samba eXPerience 2005

Göttingen, Germany

4th May 2005

Active Directory network protocols and traffic

Jean-Baptiste Marchand

<Jean-Baptiste.Marchand@hsc.fr>

Agenda

- Introduction
- Active Directory network procotols overview
- Capturing Active Directory network traffic
- Analyzing Active Directory traffic with ethereal
- Demonstration
- Conclusion
- References
- Greetings

Introduction

- Some good reasons to study Active Directory network protocols
  - Demystify Active Directory, looking at the protocols on the wire
  - Help to analyze network traces for troubleshooting purposes
  - Discover protocols involved in typical Active Directory deployments
    - Useful to implement a network security policy
- Why is it possible today?
  - Active Directory network protocols have been documented over the years and are now well understood
  - ethereal, the open-source network analyzer of choice
    - has an excellent support of Active Directory network protocols
    - can be used effectively to analyze network traffic in AD domains

Active Directory network protocols

- Active Directory domains rely on Internet standard protocols
  - DNS
  - LDAP
  - Kerberos V
  - SNTP
- NT 4.0 domains protocols are still used
  - SMB/CIFS
  - MSRPC
- Kerberos V is Active Directory network authentication protocol
  - Replaces NTLM authentication protocol
  - SMB, MSRPC, LDAP and DNS all support Kerberos authentication

Capturing Active Directory network traffic

- Capturing network traffic
  - Check local policies and procedures to determine if network sniffing is allowed
  - Depending on the network topology, might require to configure port mirroring on network devices
  - Network sniffing is possible on typical Unix systems supported by libpcap
    - If supported by the OS, do not run the sniffing tool (ex. tcpdump) as root
  - Recent Windows systems have a command-line network sniffing tool: netcap.exe (in netmon capture format, supported by ethereal)
- Analyzing network traffic
  - ethereal (http://www.ethereal.com/) is the network analyzer of choice for all usages, including for Windows network protocols

Using ethereal to analyze network traffic

- Analysis features
  - *Protocol Hierarchy* function : overview of network protocols found in a network trace
  - *Conversations* functions: overview of conversations at the different network levels (Ethernet, IP, TCP/UDP)
- Filtering features
  - ethereal display filters: used to limit displayed frames
  - Most ethereal dissectors give access to filterable fields, corresponding to data fields decoded in frames
  - Ex : `smb.cmd` (SMB command found in the header of a SMB frame)
  - *Prepare a Filter* and *Apply a Filter* functions

Display filters for Active Directory protocols

- Useful display filters for Active Directory protocols
  - dns : DNS queries and responses
  - smb: SMB sessions
  - dcerpc : MSRPC traffic
    - dcerpc && smb (ncacn_np), dcerpc && tcp && not smb(ncacn_ip_tcp)
  - ntp : (S)NTP traffic
  - ldap && udp: CLDAP traffic
  - ldap && tcp : LDAP traffic
  - kerberos && udp : Kerberos AS and TGS exchanges
  - kerberos && tcp : Kerberos AP exchanges
    - kerberos && smb : SMB sessions authenticated using Kerberos
    - kerberos && dcerpc : DCE-RPC sessions authenticated using Kerberos
    - kerberos && ldap : LDAP sessions authenticated using Kerberos

DNS and CLDAP traffic

- DNS traffic (dns)
  - SRV records lookup
    - _service._protocol.DnsDomainName
    - Ex: _ldap._tcp.sitename._sites.dc._msdcs.domainname to locate a domain controller in the current site
  - Dynamic updates
    - Can be authenticated with Kerberos, using GSS-TSIG (RFC 3645)
- CLDAP traffic (ldap && udp)
  - Connection-less LDAP (389/udp)
  - Used to query registered Active Directory domain controllers, previously identified with SRV records lookup
  - Can be manually reproduced: C:\>nltest /dsgetdc:domainname

