HERVÉ SCHAUER CONSULTANTS
Cabinet de Consultants en Sécurité Informatique depuis 1989
Spécialisé sur Unix, Windows, TCP/IP et Internet

Windows Security OSSIR group

13th September 2004

Active Directory network protocols and traffic

Jean-Baptiste Marchand
<Jean-Baptiste.Marchand@hsc.fr>

Agenda

- Active Directory network protocols overview
- Network traffic analysis with ethereal
- Network traffic for each protocol
- Active Directory typical scenarios
- Other approaches
- Conclusion
- References

Active Directory network protocols

- Active Directory is based on network protocols
  - Standardized: DNS, LDAP, Kerberos V, SNTP
  - Proprietary: SMB/CIFS, MSRPC
- Use of Internet protocols, enbraced and extended by Microsoft

Internet protocols: DNS

- DNS
  - Specifications: many RFCs
    - http://www.dns.net/dnsrd/rfc/
  - Name resolution service (replaces NetBIOS name resolution used in NT domains)
    - Dynamic DNS entries update
    - GSS-TSIG (RFC 3645)
  - Domain services localization
    - SRV DNS records

Internet protocols: LDAP

- LDAP
  - Specifications: see RFC 3377
  - Active Directory is a directory that can be queried using LDAP
    - Ports 389 (TCP and UDP), 636 (LDAPS), 3268 and 3269 (AD Global Catalog)
  - Specific SASL mechanism: GSS-SPNEGO
  - Windows systems also access Active Directory using MSRPC
    - `samr` and `drsuapi` RPC interfaces
  - Sensitive information is encrypted
    - LDAP sessions using TCP port 389, encrypted using GSS-SPNEGO
    - Encrypted MSRPC operations (*packet privacy*)
  - LDAP does not include directory replication standardization
    - Active Directory replication uses MSRPC or SMTP

Internet protocols: Kerberos V

- Kerberos V
  - Network authentication protocol
  - Protocol defined at MIT then standardized at the IETF, widely used in Unix environments
  - Embraced and extended by Microsoft
    - RC4-HMAC cipher, TCP transport, PAC (Privilege Access Certificate), PKINIT, …
    - Standard interfaces are implemented for compatibility but are not used by native Windows clients
      - Example: kpasswd service (for password changing)
  - Kerberos V has been integrated to Windows services using the SSPI layer
    - SPNEGO, for negotiation between different security packages (NTLM, Kerberos V, Schannel, …)

Internet protocols: SNTP

- SNTP
  - Simple Network Time Protocol, version 3 (RFC 1769)
  - Simplified version of the NTP protocol (RFC 1305)
    - same packet format, using UDP port 123
    - less precise than NTP (but enough for Kerberos V)
  - Synchronization packets are signed
    - usually ignored in SNTP
    - used to authenticate synchronization packets

Proprietary protocols: SMB/CIFS

- SMB/CIFS
  - Windows domains resource sharing protocol
    - Frequently confused with NetBIOS over TCP/IP
  - Used for file and printer sharing
  - Also a possible transport for MSRPC
    - Transport using named pipes (`ncacn_np`)
    - Active Directory prefers TCP/IP transport, as opposed to NT 4.0
      - SMB transport is still used when a machine is joined to a domain
  - Group Policy: `sysvol` share
    - `gpt.ini`, `registry.pol`, `*.adm`, `GptTmpl.inf` files
  - Connection scripts: `netlogon` share

Proprietary protocols: MSRPC

- MSRPC
  - MS implementation of the DCE RPC standard
  - Active Directory domains are based on key RPC interfaces:
    - `lsarpc`: LSA access (Local Security Authority)
    - `netlogon`: network authentication service
    - `samr`: SAM access (NT 4.0 backward compatibility, works with Active Directory)
    - `drsuapi`: Active Directory access
  - Active Directory uses TCP transport for these RPC services
    - Portmapper listening on TCP port 135
    - Default ports range for RPC services listening on TCP
      - 1025-5000 (default interval), to be modified with `rpccfg`
    - Reminder: NT 4.0 was based on RPC services over SMB, over NetBIOS over TCP/IP (TCP port 139)

