The golden age of hacking

Windows

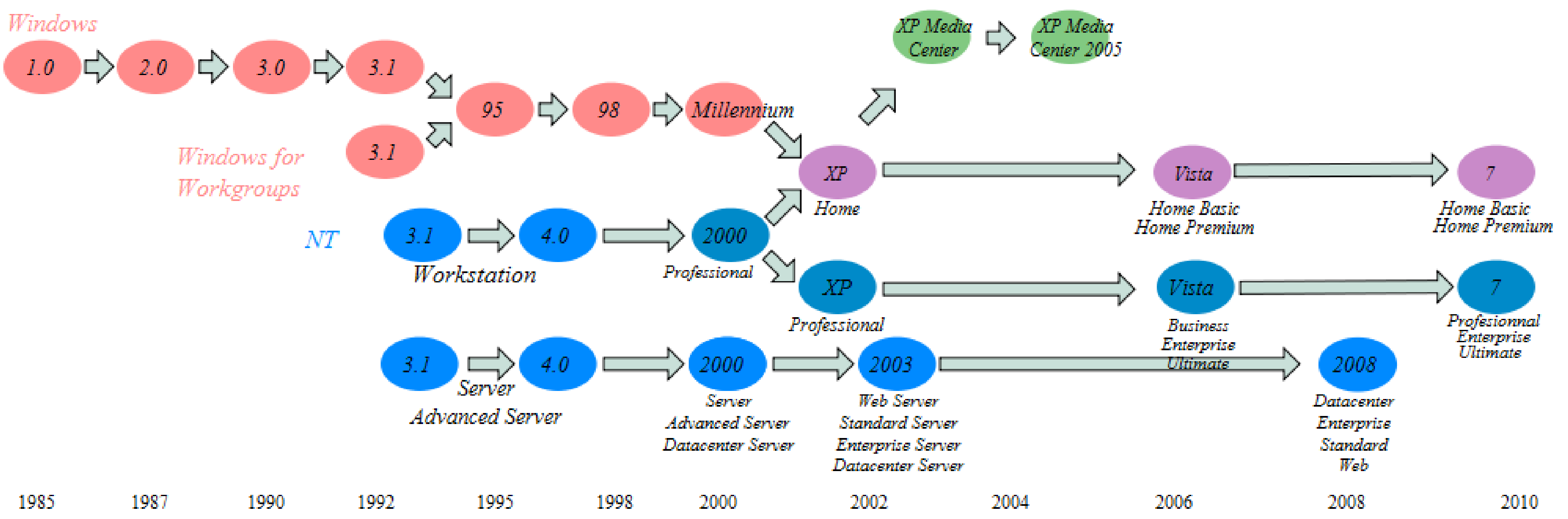
Reconnaissance

Google hacking

MS Windows

http://sv.wikipedia.org/wiki/Microsoft_Windows

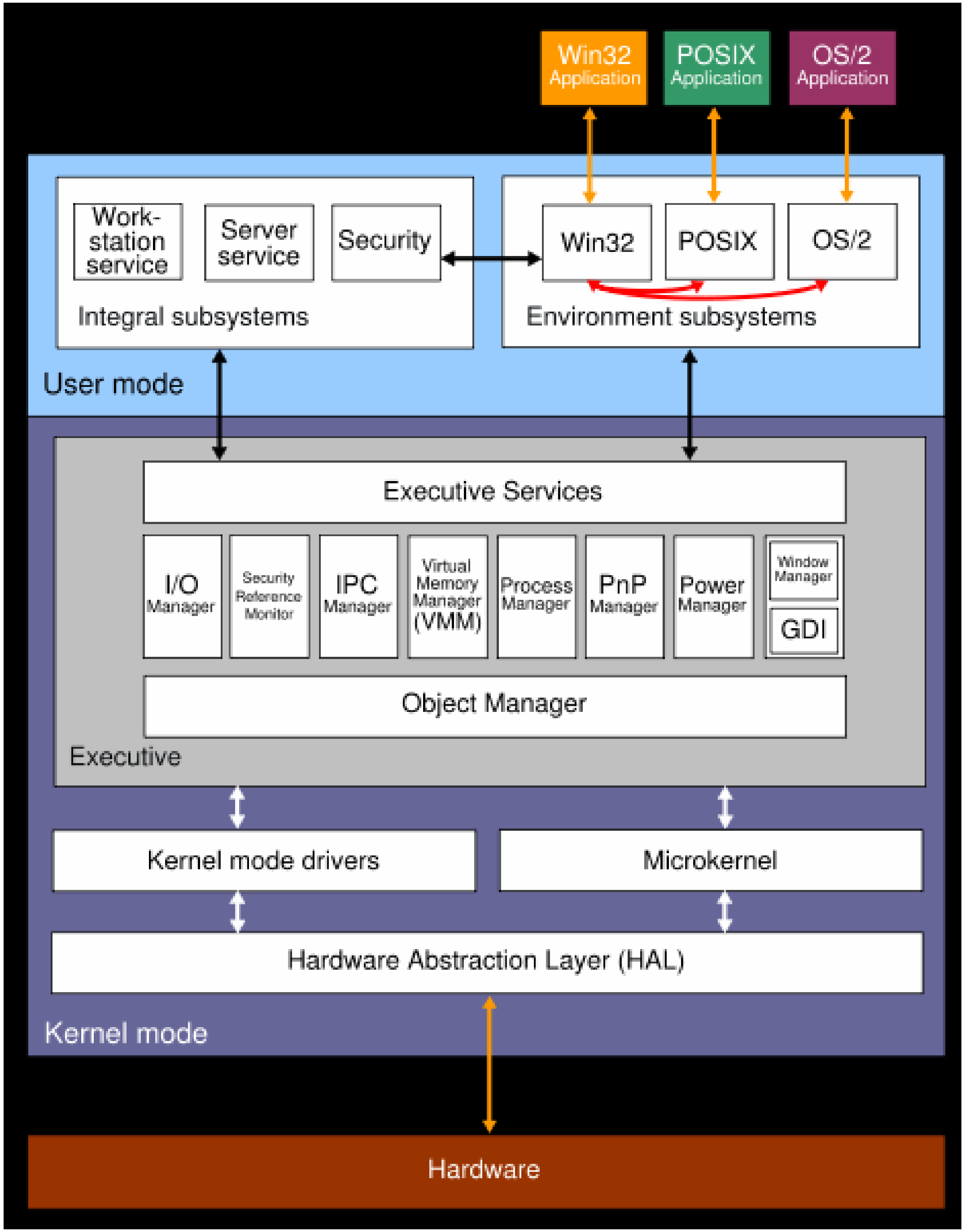
- Sure, the Almighty could create the world in six days. He didn’t have to deal with any legacy infrastructure!
  - Comment from a system developer trying to support backward compability ☺
- NT and DEC (Digital Equipment Corp.) VMS heritage
  - OS/2 & IBM



Microkernel

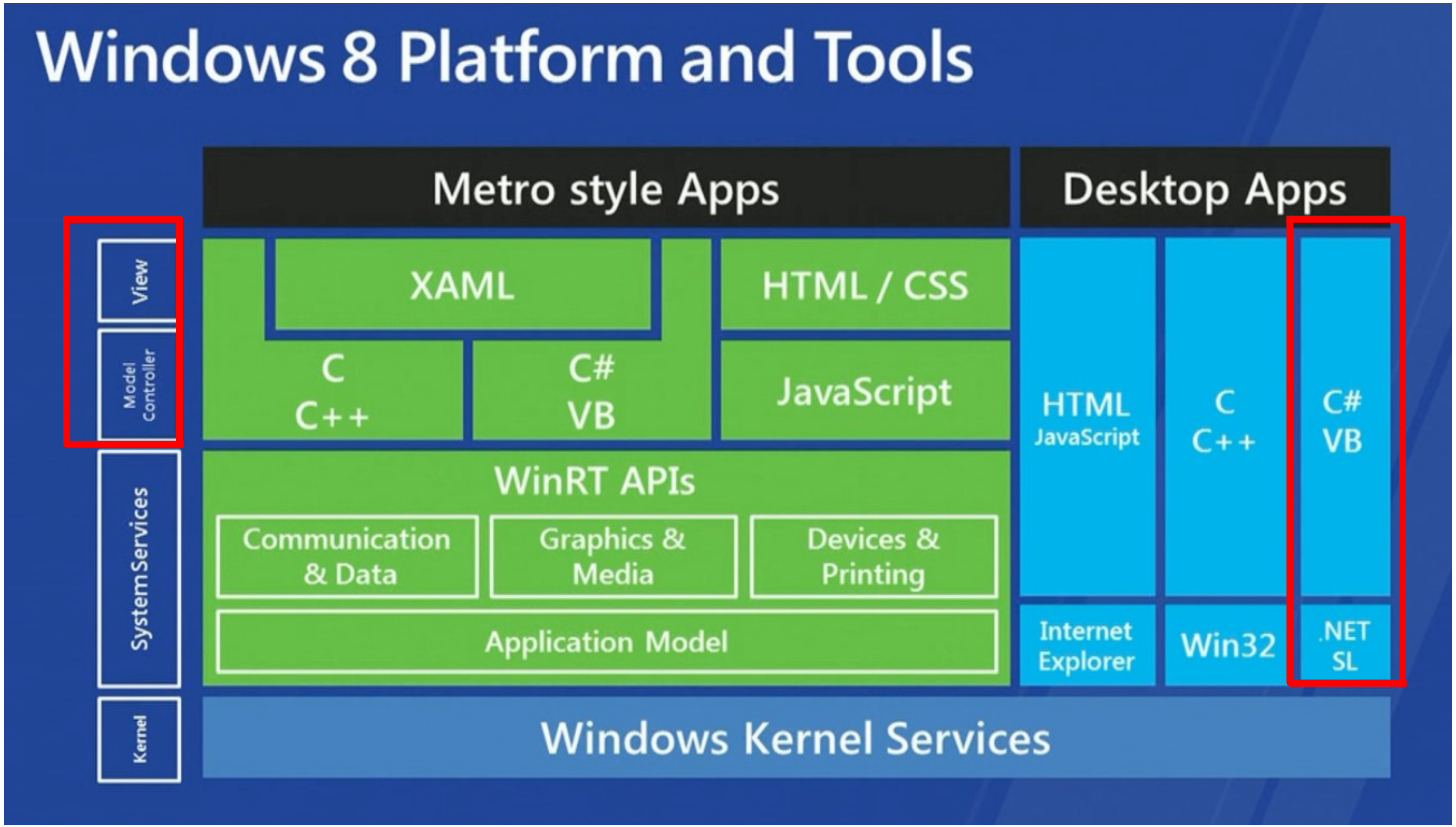
- A near-minimal kernel which provides the *mechanisms* needed to implement an OS
  - This includes low-level address space management, thread management, and inter-process communication (IPC)
- Operating-system services are provided by user-mode *servers* which are granted high privileges. These include device drivers, protocol stacks, file systems and user-interface code
  - Pros: better achieves least privilege, can tolerate failures/errors in device drivers, etc.
  - Cons: performance, failure in key OS services still brings down the system

