setting recommended value is `Success and Failure`. For the Enterprise Member Server and Enterprise Domain Controller profile(s), the Audit Logon and Audit Account Logon policy setting recommended value is `Success`. Audit Logoff policy setting recommended value is `Success` for all profiles (CIS, 2012).

GPO configuration is configured as following for the `account logon` and `logon/logoff` events to the recommended value prescribed above:

```
# Logon advanced audit GPO setting

Computer Configuration\Windows Settings\Security Settings\Advanced Audit
Policy Configuration\System Audit Policies - Local Group Policy
Object\Logon/Logoff\Audit Logon\Audit Policy: Logon-Logoff: Logon

# Logoff advanced audit GPO setting

Computer Configuration\Windows Settings\Security Settings\Advanced Audit
Policy Configuration\System Audit Policies - Local Group Policy
Object\Logon/Logoff\Audit Logoff\Audit Policy: Logon-Logoff: Logoff

# Account Logon advanced audit GPO setting

Computer Configuration\Windows Settings\Security Settings\Advanced Audit
Policy Configuration\System Audit Policies - Local Group Policy
Object\Account Logon\Audit Credential Validation\Audit Policy: Account
Logon: Credential Validation
```

Logon script can be set to run this `auditpol` commands and configure the detailed audit policy for `account logon` and `logon/logoff` events to the recommended value prescribed above:

```
# Enable Logon advanced audit GPO setting for success and failure
auditpol /set /subcategory:"Logon" /success:enable /failure:enable
```

© 2013 SANS Institute, Author retains full rights.

```
# Enable Logoff advanced audit GPO setting for success
auditpol /set /subcategory:"Logoff" /success:enable /failure:disable

# Enable Account Logon advanced audit GPO setting for success and failure
auditpol /set /subcategory:"Credential Validation" /success:enable
/failure:enable
```

Above defined audit settings are validated with the following `auditpol` commands:

```
# Audit Logon advanced audit setting

auditpol /get /subcategory:"Logon"


# Audit Logoff advanced audit setting

auditpol /get /subcategory:"Logoff"

# Audit Account Logon advanced audit setting

auditpol /get /subcategory:"Credential Validation"
```

© 2013 SANS Institute, Author retains full rights.

5.2. Account Logon Events

Audit `Account Logon` policy setting generates events for credential validation. These events occur on the machine which is authoritative for the credentials**.** These `Audit account logon events` could have been named `Audit authentication events` in the policy for more clarity. For domain accounts, the domain controller is authoritative. For local accounts, the local machine is authoritative. Since domain accounts are used much more frequently in enterprise environments than local accounts, most of the `Account Logon` events occur on the domain controllers which are authoritative for the domain accounts. However, these events can occur on any machine, and may occur in conjunction with or on separate machines from logon/logoff events (Fitzgerald, 2005). Here is the list of these event IDs across different Windows OS versions.

Author retains full rights.

Windows 2000 Family	Windows XP & 2003 Family	Windows Vista, 7, 8 & 2008, 2012 Family	Description
672	672	4768	An authentication service (AS) ticket was successfully issued and validated (2000). An authentication service (AS) ticket was requested (2008). It is logged on DC Only.
673	673	4769	A ticket granting service (TGS) ticket was granted. Win2003 and Win2008 use this for both successful and failed service ticket requests with the proper Kerberos result/failure code.
674	674	4770	A security principal renewed an AS ticket or TGS ticket.
675	675	4771	Preauthentication failed. This event is generated on a Key Distribution Center (KDC) for the Kerberos errors during authentication.
676	672	4768	Authentication ticket request failed. See the Kerberos Error Code.
677	673	4769	A TGS ticket was not granted (failed). This event 677 in Windows 2000 is replaced with 673 in Windows XP/2003 family) and 4769 with later versions with audit type/codes for failures.
678	678	4774	An account was successfully mapped for logon to a domain account. Not common.
680	680	4776	Account used for logon by. Logged for local user (local SAM) authentication. DC logs this event for NTLM authentication.
681	680	4776	Logon failure on Windows 2000 for NTLM authentication. A domain account logon was attempted. This event is replaced with 680 in Windows XP/2003 family and 4776 with Windows 2008/Vista onwards with the audit type/codes for failures.
682	682	4778	A user has reconnected to a disconnected terminal session.
683	683	4779	A user disconnected a terminal session without logging off.

5.3. Logon Events

The `Audit logon events` policy setting when enabled records all attempts to log on to the local computer, whether by using a domain account or a local account (Smith, 2012). Audit `Logon/Logoff` generates events for the creation and destruction of logon sessions. These events occur on the machine accessed**.** In the case of an interactive logon, these would be generated on the machine logged on to. In the case of network logon such as share access, these events would be generated on the machine hosting the resource that was accessed (Fitzgerald, 2005). Here is the list of these event IDs across different Windows OS versions.

Windows 2000 Family	Windows XP & 2003 Family	Windows Vista, 7, 8 & 2008, 2012 Family	Description
528	528	4624	Successful logon: A user successfully logged on to a computer. For information about the type of logon, see the next section.
529	529	4625	Logon failure. A logon attempt was made with an unknown user name or a known user name with a bad password. For Windows 2008 and above, event ID 4625 logs every failed logon attempt with failure status code regardless of logon type or type of account.
530	530	4625	Logon failure for a logon attempt to log on outside of the allowed time.
531	531	4625	Logon failure for a logon attempt using a disabled account.
532	532	4625	Logon failure for a logon attempt using an expired account.
533	533	4625	Logon failure. A logon attempt was made by a user who is not allowed to log on at this computer.
534	534	4625	Logon failure. The user attempted to log on with a type that is not allowed.
535	535	4625	Logon failure. The password for the specified account has expired.
536	536	4625	Logon failure. The Net Logon service is not active.
537	537	4625	Logon failure. The logon attempt failed for other reasons. In some cases, the reason for the logon failure may not be known.
538	538	4634	The logoff process was completed for a user.
539	539	4625	Logon failure. The account was locked out at the logon.
540	540	4624	Successful network logon: A user successfully logged on over a network.
538	551	4647	A user initiated the logoff process. It is logged for Interactive and RemoteInteractive logons in place of logoff event 538/4634.
552	552	4648	A user successfully logged on to a computer using explicit credentials while already logged on as a different user.
682	682	4778	A user has reconnected to a disconnected terminal session.
683	683	4779	A user disconnected a terminal session without logging off.

tains full rights.