Network authentication

- Kerberos V is the network authentication protocol used in AD
  - Replaces NTLM
  - Supports mutual authentication
  - Aforementionned network protocols have been modified to support Kerberos
    - SMB/CIFS sessions authentication
    - LDAP sessions authentication
    - MSRPC calls authentication
    - Dynamic DNS updates authentication
  - Kerberos V support was added using a negotiation protocol, SPNEGO (Simple Protected Negotiation Mechanism, RFC 2478)
    - Multiple errors in Microsoft SPNEGO implementation, leading to serious interoperability problems

Network traffic analysis: goals

- Possible goals of network traffic analysis
  - Understanding Active Directory
  - Validating key mechanisms of Active Directory domains
    - Ex 1: Kerberos tickets renewal
    - Ex 2: Group Policy processing
  - Tracking anomalies

Network traffic analysis: methodology

- Require access to domain controllers network traffic
  - To capture network traffic
- Require a network analyzer supporting aforementionned protocols
  - Recommended network analyzer: ethereal
  - Free software, working on Unix and Windows
  - Support of multiple network protocols, including Windows-oriented protocols (SMB/CIFS and MSRPC)
  - Support of Kerberos tickets decryption
    - On Unix with Heimdal (http://www.pdc.kth.se/heimdal/)
  - http://www.ethereal.com/

Network traffic typology

- Network traffic typology overview
  - Examining observed protocols
    - ethereal `Protocol Hierarchy` function
  - Examining traffic typology
    - ethereal `Conversations` function
    - `IPv4 conversations` : conversations at the IP level
    - `TCP, UDP conversation` : (IP addresses, ports) (source and destination)

Protocol Hierarchy function

Protocol	% Packets	Packets	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
⊟ Frame	100.00%	278	73952	0.003	0	0	0.000
⊟ Ethernet	100.00%	278	73952	0.003	0	0	0.000
Address Resolution Protocol	2.88%	8	462	0.000	8	462	0.000
⊟ Internet Protocol	97.12%	270	73490	0.003	0	0	0.000
⊟ User Datagram Protocol	12.95%	36	20158	0.001	0	0	0.000
Domain Name Service	5.04%	14	2123	0.000	14	2123	0.000
⊟ Lightweight Directory Access Protocol	2.16%	6	1315	0.000	3	664	0.000
Lightweight Directory Access Protocol	1.08%	3	651	0.000	3	651	0.000
Kerberos	5.04%	14	16500	0.001	14	16500	0.001
Network Time Protocol	0.72%	2	220	0.000	2	220	0.000
⊟ Transmission Control Protocol	82.73%	230	53082	0.002	114	12540	0.001
⊟ DCE RPC	12.95%	36	9223	0.000	12	2823	0.000
DCE/RPC Endpoint Mapper	2.16%	6	1160	0.000	6	1160	0.000
Microsoft Network Logon	3.60%	10	3376	0.000	10	3376	0.000
Microsoft Directory Replication Service	2.88%	8	1864	0.000	8	1864	0.000
⊟ NetBIOS Session Service	11.51%	32	6669	0.000	0	0	0.000
SMB (Server Message Block Protocol)	11.51%	32	6669	0.000	32	6669	0.000
⊟ Lightweight Directory Access Protocol	15.83%	44	23807	0.001	42	22481	0.001
Lightweight Directory Access Protocol	0.72%	2	1326	0.000	2	1326	0.000
Hypertext Transfer Protocol	1.44%	4	843	0.000	4	843	0.000
Internet Control Message Protocol	1.44%	4	250	0.000	4	250	0.000

TCP conversations

Ethernet: 3 | Fibre Channel | FDDI | IPv4: 2 | IPX | TCP: 13 | Token Ring | UDP: 17

TCP Conversations

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A->B	Bytes A->B	Packets A<-B	Bytes A<-B
192.70.106.144	1046	192.70.106.151	80	11	1249	5	625	6	624
192.70.106.144	1029	192.70.106.151	135	15	1604	9	908	6	696
192.70.106.144	1052	192.70.106.151	135	12	1040	7	638	5	402
192.70.106.144	1056	192.70.106.151	389	23	7166	13	3157	10	4009
192.70.106.144	1043	192.70.106.151	389	20	7815	12	3096	8	4719
192.70.106.144	1045	192.70.106.151	389	15	3103	9	2240	6	863
192.70.106.144	1057	192.70.106.151	389	12	3891	7	2019	5	1872
192.70.106.144	1058	192.70.106.151	389	12	3823	7	1974	5	1849
192.70.106.144	1059	192.70.106.151	389	12	3869	7	2019	5	1850
192.70.106.144	1035	192.70.106.151	445	44	8835	25	5700	19	3135
192.70.106.144	1039	192.70.106.151	1025	22	5685	12	4078	10	1607
192.70.106.144	1031	192.70.106.151	1025	18	3702	11	2324	7	1378
192.70.106.144	1030	192.70.106.151	1025	14	1300	8	828	6	472