- The Windows NT operating system family (including XP, Vista/7)
- A layered "microkernel"
- API Communication
- User mode
  - Integral subsystems
  - Environment subsystems
- Kernel mode
  - Executive subsystem
  - HAL



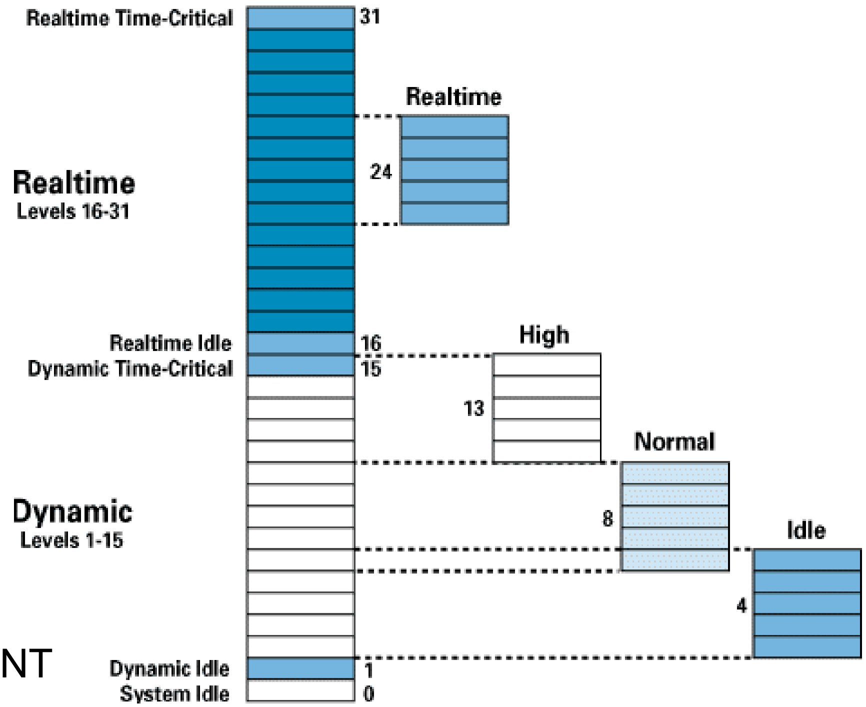
Windows 8 and HTML5

- XAML (Extensible Application Markup Language) is a declarative markup language which defines the view/design of an application
  - As applied to the .NET Framework programming model, XAML simplifies creating a UI for a .NET Framework and Silverlight (SL) applications together with Windows Presentation Foundation (WPF)
  - WinRT – An object oriented replacement for Win32



Kernel cont., domains before AD

- Integral subsystems
  - Win32 APIs which provides system calls into the kernel
  - Security functions as AD
- Executive subsystems
  - Security reference monitor
    - Check permissions of files and access to kernel mode etc.
  - Object manager
    - Manages all objects (OIDs) in the system as files, pipes etc.



http://en.wikipedia.org/wiki/Architecture_of_Windows_NT

- AD (Active Directory)
  - All domain controllers are authoritative
- Domain vs. Workgroup
- PDC vs. BDC (master and servant)
- The Security Account Manager (SAM)