6. Logon Analysis

Windows has the ability to generate a detailed audit record of security events on each system. Windows logs events for the two types of security accounts: `Computer` and `User` for their logon and authentication. Computer account authentication events list computer name for the user name and is recognized with `$` appended to the computer name. Windows system services and applications are configured to run under various different types of accounts. For example, a service or an application on a computer can access domain resources by using the network service, local system, or domain user accounts. This section explores how to analyze and differentiate these logon and authentication events.

6.1. Decoding Logon Types and Logon Codes

There are many different ways logon can occur to a computer. Logon/logoff events specify the `Logon Type` code which reveals the type of logon that prompted the event. When event `528` (Windows 2003, XP family) or event `4624` (Windows 2008/2012, Vista/7/8 family) is logged, a logon type is also listed in the event log. This table below describes these different logon types.

Logon Type	Logon Title	Description
2	Interactive	A user logged on from console to this computer.
3	Network	A user or computer logged on to this computer from the network.
4	Batch	Batch logon type is used by batch servers, where processes may be executing on behalf of a user without their direct intervention.
5	Service	A service was started by the Service Control Manager.
7	Unlock	This workstation was unlocked.
8	NetworkCleartext	A user logged on to this computer from the network. The user's password was passed to the authentication package in its unhashed form. The built-in authentication packages all hash credentials before sending them across the network. The credentials do not traverse the network in plaintext also called cleartext.

© SANS Institute. Author retains full rights.

9	NewCredentials	A caller cloned its current token and specified new credentials for outbound connections. The new logon session has the same local identity, but uses different credentials for other network connections.
10	RemoteInteractive	A user logged on to this computer remotely using Terminal Services or Remote Desktop.
11	CachedInteractive	A user logged on to this computer with network credentials that were stored locally on the computer. The domain controller was not contacted to verify the credentials.

Logon Types (Microsoft TechNet, 2005)

In Windows Server 2000/2003, XP family event IDs `528` and `540` signify a successful logon, event ID `538` a logoff and all the other events in this category identify different reasons for a logon failure. Event ID `528` is for all logons except `network logons` such as SMB/Microsoft-DS logons (i.e. connecting to a share). Event ID `540` is for `network` logon which is `logon type 3`. RDP, IIS, FTP logons, etc., are event ID `528` even though credentials may have come from over the network (Fitzgerald, 2004). Event ID `680` is logged for logon attempts with local SAM accounts on member servers and workstations. Event ID `680` is also logged on DC when a domain controller successfully authenticates a user via NTLM instead of Kerberos

In Windows Server 2008/2012, Vista/7/8 family, successful logon events (previous event IDs 528, 540) are combined into a single event ID `4624` and logon failure events are combined into one event ID 4625 with the proper error codes to identify different reason for logon failure. Event ID `4776` is logged for logon attempts with local SAM accounts on member servers and workstations, and is also logged on DC when a domain controller successfully authenticates a user via NTLM.

Following there are two tables, Kerberos Failure Codes and NTLM Error Codes, which are used to troubleshoot the common logon failures associated with event IDs related to logon/logoff events:

Error Code	**Description**
6	The username doesn't exist.
12	Workstation restriction; logon time restriction.
18	Account disabled, expired, or locked out.
23	The user's password has expired.

© 2013 SANS Institute, Author retains full...

24	Pre-authentication failed; usually means bad password
32	Ticket expired. This is a normal event that gets frequently logged by computer accounts.
37	The workstation's clock is too far out of synchronization with the DC's clock.

Kerberos Failure Codes (Smith, 2005)

Error code		Explanation
Decimal	**Hexadecimal**	
3221225572	C0000064	user name does not exist
3221225578	C000006A	user name is correct but the password is wrong
3221226036	C0000234	user is currently locked out
3221225586	C0000072	account is currently disabled
3221225583	C000006F	user tried to logon outside his day of week or time of day restrictions
3221225584	C0000070	workstation restriction
3221225875	C0000193	account expiration
3221225585	C0000071	expired password
3221226020	C0000224	user is required to change password at next logon

NTLM Error Codes (Smith, 2005)

© 2015 Author retains full rights.

6.2. Where and What to Look

Account logon events are generated on domain controllers for the account logon using domain accounts and on local computers for local account logon activity. With both `account logon` and `logon/logoff` audit policy categories enabled, logons that use a domain account generate a `logon or logoff` event on the workstation or server, and generate an `account logon event` on the domain controller. In addition to this, interactive logons using a domain account generates a `logon event` on the domain controller as the group policies and logon scripts are retrieved upon user log on (Microsoft TechNet, 2005). `Audit account logon events` on the domain controllers should be monitored to track all domain account

authentications. If the user logs on to a server or workstation using local account, `Account Logon` authentication events are logged on to that local server or workstation where the account exists. `Logon/Logoff` events are also logged on to that server or workstation for the system access.

These Logon events examples are described in the Appendix A and Appendix B section for the computer/user account logons, and for the resource access using domain account versus local account. In the next two diagrams, Logon and Authentication are explained, and are associated with the corresponding event IDs at the respective locations to make it easy for event lookup during an investigation.

6.3. Tracking a User

When a user turns on his Windows XP computer and enters his domain credentials, workstation needs to know if it is a genuine user so it sends an authentication request via Kerberos to the domain controller. With Kerberos pre-authentication in Windows, the domain controller checks the user's credentials before authentication ticket is issued. With the correct credentials, Windows logs a successful event ID `672` (Windows 2003/XP) or `4768` (Windows 2008 and above), `Authentication ticket granted` event on domain controller. Event ID `672` or `4768` with the user name in the event's description can be interpreted as user's initial logon at his workstation. User's workstation is identified with the `Client Address` field in event's description. All Kerberos events include `Client Address` which identifies the IP address of the client computer. The `Supplied Realm Name` identifies the domain of the user account in the event. Other Kerberos events identify the domain as `User Domain` or prefix the user name with the domain. Once the Kerberos pre-authentication is successful and a Kerberos TGT was granted, actual access will not occur until a service ticket is granted, which is audited by event ID `673` (Windows 2003/XP) or `4769` (Windows 2008 and above). Windows Kerberos events thus allow to easily identify a user's initial logon at his workstation using event ID `672/4768` and then track each server subsequently accessed using event ID `673/4769,service ticket granted` event. In the case of user typing bad password or other issues, failed authentication can be tracked using event IDs `675` and `676` (Windows 2000), event IDs `676` and failed event ID `672` on Windows Server 2003, event IDs `4768 or`

© 2013 SANS Institute, Author retains full rights.