UDP conversations

Ethernet: 3 | Fibre Channel | FDDI | IPv4: 2 | IPX | TCP: 13 | Token Ring | UDP: 17

UDP Conversations

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A->B	Bytes A->B	Packets A<-B	Bytes A<-B
192.70.106.144	1026	192.70.106.151	53	4	758	2	244	2	514
192.70.106.144	1047	192.70.106.151	53	2	252	1	83	1	169
192.70.106.144	1048	192.70.106.151	53	2	252	1	126	1	126
192.70.106.144	1049	192.70.106.151	53	2	251	1	87	1	164
192.70.106.144	1050	192.70.106.49	53	2	231	1	171	1	60
192.70.106.144	1053	192.70.106.151	53	2	379	1	122	1	257
192.70.106.144	1036	192.70.106.151	88	2	1728	1	361	1	1367
192.70.106.144	1037	192.70.106.151	88	2	2666	1	1346	1	1320
192.70.106.144	1038	192.70.106.151	88	2	2645	1	1339	1	1306
192.70.106.144	1040	192.70.106.151	88	2	2666	1	1346	1	1320
192.70.106.144	1041	192.70.106.151	88	2	2600	1	1324	1	1276
192.70.106.144	1044	192.70.106.151	88	2	2720	1	1364	1	1356
192.70.106.144	1051	192.70.106.151	88	2	1475	1	1335	1	140
192.70.106.144	123	192.70.106.151	123	2	220	1	110	1	110
192.70.106.144	1028	192.70.106.151	389	2	467	1	250	1	217
192.70.106.144	1034	192.70.106.151	389	2	424	1	207	1	217
192.70.106.144	1054	192.70.106.151	389	2	424	1	207	1	217

Network traffic filtering

- Network traffic filtering
  - ethereal supports display filters
  - Most of ethereal dissectors give access to filterable fields, corresponding to data fields decoded in data frames
  - Displayed frames filtering can be specified using any filterable fields
  - `Apply as filter` and `Prepare a filter` functions

Display filters examples

- Display filters for Active Directory protocols
  - `smb`: SMB sessions
  - `ldap && udp`: CLDAP traffic
  - `ldap && tcp`: LDAP traffic
  - `dcerpc`: MSRPC traffic
  - `kerberos && udp`: Kerberos exchanges (UDP port 88)
  - `kerberos.msg.type == 10`: AS-REQ Kerberos messages
  - `smb && kerberos`, `ldap && kerberos`, `dcerpc && kerberos` : Kerberos authentification frames inside SMB, LDAP and MSRPC (AP-REQ and AP-REP messages)
    - Equivalent to: `kerberos && tcp`