LSA (Local Security Authority)

http://en.wikipedia.org/wiki/Local_Security_Authority_Subsystem_Service

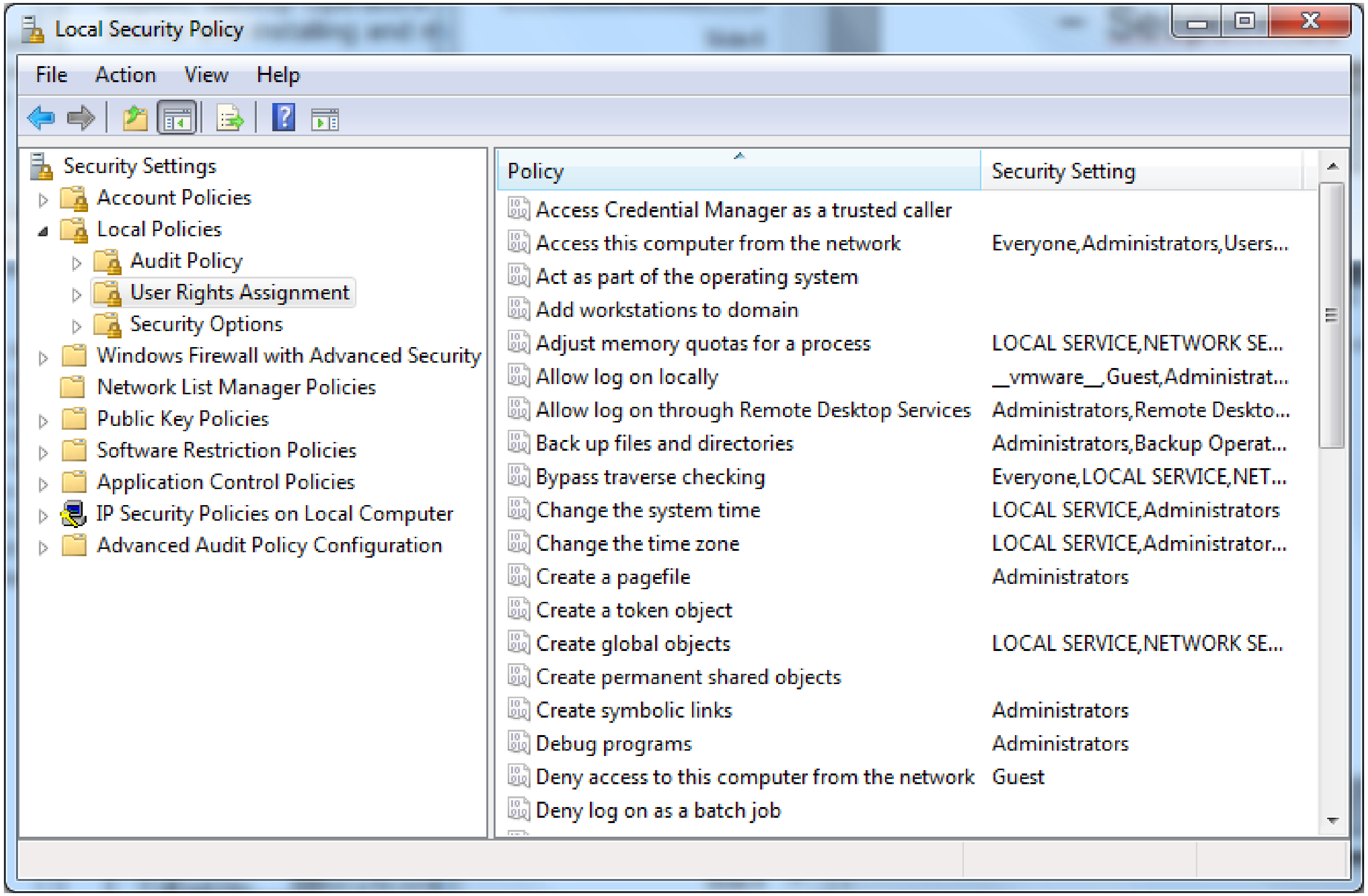
- Local Security Authority Subsystem Service (LSASS)
  - Verifies users logging on to a Windows computer or server
  - Handles password changes, and creates access tokens
  - Writes to the Windows Security Log
- SAM registry database store hashed passwords etc.
  - Dumped live with tools like Cain (also dead file), fgdump etc.
  - Two passwords was stored if password was < 15 chars
  - Account name, Relative ID (RID), LM & NT hash, optional fields…
  - LM hash
    - Adjust password to 14 chars, convert all to uppercase and pad with zeros, then split the ”fixed length” password to two 7-byte strings
    - These vaules create two 64-bit DES keys which encrypts ”KGS!@#$%” and creates two chipertext values that are the concatenated ”hash”
    - http://en.wikipedia.org/wiki/Lm_hash
  - NT(LM) hash
    - Hashed 3 times with 128 bit MD4
  - There is no salt in none of the algorithms which is standard in UNIX
    - http://en.wikipedia.org/wiki/Salt_%28cryptography%29