4771 on Windows Server 2008. Kerberos failure code in the event, mentioned earlier, helps determine the cause of the logon failure (Smith, 2005).

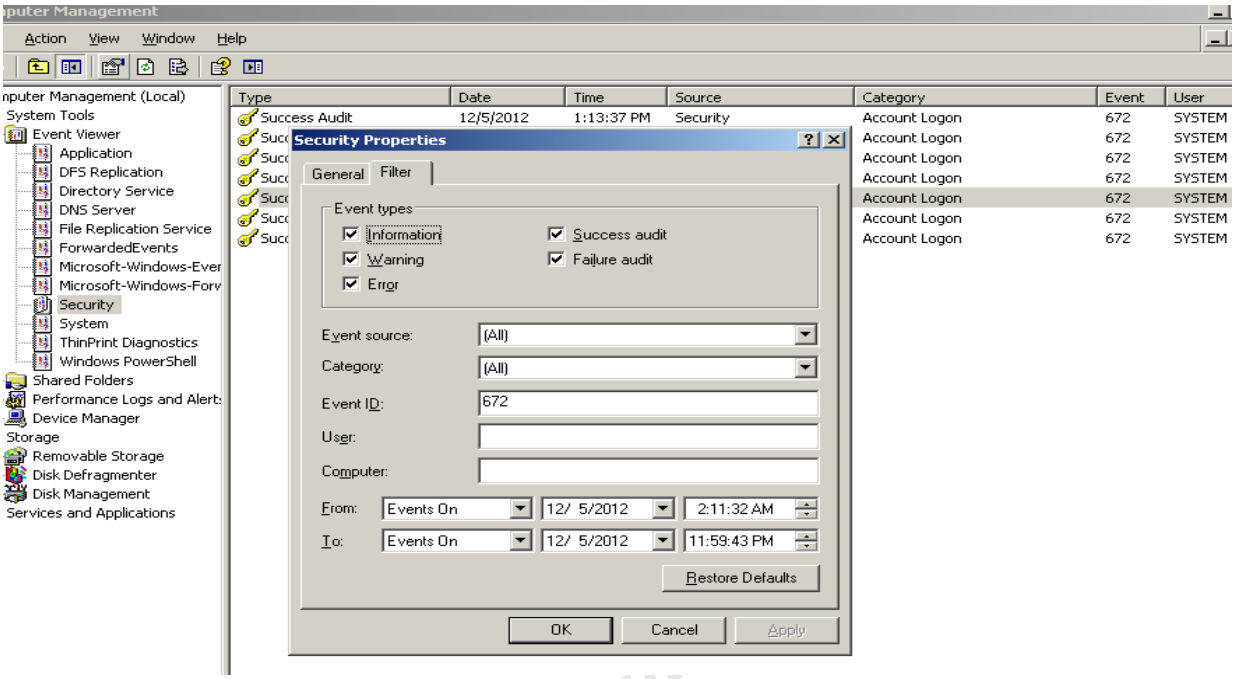
In addition to tracking using Kerberos tickets on domain controllers as mentioned above, User is also audited by Audit Logon/Logoff events 528, 540 / 538 (Windows 2003/XP), or 4624/4634 (Windows 2008 and above) logged to the systems accessed. These events are succeeded by event ID 673/4769 logged on the domain controller in case of Kerberos authentication. These are logged irrespective of a user logging on using local SAM account or a domain account. Type of account logon is then determined by looking at the Logon Type filed of these events. These events include Logon ID field, which is a unique number between reboots that identifies the logon session for these logons. Logon ID is useful for correlating many other events generated by user during this logon session. After having client IP and other systems' information used by that user, security logs from those systems are analyzed to see that user's activities and, these systems, if necessary, becomes the focus of the forensic analysis for a security investigation.

A user's effective login session from workstation logon to workstation logoff is determined by several factors. There is no Account Logoff authentication event on the domain controller and user can close session for the day in many different ways such as putting it to sleep, turn it off, system crash etc. For the logoff, local security event log on the concerned workstation needs to be analyzed for the audit logon/logoff events instead of audit account logon events. It is also necessary to correlate the log with other events such as shutdown time, startup time, unlock time etc to determine effective login session. Logon types in the audit logon/logoff events determines the unlocks, interactive logons, locks etc. such as type 7 logout event is lock, type 7 login is unlock.

© 2013 SANS Institute, Author retains full rights.

6.4. Querying Events

Windows provides Event Viewer, Microsoft Management Console (MMC), to review the events from various Windows event logs' channels. It allows for filtering the events based on various fields such as event ID, user ID, and time period. Here is one snapshot of Event Viewer.



There are various third party tools and scripts that can connect to Windows Event Log API for collecting and filtering the desired events. There are different ways shown in this section to query the specific events from Windows log using Windows command line utilities such as WMIC, PowerShell etc.

PowerShell

This command in the PowerShell command window (shell) extracts last 100 `Account Authentication` events on the local system today excluding some noise users such as `SYSTEM, NETWORK SERVICE, LOCAL SERVICE, and ANONYMOUS LOGON`.

```
PS>get-eventlog -log security | where-object {$_.EventID -match "^680$|
^528$|^672$|^4768$|^4776$" -AND $_.UserName -notmatch 'SYSTEM|NETWORK
SERVICE|LOCAL SERVICE|ANONYMOUS LOGON' -AND $_.TimeGenerated -gt
[datetime]::today } | sort-object -property TimeGenerated | select-object
-last 100 | Format-Table -AutoSize -Wrap
```

This command extracts last 50 `Logon` and `Authentication` events on the remote system from last `5` days for user `testuser1` on the remote system `remotesystem` giving event message details in the output.

```
PS>get-eventlog -computername remotesystem -log security | where-object
{$_.EventID -match "^680$|^528$|^540$|^672$|^4768$|^4624$|^4776$" -AND
```