Kerberos authentication: SMB, MSRPC, LDAP

Filter: kerberos && tcp | Add Expression... | Clear | Apply

No.	Time	Source	Destination	Protocol	Info
55	2004-07-15 11:18:56.957848	192.70.106.144	192.70.106.151	SMB	Session Setup AndX Request
57	2004-07-15 11:18:57.016509	192.70.106.151	192.70.106.144	SMB	Session Setup AndX Response
75	2004-07-15 11:18:57.927875	192.70.106.144	192.70.106.151	DCERPC	Bind: call_id: 1 UUID: DRSUAPI
77	2004-07-15 11:18:57.958316	192.70.106.151	192.70.106.144	DCERPC	Bind_ack: call_id: 1 accept max_>
78	2004-07-15 11:18:57.960004	192.70.106.144	192.70.106.151	DCERPC	Alter_context: call_id: 1 UUID: I
104	2004-07-15 11:18:58.521506	192.70.106.144	192.70.106.151	LDAP	MsgId=3 Bind Request, DN=(null)
105	2004-07-15 11:18:58.599533	192.70.106.151	192.70.106.144	LDAP	MsgId=3 Bind Result
112	2004-07-15 11:18:58.667594	192.70.106.144	192.70.106.151	LDAP	MsgId=7 Bind Request, DN=(null)
113	2004-07-15 11:18:58.749381	192.70.106.151	192.70.106.144	LDAP	MsgId=7 Bind Result
217	2004-07-15 11:20:00.033894	192.70.106.144	192.70.106.151	LDAP	MsgId=3 Bind Request, DN=(null)
218	2004-07-15 11:20:00.116670	192.70.106.151	192.70.106.144	LDAP	MsgId=3 Bind Result
230	2004-07-15 11:20:00.238930	192.70.106.144	192.70.106.151	LDAP	MsgId=10 Bind Request, DN=(null)
231	2004-07-15 11:20:00.324893	192.70.106.151	192.70.106.144	LDAP	MsgId=10 Bind Result
243	2004-07-15 11:20:00.381976	192.70.106.144	192.70.106.151	LDAP	MsgId=15 Bind Request, DN=(null)
244	2004-07-15 11:20:00.474899	192.70.106.151	192.70.106.144	LDAP	MsgId=15 Bind Result
255	2004-07-15 11:20:00.504705	192.70.106.144	192.70.106.151	LDAP	MsgId=20 Bind Request, DN=(null)
256	2004-07-15 11:20:00.574816	192.70.106.151	192.70.106.144	LDAP	MsgId=20 Bind Result

Typical scenarios

- Typical scenarios
  - System join to an Active Directory domain
  - Domain member or domain controller startup
  - Machine account password change
    - Every 30 days by default
  - User authentication on a domain
  - Domain controllers replication
  - Group Policy applications
  - ...

DNS and CLDAP traffic

- DNS traffic
  - SRV records resolution
    - _service._protocol.DnsDomainName
    - Ex: `_ldap._tcp.sitename._sites.dc._msdcs.domainname` to locate a domain controller inside a given site
- CLDAP traffic
  - Obtaining the closest domain controller
  - `DsGetDcName()` API, implemented by a pseudo RPC call to Active Directory
    - Site name is kept in cache (`DynamicSiteName` registry value)
  - ethereal display filter: `ldap && udp`
  - Documented in the *Locating Active Directory Servers* section of Windows 2000 Resource Kit documentation

DNS traffic: dynamic updates (1/2)

- DNS dynamic updates
  - Implemented by the dhcp service (even if IP address is static)
    - `Register this connection's addresses in DNS` (enabled by default)
    - at machine startup with static IP address (A and PTR)
    - at each IP address change with dynamic IP address (DHCP)
      - Depends on DHCP server configuration (by default, only A record)
    - each 24 hours by default
      - `DefaultRegistrationRefreshInterval` registry value
      - Default TTL of 20 minutes for updated records {A, PTR} (`DefaultRegistrationTtl` registry value)
    - manual registration: `ipconfig /registerdns`

DNS traffic: dynamic updates (2/2)

LDAP traffic

- LDAP traffic
  - typically authenticated using the GSS-SPNEGO SASL mechanism
    - empty dn (*distinguished name*) in LDAP bind
  - starts with a request to obtain certain attributes of the RootDSE
    - `SupportedSASLMechanisms`
    - `LdapServiceName`
  - LDAP traffic can be encrypted
  - Examination of search parameters when traffic is unencrypted
    - Base DN, scope, filters, attributes, ...
  - LDAP request errors
    - `ldap.result.errormsg` display filter

MSRPC traffic (1/2)

- MSRPC traffic
  - RPC services localization over TCP/IP
    - endpoint mapper, TCP port 135 (`epm`)
    - Returns the TCP port on which a given RPC service is listening
    - `map` operation, unauthenticated
  - Local Security Authority access (`lsa`)
    - Kerberos authentication
    - TCP port (typically 1025, must be set to a static port, as documented in MSKB #224196)
    - Ex: `LsarQueryInformationPolicy(2)` operations
  - Active Directory access, using SAM RPC interface (`samr`)
    - Kerberos authentication, using same TCP port as LSA access
    - Ex: machine account creation on a DC for a new member server is implemented using the `SamrCreateUser2InDomain` operation