Accounts and groups

- Default accounts
  - Administrator (RID=500)
    - Not possible to delete or to be locked out from log in
  - Guest
    - Not possible to delete, should be disabled
  - Securing account strategies
    - Rename, decoys, remove description strings etc.
      - Additional admin account, disable original and/or rename account
- Groups are usually used for access control
  - Pre-Win2k/AD there were only **global** and **local** groups
  - Resource access were usually: user > global > local group
  - Not possible to do: global > global or local > local group
- Default groups and other special groups
  - A number of groups, run **lusrmgr.msc** to handle user/group settings or Microsoft Management Console - mmc.exe
  - SYSTEM is the ”holy grail” special user/group (not possible to logon and hidden in GUI)

Privilege control

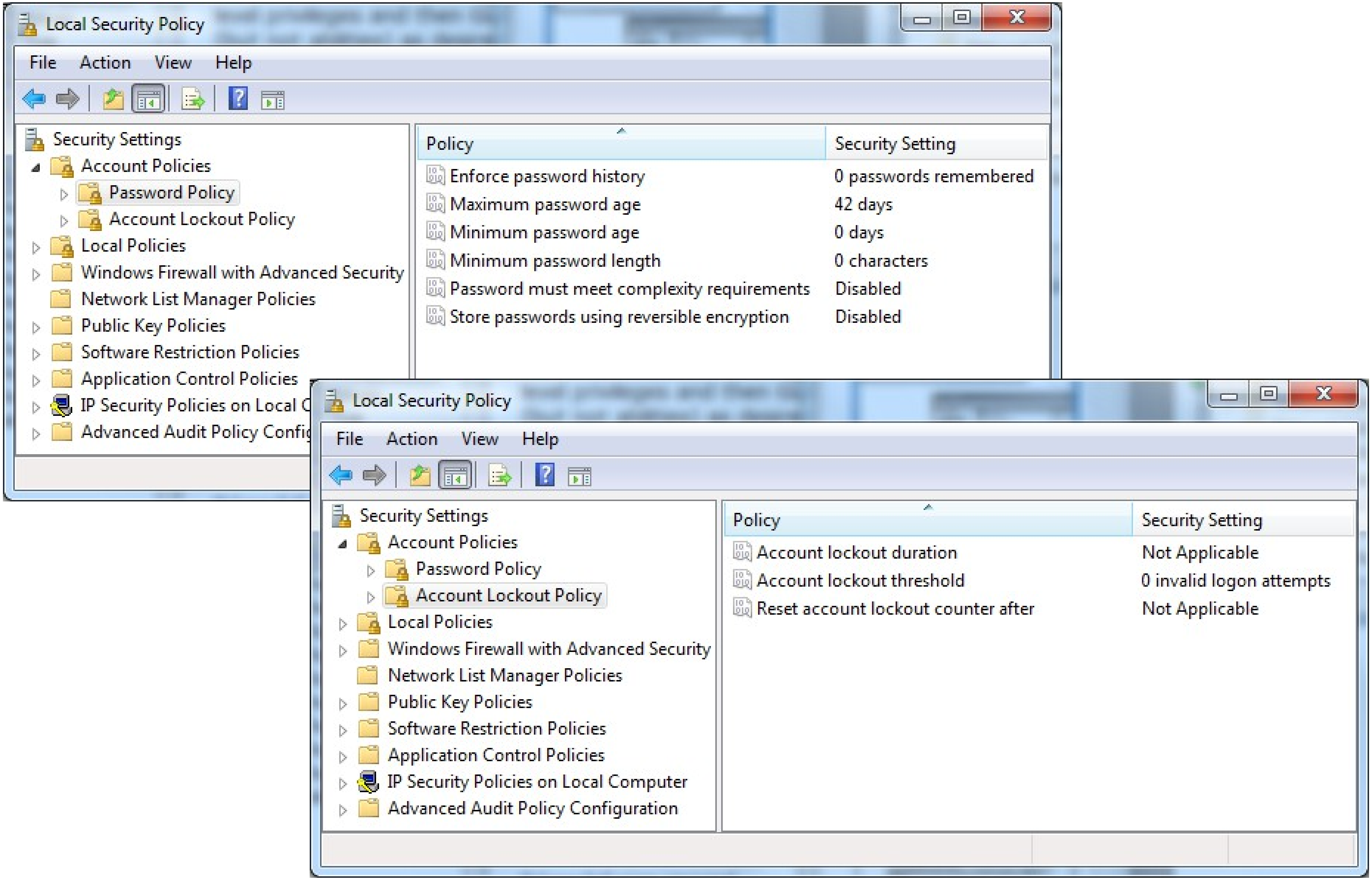
- Rights and abilities
  - Depends on group and settings in Local Security Policy
  - Secpol.msc



Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Firewall with Advanced Security
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Computer
Advanced Audit Policy Configuration

Policy	Security Setting
Access Credential Manager as a trusted caller	
Access this computer from the network	Everyone,Administrators,Users...
Act as part of the operating system	
Add workstations to domain	
Adjust memory quotas for a process	LOCAL SERVICE,NETWORK SE...
Allow log on locally	__vmware__,Guest,Administrat...
Allow log on through Remote Desktop Services	Administrators,Remote Deskto...
Back up files and directories	Administrators,Backup Operat...
Bypass traverse checking	Everyone,LOCAL SERVICE,NET...
Change the system time	LOCAL SERVICE,Administrators
Change the time zone	LOCAL SERVICE,Administrator...
Create a pagefile	Administrators
Create a token object	
Create global objects	LOCAL SERVICE,NETWORK SE...
Create permanent shared objects	
Create symbolic links	Administrators
Debug programs	Administrators
Deny access to this computer from the network	Guest
Deny log on as a batch job	

Account policies



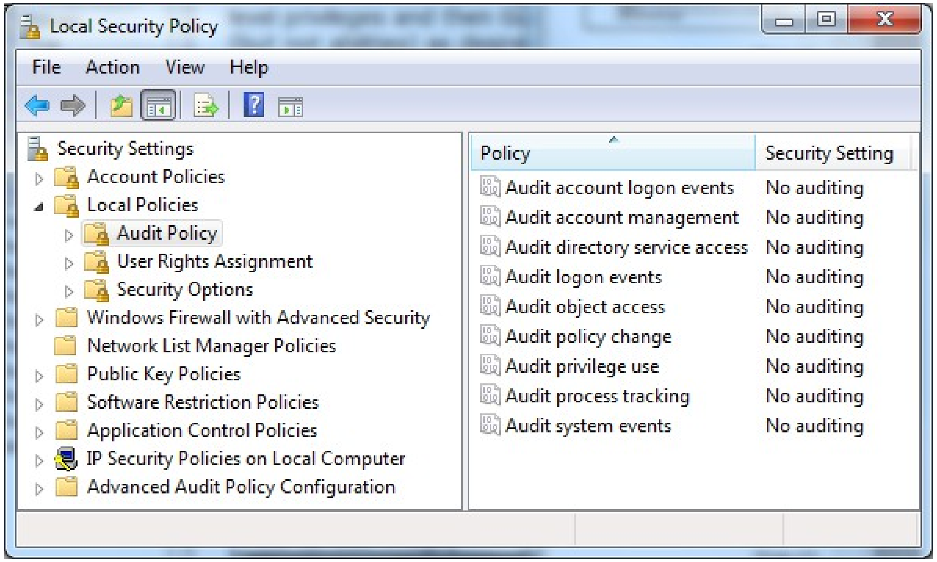
Security Settings
- Account Policies
  - Password Policy
  - Account Lockout Policy
- Local Policies
- Windows Firewall with Advanced Security
- Network List Manager Policies
- Public Key Policies
- Software Restriction Policies
- Application Control Policies
- IP Security Policies on Local Computer
- Advanced Audit Policy Configuration

Policy	Security Setting
Enforce password history	0 passwords remembered
Maximum password age	42 days
Minimum password age	0 days
Minimum password length	0 characters
Password must meet complexity requirements	Disabled
Store passwords using reversible encryption	Disabled

Policy	Security Setting
Account lockout duration	Not Applicable
Account lockout threshold	0 invalid logon attempts
Reset account lockout counter after	Not Applicable