Active Directory MSRPC interfaces

- MSRPC (Microsoft implementation of DCE-RPC) transports
  - ncacn_np: DCE-RPC over SMB (named pipes)
  - ncacn_ip_tcp: DCE-RPC over TCP
    - Endpoint mapper service (epm), to discover dynamic TCP ports
- MSRPC Active Directory interfaces
  - lsass.exe RPC interfaces
    - samr : SAM (Security Account Manager) RPC service
    - lsarpc : LSA (Local Security Authority) RPC service
    - netlogon : netlogon RPC service
    - drsuapi : Active Directory RPC access service
  - These 4 RPC interfaces can be restricted to a single TCP port
    - The endpoint mapper then always answers with the same static port
    - http://support.microsoft.com/?id=224196

MSRPC traffic : ncacn_np transport

- MSRPC traffic : ncacn_np transport
  - SMB session to the IPC$ share (ncacn_np MSRPC transport)
  - ethereal display filter: dcerpc && smb
  - Named pipes name identify the MSRPC interface
    - \pipe\lsarpc : lsarpc interface
    - \pipe\samr : samr interface
    - \pipe\netlogon : netlogon interface
  - ncacn_np transport used during an Active Directory join and unjoin process
    - Access to the samr interface via \pipe\samr: computer account administration
  - Domain controllers access to lsarpc and netlogon interfaces
    - Including for netlogon operations added in Active Directory

MSRPC traffic: ncacn_ip_tcp transport

- MSRPC traffic : ncacn_ip_tcp transport
  - ethereal display filter : dcerpc && tcp && not smb
  - MSRPC interfaces
    - epm : endpoint mapper (135/tcp), to discover allocated dynamic ports
    - netlogon : used to establish the netlogon secure channel at system startup
    - drsuapi
      - Used by domain members and domain users to query Active Directory using MSRPC instead of LDAP
      - DRSCrackNames() , implementing the DsCrackNames() API
      - Used for Active Directory database replication between domain controllers
    - frsrpc
      - Used for Active Directory file replication between domain controllers
  - These interfaces can be configured to listen on fixed ports
    - One TCP port for samr, lsarpc, netlogon and drsuapi
    - One TCP port for frsrpc

Group Policy: introduction

- Group Policy
  - Active Directory mechanism to centrally deploy software configuration
    - Individual settings are defined by Group Policy Objects (GPO)
    - Two types of GPOs
      - Settings affecting the computer configuration
      - Settings affecting the user environment
    - A set of GPOs is often designated as a GPO
  - GPO are linked to an Active Directory container
    - Linked to an AD site
    - Linked to an AD organizational unit
    - Linked to an AD domain
  - Precedence order: L S D OU
    - L(ocal GPO) S(ite GPO) D(omain GPO) OU (Organizational Unit GPO)

Group Policy traffic (1/2)

- Group Policy
  - GPO (machine settings) are processed when a domain member server starts
  - GPO (user settings) are processed when a domain user logs on a domain member server
  - GPO are then frequently refreshed
- Group Policy in Active Directory
  - Linked GPO are stored in Active Directory
    - LDAP unencrypted queries (gPLink and gPOptions attributes) to determine linked GPO (site-level GPOs, domain-level GPOs, OU-level GPOs)
    - ethereal display filter: ldap.attribute = "gPLink"
    - gPLink contains the DN where the GPO is defined in AD
    - Additional LDAP query for several attributes of returned DN entry, including gPCFileSysPath

Group Policy traffic (2/2)

- Group Policy : sysvol SMB share
  - GPCFileSysPath points to a DFS path referring to the sysvol share
  - \\domain_name\sysvol\domain_name\Policies\GPO_GUID\
    - \gpt.ini file
    - \Machine, \User subdirectories
    - \Adm subdirectory
- Group Policy SMB traffic
  - DFS referrals to locate the sysvol share
  - Reading of the gpt.ini file
  - Depending on the content of gpt.ini, additional files are retrieved
    - \Machine\registry.pol, \User\registry.pol
    - Additional files, depending on the content of the .pol files

MSRPC traffic between AD domain controllers (1/2)