MSRPC traffic (2/2)

- MSPRC traffic (cont.)
  - Authentication on the domain, using netlogon service (`rpc_netlogon`)
    - Same TCP port as LSA and SAM access
    - `NetrServerReqChallenge` and `NetrServerAuthenticate3` operations
  - Active Directory access, using RPC (instead of LDAP)
    - `drsuapi` interface, using the same TCP port
    - `DRSCrackNames` operation (`DrsBind` and `DrsUnbind`), implementing the `DsCrackNames()` API
    - Encrypted traffic, currently not decoded by ethereal

Kerberos traffic

- Kerberos traffic
  - Obtaining a TGT (Ticket Granting Ticket)
    - Startup of a domain member server
    - User authentication
    - AS-REQ (10) and AS-REP (11) messages
  - Obtaining service tickets
    - TGS-REQ (12) and TGS-REP (13) messages
    - Typical service names: host, ldap, cifs, dns, ...
  - Using service tickets
    - AP-REQ (14) and AP-REP (15) messages
    - Typically encapsulated inside SPNEGO

Active Directory Service Principal Names (SPN)

- Service Principal Names
  - Kerberos authentication to Active Directory network services is implemented requesting a ticket for a given service
  - A service is designated using a SPN (Service Principal Name)
  - `servicePrincipalName` attribute (*case-insensitive*) in the `User` Active Directory object class
  - Also, `sPNMappings` attribute (list of equivalent SPNs to the host SPN)
- On the wire
  - SPN appear in TGS-REQ, TGS-REP and AS-REQ messages
  - A TGS-REP message can contain a different SPN from the one requested
    - Canonicalization option in Windows 2000
    - Returned SPN is similar to SERVER$
    - Canonicalization is disabled in Windows Server 2003

Registered SPN on a AD DC

C:\WINDOWS\system32\cmd.exe

```
C:\>setspn -L SERVEUR
Registered ServicePrincipalNames for CN=SERVEUR,OU=Domain Controllers,DC=DomaineBlah,DC=com:
    NtFrs-88f5d2bd-b646-11d2-a6d3-00c04fc9b232/serveur.DomaineBlah.com
    DNS/serveur.DomaineBlah.com
    ldap/serveur.DomaineBlah.com/TAPI3Directory.DomaineBlah.com
    ldap/serveur.DomaineBlah.com/ForestDnsZones.DomaineBlah.com
    GC/serveur.DomaineBlah.com/DomaineBlah.com
    HOST/serveur.DomaineBlah.com/DOMAINEBLAH
    HOST/SERVEUR
    HOST/serveur.DomaineBlah.com
    HOST/serveur.DomaineBlah.com/DomaineBlah.com
    E3514235-4B06-11D1-AB04-00C04FC2DCD2/276d4866-4940-49e4-91ec-991746baf84a/DomaineBlah.com
    ldap/276d4866-4940-49e4-91ec-991746baf84a._msdcs.DomaineBlah.com
    ldap/serveur.DomaineBlah.com/DOMAINEBLAH
    ldap/SERVEUR
    ldap/serveur.DomaineBlah.com
    ldap/serveur.DomaineBlah.com/DomainDnsZones.DomaineBlah.com
    ldap/serveur.DomaineBlah.com/DomaineBlah.com
```

Kerberos tickets of a domain user (Windows 2000)

```
C:\>klist tickets

Cached Tickets: (5)

   Server: krbtgt/DOMAINEBLAH.COM@DOMAINEBLAH.COM
      KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
      End Time: 8/27/2004 0:51:47
      Renew Time: 9/2/2004 14:51:47


   Server: krbtgt/DOMAINEBLAH.COM@DOMAINEBLAH.COM
      KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
      End Time: 8/27/2004 0:51:47
      Renew Time: 9/2/2004 14:51:47


   Server: HOST/serveur.DomaineBlah.com@DOMAINEBLAH.COM
      KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
      End Time: 8/27/2004 0:51:47
      Renew Time: 9/2/2004 14:51:47


   Server: ldap/serveur.DomaineBlah.com/DomaineBlah.com@DOMAINEBLAH.COM
      KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
      End Time: 8/27/2004 0:51:47
      Renew Time: 9/2/2004 14:51:47


   Server: LDAP/serveur.DomaineBlah.com@DOMAINEBLAH.COM
      KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
      End Time: 8/27/2004 0:51:47
      Renew Time: 9/2/2004 14:51:47
```