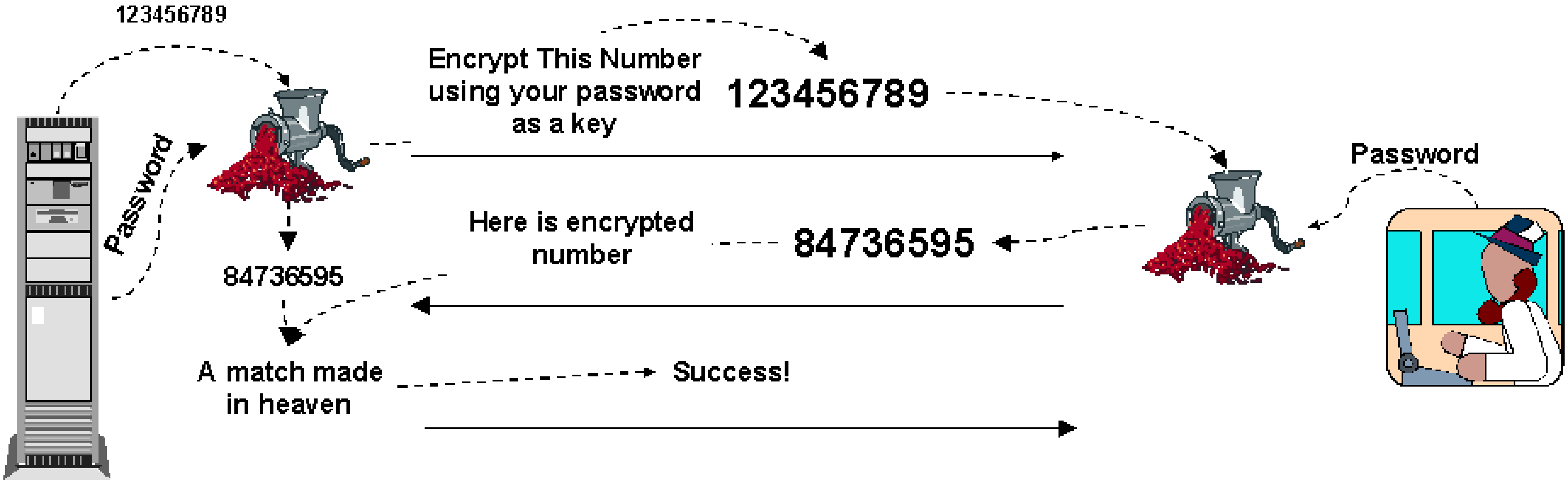
Trust and auditing

- There were four possible trusts models in Windows pre 2k
  - No trust
  - Complete trust
  - Master domain
  - Multiple master domain
  - They are based on challenge-response
- Three types of logging
  - System, security (auditing) and application logging
    - Auditing is off by default
  - Misses some important things for serious security logging
- Stores logs in "%systemroot%\system32\ + config\“ (XP) + winevt\Logs (Vista/7)
    - **Appevent.evt** - Contains a log of application usage
    - **Secevent.evt** - Records activities that have security implications such as logins
    - **Sysevent.evt** - Notes system events such as shutdowns
    - Vista/7/8 have a binary XML format (.evtx) and many many more logs
  - Tools as dumpel is useful for parsing the old logs
  - http://computer.forensikblog.de/en/2010/02/**evtx_parser**_1_0_2.html


Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Firewall with Advanced Security
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Computer
Advanced Audit Policy Configuration

Policy	Security Setting
Audit account logon events	No auditing
Audit account management	No auditing
Audit directory service access	No auditing
Audit logon events	No auditing
Audit object access	No auditing
Audit policy change	No auditing
Audit privilege use	No auditing
Audit process tracking	No auditing
Audit system events	No auditing

Challenge - Response authentication as
CHAP (Challenge Handshake Authentication Protocol)



Uses a varied shared secret authentication system without revealing the actual secret

The response is valid once and for a short time, new authentications can be done anytime

- The client makes a login attempt (not included in the state chart)
- The server generates a random number (challenge: 123456789 as an example) and encrypts the number along with the user's password as the key (which gives 84736595, the expected response)
- The server sends the challenge number to the client, as shown
- The client must be able to generate a valid response number from the challenge number using the same encryption algorithm with a valid password
- The client sends the response back to the server and if the encrypted numbers (not passwords) match each other, the client is logged in.