© 2015 SANS Institute, Au

```
$_.Message -match "testuser1" -AND $_.TimeGenerated -gt (get-date).adddays(-
5) }| sort-object -property TimeGenerated | select-object -last 50 | Format-
Table TimeCreated, ID, ProviderName, Message -AutoSize -Wrap
```

WMIC

This command extracts `Account Authentication` events on the remote system `remotesystem` to an HTML output file in a table format.

```
D:\temp>WMIC /node:remotesystem /output:c:\temp\authentication_events.html
NTEVENT WHERE "LogFile='security' and (eventcode='680' or eventcode='528' or
eventcode='672' or eventcode='4768' or eventcode='4776')" list brief
/format:htable.xsl
```

In the test, WMIC tends to throw memory exception with commands giving large log data output. It works better if events are filtered down such as to a specific time period, specific users etc. This next command extracts `Logon` and `Authentication` events on the local system since `'12/11/2012 9:55:00'` for a specific user `testuser1` outputting to a file.

```
D:\temp>WMIC NTEVENT WHERE "LogFile='security' and (eventcode='680' or
eventcode='528' or eventcode='540' or eventcode='672' or eventcode='4768' or
eventcode='4624' or eventcode='4776') AND TimeGenerated >= '12/11/2012
9:55:00' AND message like "%testuser1%"" > logon-authentication_events.log
```

Searching Events from the Archived Log

Logs are often exported and forwarded to different system for analysis, archival etc. The `Windows Resource Kit` utility, `elogdump`, can dump the contents of an Event Log on the local or a remote computer. `PsLogList`, a Windows `Sysinternals` utility, also lets dump the contents of an Event Log on the local or a remote computer using alternate security credentials. `EventCombMT` utility from Account Lockout Tools (`ALTools`), is multi-threaded tool that can gather and parse event specific logs from multiple servers at the same time to one central location. `Log parser` tool provides universal query access to text-based data such as log files, XML files and CSV files, as well as key data sources on the Windows operating system such as the Event Log, the Registry, the file system, and Active Directory. The results of the query can be custom-formatted in text based output, or they can be persisted to more specialty targets like SQL, SYSLOG, or a chart (Microsoft, 2005).

© 2013 SANS Institute, Author retains full rights.

In this section, there are few examples of doing discoveries on specific events from the text formatted archived logs. Here, successful Interactive Logons and Logoffs are extracted using `findstr`, string command, after excluding some noisy users.

```
d:\temp>findstr.exe /c:",Security,528," /c:",Security,551,"
/c:",Security,4624," /c:",Security,4647," archive.log | findstr.exe /v
/c:"User Name: NETWORK SERVICE" /c:"User Name: LOCAL SERVICE" /c:"IUSR_"
/c:"IWAM_" /c:"ANONYMOUS LOGON" | findstr.exe /c:"Logon Type: 2"
/c:",Security,551,"
```

Next, similar search for Interactive Logons and Logoffs is performed using PowerShell.

```
PS> Get-Content archive.log | Select-String -pattern
"Security,528,","Security,551,","Security,4624,","Security,4647" | Select-
String -pattern "User Name: NETWORK SERVICE","User Name: LOCAL
SERVICE","IUSR_","IWAM_", "ANONYMOUS LOGON" -notmatch | Select-String
-pattern ",2," | out-file filtered_events1.txt -noclobber -width 350
```

Next, similar search for successful Logons and Logoffs is performed using PowerShell on the Windows 2003 domain controller archived log.

```
PS> Get-Content archive.log | Select-String -pattern "Security,528,",
"Security,538,","Security,680,","Security,672,","Security,676,","Security,54
0," | Select-String -pattern "User Name: NETWORK SERVICE","User Name: LOCAL
SERVICE","IUSR_","IWAM_","ANONYMOUS LOGON" -notmatch | out-file
filtered_events2.txt -noclobber -width 350
```

When working at the enterprise level, it becomes difficult task to get to the specific event from millions or billions of events due to resource and time constraints. According to Randy F. Smith (Smith, 2012), Windows has the ability to generate a detailed audit record of security events on each system, but exploiting that information is a lot like mining low-grade ore, which has to be subjected to a laborious refining process before reaching to the gold. Unless the needs are limited to occasional investigations, there should be some type of automated solution for collecting, monitoring, reporting, and archiving the Security logs that are scattered throughout the network.

7. Conclusion

An Investigator can mislead an investigation by not carefully analyzing all kinds of logons and understanding how they work. This paper guides with discovery and analysis of the

© 2013 SANS Institute, Author retains full rights.

logon process events when doing the incident response or pursuing a complex digital forensic investigation to a suspected event on a Windows platform. Windows system can provide detailed audit records of the logon and other security events. Windows network environment can produce enormous amount of log events due to regular stuff such as automatic ticket renewals, system services startups, active directory services etc. Centralized logging, and Security Information and Event Management (SIEM) solutions can help with the automation of security log collection, archiving, monitoring and reporting.

© 2013 SANS Institute, Author retains full rights.

8. References

Burr, William E. & Dodson, Donna F. & Newton, Elaine M. & Perlner, Ray A. & Polk, W. Timothy & Gupta, Sarbari & Nabbus, Emad A. (Dec, 2011). Electronic Authentication Guideline, NIST Special Publication 800-63-1. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-1.pdf

Fitzgerald, Eric (Aug, 2005). Deciphering Account Logon Events. Retrieved from http://blogs.msdn.com/b/ericfitz/archive/2005/08/04/447934.aspx

Fitzgerald, Eric (Dec, 2004). Events 528 and 540. Retrieved from http://blogs.msdn.com/b/ericfitz/archive/2004/12/09/279282.aspx

Goldman, David (Sep, 2012). Your smartphone will (eventually) be hacked. Retrieved from http://money.cnn.com/2012/09/17/technology/smartphone-cyberattack/index.html

GuyTe (Nov, 2010). Optimizing NTLM authentication flow in multi-domain- environments. Retrieved from http://blogs.technet.com/b/isrpfeplat/archive/2010/11/05/optimizing-ntlm-authentication-flow-in-multi-domain-environments.aspx