- AD database replication
  - Multi-master replication topology: changes can originate from any DC
  - Active Directory intra-site replication use MSRPC (ncacn_ip_tcp)
  - Operations in the drsuapi interface
    - DRSReplicaSync() : send a change notification to a replication partner
    - DRSGetNCChanges()
      - Obtain updates for a specified naming context (NC = partition of the AD database)
  - Operations parameters are encrypted
    - ethereal Kerberos decryption supports DCE-RPC data decryption!
    - In addition, replication data may be compressed
  - Active Directory replication administration tools
    - repadmin.exe: CLI interface, with many options
    - replmon.exe: GUI monitoring interface

MSRPC traffic between AD domain controllers (2/2)

- AD File Replication Service (FRS)
  - Multi-master replication at the file level
  - Used to replicate sysvol share files
  - frsrpc MSRPC interface (ncacn_ip_tcp)
    - Setting the FRS MSRPC port: http://support.microsoft.com/?id=319553
  - Updates sent using the FrsRpcSendCommPkt operation
    - Data is encrypted
    - ethereal has a stub dissector for the frsrpc interface

ethereal Kerberos decryption feature

- One of (the many) ethereal "killer" features
  - ethereal can be linked with a Kerberos implementation (currently, Heimdal on Unix)
  - A keytab file can be used by the Kerberos dissector to decrypt
    - Kerberos exchanges with the KDC : AS and TGS sub-protocols
    - Kerberos authentication between Kerberos principals : AP sub-protocol

    → Authentication in SMB, LDAP, MSRPC, DNS (using SPNEGO)
    - Try to decrypt Kerberos blobs and Kerberos keytab file preference settings
  - Recently, decryption of LDAP and MSRPC payload has been added
    - Kerberos session keys are added in the context of ethereal Kerberos decryption module
    - These session keys can then be used to decrypt payload exchanged between principals
  - Some primitive network analyzers apparently do not support Kerberos decryption ☺

Ethereal kerberos decryption applied to Active Directory network traffic

- Microsoft Kerberos implementation
  - Uses by default the rc4-hmac encryption algorithm
  - Kerberos principals keys are NT hashes
  - Domain account NT hashes can be easily extracted from a AD domain controller using the pwdump{2,3,4,5} utility
    - requires local administrator privileges
  - A keytab entry can be created, given the principal name and the NT hash
    - -H option of the ktutil's add command (in recent Heimdal snapshots)
    - $ ktutil -k keytab add –principal=mydc\$@KRB.REALM -e arcfour-hmac-md5 -H –password=NT_hash_in_hex -V 1

Demonstration

- Network trace of a domain join process
  - Active Directory Domain controller location process (DNS + CLDAP)
  - Computer account creation (samr)
  - Kerberos tickets decryption (including MS Kerberos PAC)
- Network trace of network traffic between domain controllers
  - drsuapi replication traffic (decrypted)
  - frsrpc replication traffic

Conclusion

- ethereal is the perfect tool to analyze Active Directory network traffic
  - Excellent support of all AD protocols (including SMB and MSRPC)
  - The Kerberos decryption feature is a must-have tool
- Looking at Active Directory network protocols on the wire is required in many different situations
  - Troubleshooting issues
  - Active Directory internals digging
  - Network security auditing, including for penetration tests
- Easy to experiment!

References

- ethereal
  - http://www.ethereal.com/
  - http://wiki.ethereal.com/
- Windows network services internals
  - http://www.hsc.fr/ressources/articles/win_net_srv/
- Active Directory network protocols and traffic (September 2004)
  - http://www.hsc.fr/ressources/presentations/ad_proto_traffic/
- This presentation is available at
  - http://www.hsc.fr/ressources/presentations/sambaxp2005/ad_traffic.pdf

Greetings

- Hervé Schauer Consultants (HSC)
  - French IT security consulting agency I work for
- ethereal team and particularly Ronnie Sahlberg
  - Prolific ethereal developper!
  - Implementer of many MSRPC dissectors, including auto-generated dissectors using some of Samba4 IDL files
  - Implementer of the Kerberos decryption feature
- Samba team
  - Jim McDonough and Anthony Liguori's work on CLDAP
  - Stefan Metzmacher's work on the drsuapi MSRPC interface