Kerberos tickets of a domain user (Windows XP)

```
C:\>klist tickets

Cached Tickets: (6)

   Server: krbtgt/DOMAINEBLAH.COM@DOMAINEBLAH.COM
      KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
      End Time: 7/30/2004 5:56:27
      Renew Time: 8/5/2004 19:56:27


   Server: krbtgt/DOMAINEBLAH.COM@DOMAINEBLAH.COM
      KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
      End Time: 7/30/2004 5:56:27
      Renew Time: 8/5/2004 19:56:27


   Server: ldap/serveur.DomaineBlah.com/DomaineBlah.com@DOMAINEBLAH.COM
      KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
      End Time: 7/30/2004 5:56:27
      Renew Time: 8/5/2004 19:56:27


   Server: cifs/serveur.domaineblah.com@DOMAINEBLAH.COM
      KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
      End Time: 7/30/2004 5:56:27
      Renew Time: 8/5/2004 19:56:27


   Server: LDAP/serveur.DomaineBlah.com@DOMAINEBLAH.COM
      KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
      End Time: 7/30/2004 5:56:27
      Renew Time: 8/5/2004 19:56:27


   Server: host/wxpdflt.domaineblah.com@DOMAINEBLAH.COM
      KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
      End Time: 7/30/2004 5:56:27
      Renew Time: 8/5/2004 19:56:27
```

Kerberos tickets on a domain controller (1/2) (LOCALSYSTEM logon session)

```
C:\>klist tickets

Cached Tickets: (9)

   Server: krbtgt/DOMAINEBLAH.COM@DOMAINEBLAH.COM
      KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
      End Time: 9/7/2004 20:32:06
      Renew Time: 9/14/2004 10:32:06


   Server: krbtgt/DOMAINEBLAH.COM@DOMAINEBLAH.COM
      KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
      End Time: 9/7/2004 20:32:06
      Renew Time: 9/14/2004 10:32:06


   Server: krbtgt/DOMAINEBLAH.COM@DOMAINEBLAH.COM
      KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
      End Time: 9/7/2004 20:32:06
      Renew Time: 9/14/2004 10:32:06


   Server: W2KKDC$@DOMAINEBLAH.COM
      KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
      End Time: 9/7/2004 20:32:06
      Renew Time: 9/14/2004 10:32:06


   Server: SERVEUR$@DOMAINEBLAH.COM
      KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
      End Time: 9/7/2004 20:32:06
      Renew Time: 9/14/2004 10:32:06
```

Kerberos tickets on a domain controller (2/2) (LOCALSYSTEM logon session)

```
   Server: ldap/w2kkdc.DomaineBlah.com/DomaineBlah.com@DOMAINEBLAH.COM
      KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
      End Time: 9/7/2004 20:32:06
      Renew Time: 9/14/2004 10:32:06


   Server: ldap/w2kkdc.DomaineBlah.com@DOMAINEBLAH.COM
      KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
      End Time: 9/7/2004 20:32:06
      Renew Time: 9/14/2004 10:32:06


   Server: HOST/serveur.DomaineBlah.com@DOMAINEBLAH.COM
      KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
      End Time: 9/7/2004 20:32:06
      Renew Time: 9/14/2004 10:32:06


   Server: E3514235-4B06-11D1-AB04-00C04FC2DCD2/276d4866-4940-49e4-91ec-991746ba
f84a/DomaineBlah.com@DOMAINEBLAH.COM
      KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
      End Time: 9/7/2004 20:32:06
      Renew Time: 9/14/2004 10:32:06


C:\>
```

Kerberos traffic: errors

- Kerberos traffic: common errors
  - KRB-ERROR (30) messages (`kerberos.msg.type == 30`)
    - KRB5KRB_AP_ERR_SKEW
      - Time synchronization problem
    - KRB5KDC_ERR_PREAUTH_FAILED
      - Pre-authentication error (typically, incorrect password)
    - KRB5KRB_AP_ERR_TKT_EXPIRED
      - Expired ticket, to be renewed
      - LSA keeps user passwords in cache and can request a new TGT, within a maximum limit of 7 days (*Max. Lifetime for user ticket renewal*)
    - KRB5KDC_ERR_S_PRINCIPAL_UNKNOWN
      - Principal not recognized by the KDC
      - Missing SPN (servicePrincipalName attribute) in an AD account?
      - Also when an IP address is used in a UNC path
        - NTLM authentication fallback