Kent, K., Chevalier, S., Grance, T. & Dang, Hung (Aug, 2006). Guide to Integrating Forensic Techniques into Incident Response, NIST Special Publication 800-86-1. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf

Mar, Wilson (2011). Kerberos Authentication Security. Retrieved from http://www.wilsonmar.com/kerberos.htm

Microsoft (2005). Log parser. Retrieved from http://www.microsoft.com/en-us/download/details.aspx?id=24659

Microsoft Support (2012). Well-known security identifiers in Windows operating systems. Retrieved from http://support.microsoft.com/kb/243330

Microsoft TechNet (2003). How Security Identifiers Work. Retrieved from http://technet.microsoft.com/en-us/library/cc778824.aspx

Microsoft TechNet (2003). Kerberos Authentication Overview? Retrieved from http://technet.microsoft.com/library/hh831553.aspx

Microsoft TechNet (2003). Logon and Authentication Technologies. Retrieved from http://technet.microsoft.com/en-us/library/cc780455.aspx

Microsoft TechNet (2003). Overview of the Authentication Strategy Design Process. Retrieved from http://technet.microsoft.com/en-us/library/cc759350.aspx

Microsoft TechNet (2003). What Are Access Tokens? Retrieved from http://technet.microsoft.com/en-us/library/cc759267%28v=ws.10%29.aspx

© 2013 SANS Institute, Author retains full rights.

Microsoft TechNet (2005). Audit account logon events. Retrieved from http://technet.microsoft.com/en-us/library/cc787176.aspx

Microsoft TechNet (2005). Audit logon events. Retrieved from http://technet.microsoft.com/en-us/library/cc787567%28v=ws.10%29.aspx

Microsoft TechNet (2005). Auditing Policy. Retrieved from http://technet.microsoft.com/en-us/library/cc779526(v=ws.10).aspx

Microsoft TechNet (2009). Audit Policy Settings Under Local Policies\Audit Policy. Retrieved from http://technet.microsoft.com/en-us/library/dd941595.aspx

Microsoft TechNet (2009). Creating a Strong Password Policy. Retrieved from http://technet.microsoft.com/en-us/library/cc780455.aspx

Microsoft TechNet (2009). How the Kerberos Version 5 Authentication Protocol Works. Retrieved from http://technet.microsoft.com/en-us/library/cc772815%28v=ws.10%29

Microsoft TechNet (2011). Windows Authentication. Retrieved from http://technet.microsoft.com/en-us/library/cc755284.aspx

Microsoft TechNet (2012). NTLM Overview. Retrieved from http://technet.microsoft.com/en-us/library/hh831571.aspx

Microsoft TechNet (2012). Windows Authentication Overview. Retrieved from http://technet.microsoft.com/en-us/library/hh831472.aspx

MSDN (2003). Access Tokens. Retrieved from http://msdn.microsoft.com/en-us/library/windows/desktop/aa374909.aspx

MSDN (2012). Access Control Lists. Retrieved from http://msdn.microsoft.com/en-us/library/windows/desktop/aa374872.aspx

MSDN (2012). So What Is Active Directory? Retrieved from http://msdn.microsoft.com/en-us/library/windows/desktop/aa746492.aspx

Northrup, Anthony & Thomas, Orin (Apr, 2004). MCSA/MCSE Self-Paced Training Kit (Exam 70-299): Implementing and Administering Security in a Microsoft® Windows Server(TM) 2003 Network. (Microsoft Press, ISBN: 073562061X)

Smith, Randall F. (2005). Deciphering Authentication Events on Your Domain Controllers. Retrieved from http://www.windowsecurity.com/articles/Deciphering-Authentication-Events-Domain-Controllers.html

© 2013 SANS Institute, Author retains full rights.

Smith, Randall F. (2005). Kerberos Authentication Events Explained. Retrieved from http://www.windowsecurity.com/articles/Kerberos-Authentication-Events.html

Smith, Randall F. (2005). Logon Type Codes Revealed. Retrieved from http://www.windowsecurity.com/articles/logon-types.html

Smith, Randall F. (2012). The Windows Server 2008 Security Log Revealed. Retrieved from http://www.ultimatewindowssecurity.com/securitylog/resourcekits/book2008/intro.aspx

Smith, Randall F. (2012). Understanding Logon Events in the Windows Security Log. Retrieved from http://www.ultimatewindowssecurity.com/webinars/register.aspx?id=140

The Center for Internet Security (2012). Security Configuration Benchmark For Microsoft Windows Server 2008. Retrieved from http://benchmarks.cisecurity.org/tools2/windows/CIS_Windows_Server_2008_Benchmark_v1.0.0.pdf

Walla, Mark (2012). Kerberos Explained. Retrieved from http://technet.microsoft.com/en-us/library/bb742516.aspx