Kerberos tickets decryption

```
Client Realm: DOMAINEBLAH.COM
⊞ Client Name (Principal): vtsoin$
⊟ Ticket
    Tkt-vno: 5
    Realm: DOMAINEBLAH.COM
  ⊟ Server Name (Service and Instance): LDAP/serveur.DomaineBlah.com
      Name-type: Service and Instance (2)
      Name: LDAP
      Name: serveur.DomaineBlah.com
  ⊟ enc-part rc4-hmac
      Encryption type: rc4-hmac (23)
      Kvno: 21
    ⊟ enc-part: A9ADC3F96D13DD9C26E763D3DC902B8F...
        [Decrypted using: keytab principal serveur$@DOMAINEBLAH.COM]
      ⊟ EncTicketPart
          Padding: 0
        ⊞ Ticket Flags (Forwardable, Renewable, Pre-Auth, Ok As Delegate)
        ⊞ key rc4-hmac
          Client Realm: DOMAINEBLAH.COM
        ⊞ Client Name (Principal): vtsoin$
        ⊞ TransitedEncoding DOMAIN-X500-COMPRESS
          Authtime: 2004-08-27 13:32:15 (Z)
          Start time: 2004-08-27 13:32:15 (Z)
          End time: 2004-08-27 23:32:15 (Z)
          Renew-till: 2004-09-03 13:32:15 (Z)
        ⊟ AuthorizationData AD-IF-RELEVANT
            Type: AD-IF-RELEVANT (1)
          ⊟ Data: 308202623082025EA00402020080A182...
            ⊟ IF_RELEVANT AD-Win2k-PAC
                Type: AD-Win2k-PAC (128)
              ⊟ Data: 040000000000000001000000C0010000...
                  Num Entries: 4
                  Version: 0
                ⊞ Type: Logon Info (1)
                ⊞ Type: Client Info Type (10)
                ⊞ Type: Server Checksum (6)
                ⊞ Type: Privsvr Checksum (7)
⊟ enc-part rc4-hmac
    Encryption type: rc4-hmac (23)
  ⊟ enc-part: 71CAA300948E49193D8A4AFC32FD1DA7...
      [Decrypted using: key learnt from frame 79]
```

Active Directory replication

- Active Directory replication
  - `drsuapi` MSRPC interface (one TCP port)
  - Restricting Active Directory Replication Traffic to a Specific Port (MSKB #224196)
  - Between domain controllers
    - `DRSReplicaSync` operation (drsuapi)
      - Used to notify a replication partner that updates are available for replication
    - `DRSGetNCChanges` operation (drsuapi)
      - Used to obtain updates for a given AD Naming Context
    - RPC connection to the drsuapi service are authenticated using a Kerberos ticket obtained for the following principal:
      - `e3514235-4b06-11d1-ab04-00c04fc2dcd2` (drsuapi interface UUID)
      - Destination domain controller GUID
      - DNS domain name

FRS replication (File Replication Service)

- FRS replication
  - `frsrpc` MSRPC interface (1 TCP port)
  - How to Restrict FRS Replication Traffic to a Specific Static Port (MSKB #319553)
  - Between domain controllers
    - `FrsRpcStartPromotionParent` operation at DC startup
    - `FrsRpcSendCommPkt` operation for updates replication

NTP traffic

- NTP traffic
  - w32time service, started on domain member servers
  - NT5DS mode (by default), using AD hierarchy for time synchronization
  - NTP synchronization at startup, with a domain controller
    - Identified using CLDAP at system startup
    - Each 45 minutes (3 times), then each 8 hours
  - Synchronization mechanism
    - Client sends the RID of the machine account in the request, using the KeyID field
      - This RID was previously obtained in the response of the `NetrServerAuthenticate3` operation
    - Timestamp is signed (message authentication code field)