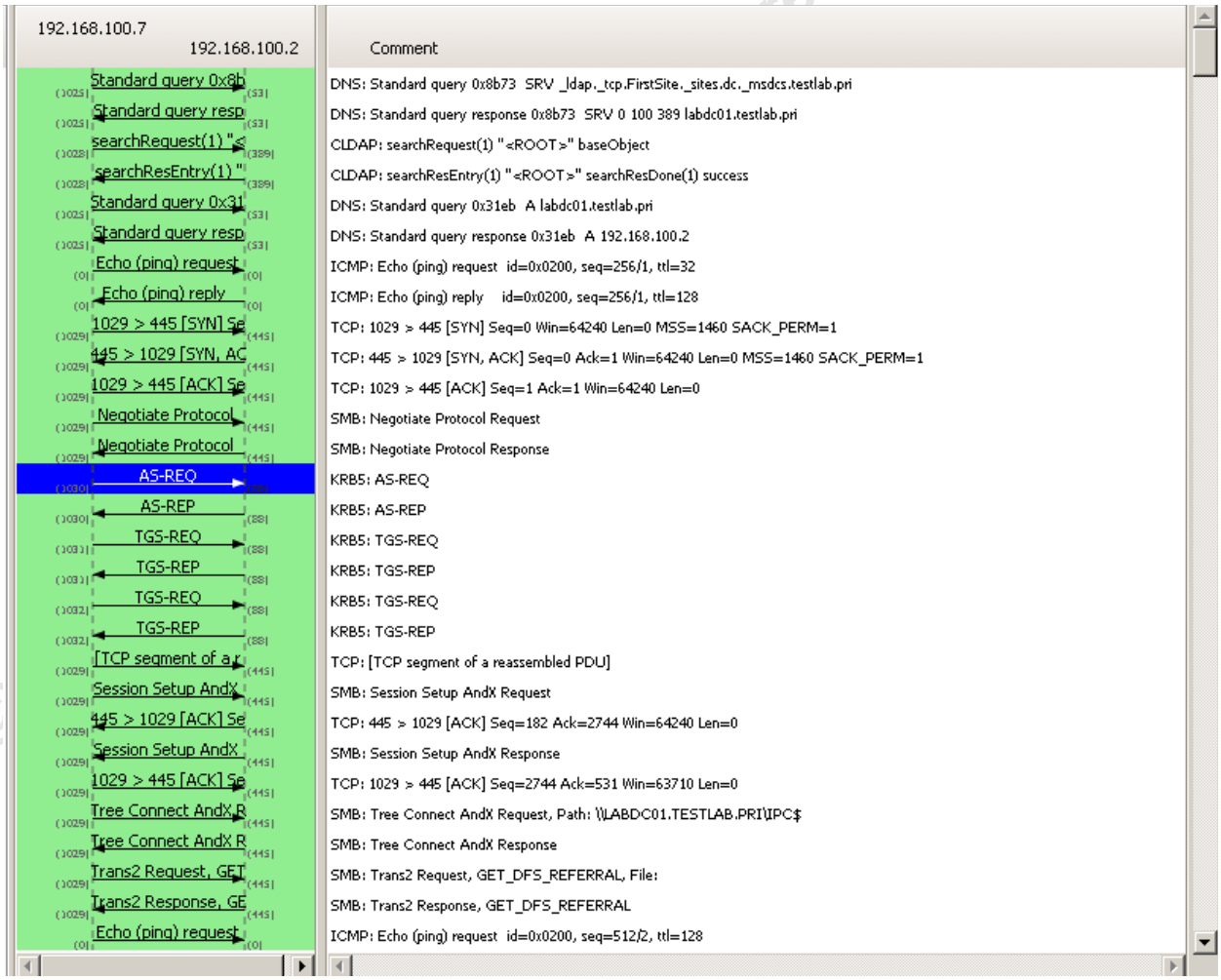
© 2013 SANS Institute, Author retains full rights.

9. Appendix A: Logging on in Domain Environment

In this section, a domain user logon is performed from a Windows XP workstation `LABXP01` into a Windows Active Directory domain `TESTLAB.PRI`. From here, we follow the logon related events onto the domain controller and the client workstation.

9.1. Kerberos Logon Handshake

This picture shows how the Kerberos authentication and ticket exchange occurs between XP client and the AD domain controller.



Kerberos Logon Handshake

© retains full rights

9.2. Account Logon Events on DC

When the workstation starts in a domain, it authenticates with the domain controller and logs this event ID 672, account logon event (authentication event) on the domain controller requesting the authentication service (AS) ticket during AS exchange.

```
Event Type:Success Audit
Event Source:    Security
Event Category:  Account Logon
Event ID:  672
Date:      12/5/2012
Time:      11:32:50 AM
User:      NT AUTHORITY\SYSTEM
Computer:  LABDC01
Description:
Authentication Ticket Request:
     User Name:        LABXP01$
     Supplied Realm Name:    TESTLAB.PRI
     User ID:                TESTLAB\LABXP01$
     Service Name:           krbtgt
     Service ID:       TESTLAB\krbtgt
     Ticket Options:         0x40810010
     Result Code:            -
     Ticket Encryption Type: 0x17
     Pre-Authentication Type:   2
     Client Address:         192.168.100.7
     Certificate Issuer Name:
     Certificate Serial Number:
     Certificate Thumbprint:
```

Domain controller and client workstation Kerberos Ticket Granting Service (TGS) Exchange takes place and the service ticket is assigned to work station and is logged with the event ID 673 on domain controller.

```
Event Type:Success Audit
Event Source:    Security
Event Category:  Account Logon
Event ID:  673
Date:      12/5/2012
Time:      11:32:50 AM
User:      NT AUTHORITY\SYSTEM
Computer:  LABDC01
Description:
Service Ticket Request:
     User Name:        LABXP01$@TESTLAB.PRI
     User Domain:            TESTLAB.PRI
     Service Name:           krbtgt
     Service ID:       TESTLAB\krbtgt
     Ticket Options:         0x60810010
     Ticket Encryption Type: 0x17
     Client Address:         192.168.100.7
     Failure Code:           -
     Logon GUID:       {364c161e-d67a-4fff-ccdd-34fa8343530b}
```

© 2013 SANS Institute, Author retains full rights.

```
     Transited Services:     -
```

Once the workstation is started and authenticated in a domain, User `testuser1` logs on with the domain credentials interactively. User is then authenticated to domain controlled using the same pattern as workstation did above using Kerberos exchanges. It logs the event ID `672` and event ID `673` on the domain controller as shown in the next two screens. The User field for the event ID `672` doesn't identify the user, which is always `SYSTEM`. Looking into the Authentication Ticket request gives the user name `testuser1`, Supplied Realm Name fields (User Domain) `TESTLAB` and Client Address `192.168.100.7` identifying the IP address of the workstation user logged on from.

```
Event Type:Success Audit
Event Source:    Security
Event Category:  Account Logon
Event ID:  672
Date:      12/5/2012
Time:      11:33:24 AM
User:      NT AUTHORITY\SYSTEM
Computer:  LABDC01
Description:
Authentication Ticket Request:
     User Name:        testuser1
     Supplied Realm Name:    TESTLAB
     User ID:                TESTLAB\testuser1
     Service Name:           krbtgt
     Service ID:       TESTLAB\krbtgt
     Ticket Options:         0x40810010
     Result Code:            -
     Ticket Encryption Type: 0x17
     Pre-Authentication Type:      2
     Client Address:         192.168.100.7
     Certificate Issuer Name:
     Certificate Serial Number:
     Certificate Thumbprint:
```

```
Event Type:Success Audit
Event Source:    Security
Event Category:  Account Logon
Event ID:  673
Date:      12/5/2012
Time:      11:33:24 AM
User:      NT AUTHORITY\SYSTEM
Computer:  LABDC01
Description:
Service Ticket Request:
     User Name:        testuser1@TESTLAB.PRI
     User Domain:            TESTLAB.PRI
     Service Name:           LABXP01$
     Service ID:       TESTLAB\LABXP01$
     Ticket Options:         0x40800000
     Ticket Encryption Type: 0x17
     Client Address:         192.168.100.7
     Failure Code:           -
```