Other approaches

- Limitations of the network analysis approach
  - With encrypted traffic: LDAP and certain MSRPC operations
  - Trafic not properly dissected by the network analyzer
    - Typically with MSRPC, where RPC operations do not contain enough information to identify the DCE RPC interface
      → ethereal Decode As DCE-RPC function
- Other approaches
  - Correlation of network traces and logged events
    - Security and System eventlog of Windows systems
  - Diagnostic tools on servers
    - Ex: NTDS object statistics using the System Monitor tool (perfmon.msc)
    - Ex: tools to examine Kerberos tickets cache

Conclusion

- A good understanding of aforementionned protocols is needed to deploy Active Directory
- Network analysis is one of the possible way to obtain this understanding
  - Looking at these protocols on the wire, in a real environment, is a good complement to technical whitepapers reading
- Network analysis can also be used to diagnose anomalies
  - When diagnostic tools or logfiles are not enough...
- ethereal is a tool of choice to analyse network traces obtained in Active Directory environments

References: network traffic

- Network traffic in Windows environments
  - Windows 2000 Startup and Logon Traffic Analysis
    - http://www.microsoft.com/technet/prodtechnol/windows2000serv/deploy/confeat/w2kstart.mspx
  - Network Ports Used by Key Microsoft Server Products
    - http://www.microsoft.com/smallbusiness/gtm/securityguidance/articles/ref_net_ports_ms_prod.mspx
  - Using Windows { XP SP1, 2000 SP4, Server 2003} in a Managed Environment
    - http://go.microsoft.com/fwlink/?LinkId={22607, 22608, 22609}

References: DNS

- DNS implementation in Active Directory
  - Windows 2000 DNS White Paper
    - http://www.microsoft.com/windows2000/techinfo/howitworks/communications/nameadrmgmt/w2kdns.asp
  - RFC 3645 : Generic Security Service Algorithm for Secret Key Transaction Authentication for DNS (GSS-TSIG)

References: Kerberos

- Protocol
  - draft-ietf-krb-wg-kerberos-clarifications-08.txt
    - RFC 1510 update (original specification of Kerberos V)
    - http://kerberos.info/
- Documents
  - Troubleshooting Kerberos Errors (Microsoft)
    - http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/tkerberr.mspx
- Tools
  - klist, kerbtray (Microsoft)
  - tktview: http://msdn.microsoft.com/msdnmag/issues/0500/security/
  - leash32: http://web.mit.edu/kerberos/

References: LDAP

- LDAP and CLDAP
  - Active Directory Domain Controller Location Service (Anthony Liguori, Samba team)
    - CLDAP description (Connectionless LDAP)
    - http://oss.software.ibm.com/linux/presentations/samba/cifs2003/Liguorifinal.pdf
  - Active Directory LDAP compliance (Microsoft)
    - http://www.microsoft.com/windowsserver2003/techinfo/overview/ldapcomp.mspx
  - Active Directory LDAP schema (Windows 2000, Windows Server 2003 and ADAM)
    - http://msdn.microsoft.com/library/en-us/adschema/adschema/active_directory_schema.asp

References: SMB/CIFS and MSRPC

- Reference book on SMB/CIFS
  - Implementing CIFS
    - http://www.ubiqx.org/cifs/
- MSRPC
  - Windows network services internals
    - http://www.hsc.fr/ressources/articles/win_net_srv/
  - Testing MSRPC (Andrew Tridgell, Samba Team)
    - http://samba.org/ftp/samba/slides/tridge_cifs04.pdf
  - MSRPC architecture & security problems related
    - http://www.xfocus.net/projects/Xcon/2003/Xcon2003_kkqq.pdf
  - Microsoft Windows RPC Security Vulnerabilities
    - http://conference.hackinthebox.org/materials/lsd/

References: SNTP

- Microsoft references
  - The Windows Time Service
    - http://www.microsoft.com/technet/prodtechnol/windows2000serv/maintain/operate/wintime.mspx
  - Basic Operation of the Windows Time Service (MSKB #224799)
  - Windows Time Service Tools and Settings (Windows Server 2003 Technical Reference)
  - Using Windows XP Professional with Service Pack 1 in a Managed Environment (Windows Time Service)
    - http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/xpmanaged/27_xpwts.mspx
  - Security aspects of time synchronization infrastructure
    - http://www.security.nnov.ru/advisories/timesync.asp

Greetings

- Emmanuel Le Chevoir and Fabien Dupont
- ethereal developpers community