©2013 Chris Institute. Author retains full rights.

```
     Logon GUID:       {3b79b41c-1985-b4a6-d55e-b8fd6a24cc7e}
     Transited Services:     -
```

9.3. Logon/Logoff Events on DC

After the workstation computer account is authenticated with the domain credentials, user again connect to domain controller to load the group policies, logon scripts, user profiles etc. and performs the further network logons to domain controller. These network logon/logoff events are marked by event IDs `540/538` logged to domain controller for each session. These events are shown here in the next two screens:

```
Event Type:Success Audit
Event Source:    Security
Event Category:  Logon/Logoff
Event ID:  540
Date:      12/5/2012
Time:      11:32:52 AM
User:      TESTLAB\LABXP01$
Computer:  LABDC01
Description:
Successful Network Logon:
     User Name:  LABXP01$
     Domain:           TESTLAB
     Logon ID:         (0x0,0x1EA52E)
     Logon Type: 3
     Logon Process:    Kerberos
     Authentication Package: Kerberos
     Workstation Name:
     Logon GUID: {e7185389-8811-0765-1ab3-ac148287d6ac}
     Caller User Name: -
     Caller Domain:    -
     Caller Logon ID:  -
     Caller Process ID: -
     Transited Services: -
     Source Network Address: 192.168.100.7
     Source Port:      1046
```

```
Event Type:Success Audit
Event Source:    Security
Event Category:  Logon/Logoff
Event ID:  538
Date:      12/5/2012
Time:      11:32:52 AM
User:      TESTLAB\LABXP01$
Computer:  LABDC01
Description:
User Logoff:
     User Name:  LABXP01$
     Domain:           TESTLAB
     Logon ID:         (0x0,0x1EA52E)
     Logon Type: 3
```

© 2013 SANS Institute, Author retains full rights.

Same is repeated with the user logon after user authentication with the domain credentials, as user connects to domain controller to load the group policies, logon scripts, user profiles etc. These network logon/logoff events are marked by event IDs `540/538` logged to domain controller for each session. These events are shown here in the next two screens:

```
Event Type:Success Audit
Event Source:    Security
Event Category:  Logon/Logoff
Event ID:  540
Date:      12/5/2012
Time:      11:33:25 AM
User:      TESTLAB\testuser1
Computer:  LABDC01
Description:
Successful Network Logon:
     User Name:  testuser1
     Domain:           TESTLAB
     Logon ID:         (0x0,0x1EA865)
     Logon Type: 3
     Logon Process:    Kerberos
     Authentication Package: Kerberos
     Workstation Name:
     Logon GUID: {1f2d3825-26bb-d6d4-88cd-6c97b3055552}
     Caller User Name: -
     Caller Domain:    -
     Caller Logon ID:  -
     Caller Process ID: -
     Transited Services: -
     Source Network Address: 192.168.100.7
     Source Port:      1055
```

```
Event Type:Success Audit
Event Source:    Security
Event Category:  Logon/Logoff
Event ID:  538
Date:      12/5/2012
Time:      11:33:55 AM
User:      TESTLAB\testuser1
Computer:  LABDC01
Description:
User Logoff:
     User Name:  testuser1
     Domain:           TESTLAB
     Logon ID:         (0x0,0x1EA865)
     Logon Type: 3
```

©2013 SANS Institute, Author retains full rights.

9.4. Logon/Logoff Events on Workstation

When the workstation is started, Logon event `540` is logged on locally to local workstation as well. For the domain user interactive logon, workstation logs the event ID `528` with logon type 2. These two events are shown in the following screens.

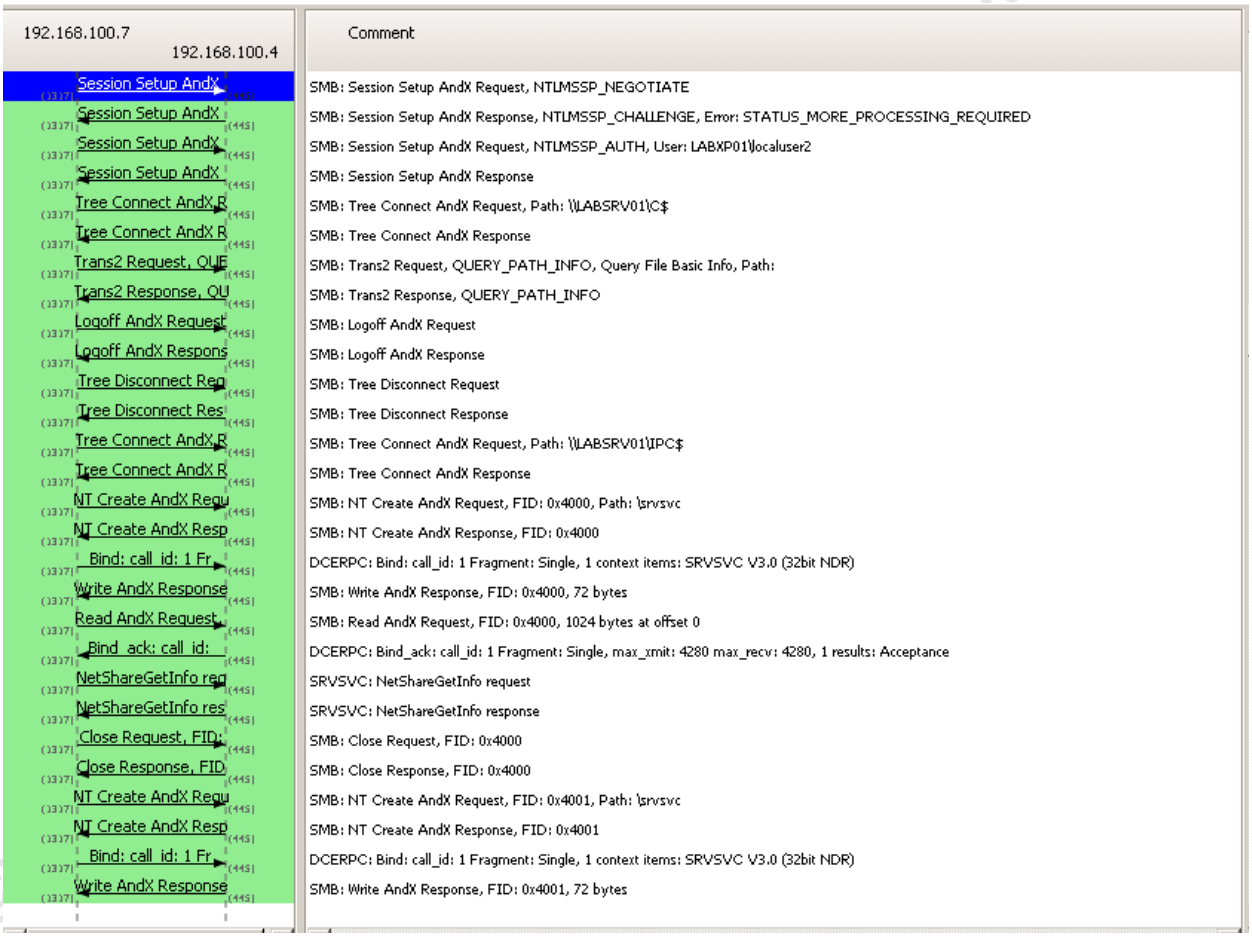
```
Event Type:Success Audit
Event Source:    Security
Event Category:  Logon/Logoff
Event ID:  540
Date:      12/5/2012
Time:      11:32:52 AM
User:      NT AUTHORITY\SYSTEM
Computer:  LABXP01
Description:
Successful Network Logon:
     User Name:  LABXP01$
     Domain:           TESTLAB
     Logon ID:         (0x0,0x1E3DA)
     Logon Type: 3
     Logon Process:    Kerberos
     Authentication Package: Kerberos
     Workstation Name:
     Logon GUID: {431c1dd9-bee1-71d0-82b6-8c3929a8e382}
```

```
Event Type:Success Audit
Event Source:    Security
Event Category:  Logon/Logoff
Event ID:  528
Date:      12/5/2012
Time:      11:33:24 AM
User:      TESTLAB\testuser1
Computer:  LABXP01
Description:
Successful Logon:
     User Name:  testuser1
     Domain:           TESTLAB
     Logon ID:         (0x0,0x2EA47)
     Logon Type: 2
     Logon Process:    GinaBkg
     Authentication Package: Negotiate
     Workstation Name: LABXP01
     Logon GUID: {9ccf2375-3acf-1e7c-d387-3b70af7baa4e}
```

© 2013 SANS Institute, Author retains full rights.

10. Appendix B: Logging on using Local Account and Mapping to different Server

In this section, we logon using local account to the workstation `LABXP01` and then maps to Windows 2003 server `LABSRV01` using the local account on server, thus forcing the NTLM authentication for resource access. In the picture below we see how the NTLM authentication handshake looks like:



full rights.

When a user logs on using the local account `localuser1,` account logon event ID `680` is logged on the workstation. It is followed by event ID `528` with the logon type `2` for the same user. In the next two screens we see the logs created on workstation by these two events.

```
Event Type:Success Audit
Event Source:    Security
Event Category:  Account Logon
Event ID:  680
Date:      12/13/2012
Time:      11:18:49 AM
User:      NT AUTHORITY\SYSTEM
Computer:  LABXP01
Description:
Logon attempt by: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
 Logon account:  localuser1
 Source Workstation: LABXP01
 Error Code: 0x0
```

```
Event Type:Success Audit
Event Source:    Security
Event Category:  Logon/Logoff
Event ID:  528
Date:      12/13/2012
Time:      11:18:49 AM
User:      LABXP01\localuser1
Computer:  LABXP01
Description:
Successful Logon:
     User Name:  localuser1
     Domain:           LABXP01
     Logon ID:         (0x0,0x158DF8)
     Logon Type: 2
     Logon Process:    User32
     Authentication Package: Negotiate
     Workstation Name: LABXP01
     Logon GUID: -
```

© 2012 SANS Institute, Author retains full rights.

When a server mapping is performed to a server LABSRV01 using local credential `LABSRV01\localuser2,` event ID `680` is logged to server for the successful NTLM authentication (error code 0x0). For the resource access, successful network logon event ID `540` is logged on to the server. This is later followed by logoff event ID `538` when this session is closed. Logon ID (`0x0,0x20E551`)in both the logon/logoff event (`540/538`) identifies that this logoff belongs to that logon session. In the next three screens, these three events are shown:

```
Event Type:Success Audit
Event Source:    Security
Event Category:  Account Logon
Event ID:  680
Date:      12/13/2012
Time:      11:22:46 AM
User:      LABSRV01\localuser2
Computer:  LABSRV01
Description:
Logon attempt by:MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
 Logon account:  localuser2
 Source Workstation:   LABXP01
 Error Code:     0x0
```

```
Event Type:Success Audit
Event Source:    Security
Event Category:  Logon/Logoff
Event ID:  540
Date:      12/13/2012
Time:      11:22:46 AM
User:      LABSRV01\localuser2
Computer:  LABSRV01
Description:
Successful Network Logon:
     User Name:  localuser2
     Domain:           LABSRV01
     Logon ID:         (0x0,0x20E551)
     Logon Type: 3
     Logon Process:    NtLmSsp
     Authentication Package: NTLM
     Workstation Name: LABXP01
     Logon GUID: -
     Caller User Name: -
     Caller Domain:    -
     Caller Logon ID:  -
     Caller Process ID: -
     Transited Services: -
     Source Network Address: 192.168.100.7
     Source Port:      0
```

```
Event Type:Success Audit
Event Source:    Security
Event Category:  Logon/Logoff
Event ID:  538
Date:      12/13/2012
Time:      11:29:38 AM
User:      LABSRV01\localuser2
Computer:  LABSRV01
Description:
User Logoff:
     User Name:  localuser2
     Domain:           LABSRV01
     Logon ID:         (0x0,0x20E551)
     Logon Type: 3
```

© 2010 SANS Institute, Author retains full rights.