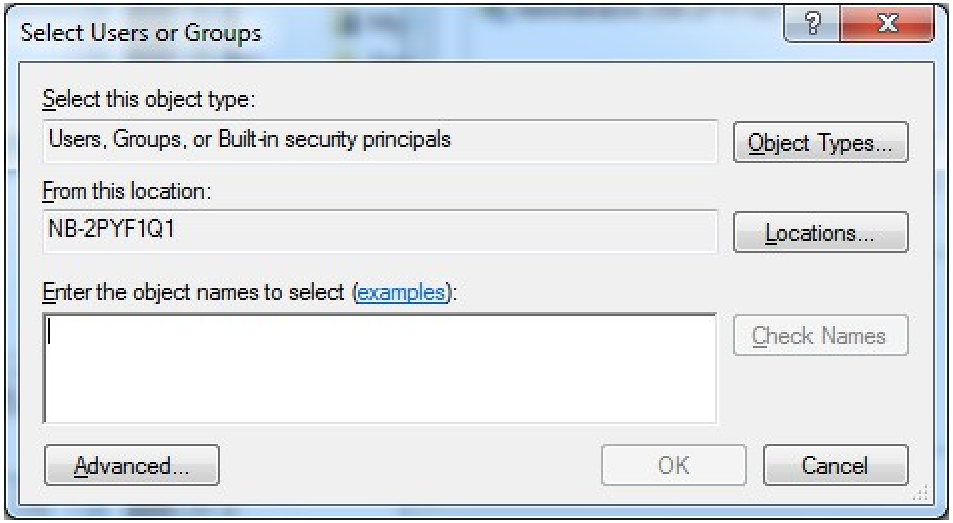
File/folder permissions

- CREATOR_OWNER
  - Every object has an owner, ownership means everything
- FAT offer no access control
- NTFS
  - Support 64 bit addressing, 255-characters
  - Four standard sets
    - No Access, Read, Change, Full Control
  - Special permissions (NTFS 4)
    - No Access, True Read, Execute, Write, Delete, Change Permissions and Take Ownership
  - Always use principle of least privileges when giving access permission
  - Limit the access from group Everyone
  - **Access rights is quite complex and bewildering, even worse in Win2k+**

Shares and permissions

net use \\<IP-address or hostname>\<share name> “passwd” /user:”username”

- Remote access depends on **both the NTFS and the share permission** working together in accordance to **least access** rule
- There are/have been flaws with default access permissions in \windows dirs
- Historically for files in \windows\repair
  - Security related files
  - Spare SAM

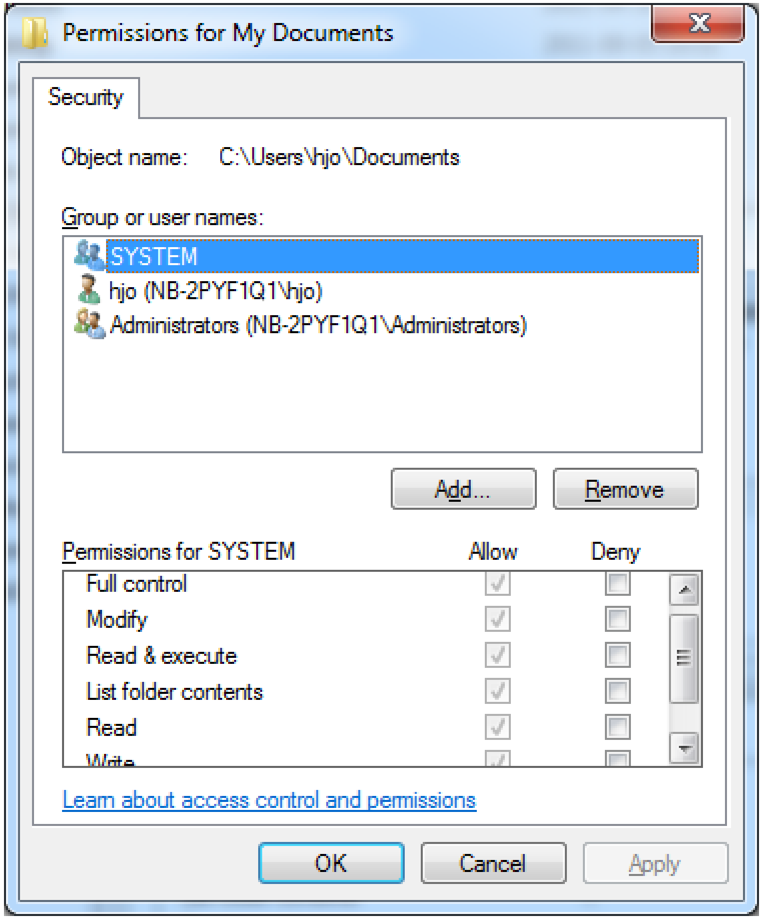


Select Users or Groups

Select this object type:
Users, Groups, or Built-in security principals

From this location:
NB-2PYF1Q1

Enter the object names to select (examples):



Permissions for My Documents

Security

Object name: C:\Users\hjo\Documents

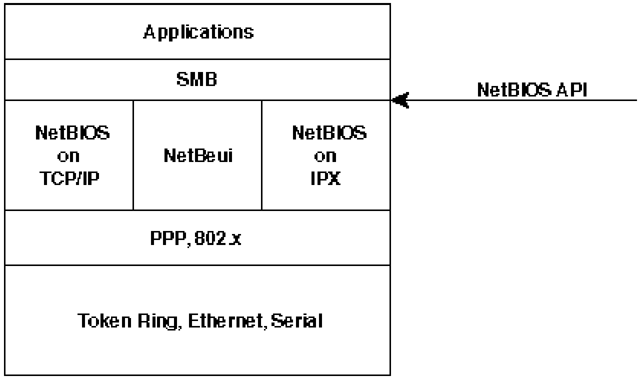
Group or user names:
SYSTEM
hjo (NB-2PYF1Q1\hjo)
Administrators (NB-2PYF1Q1\Administrators)

Permissions for SYSTEM	Allow	Deny
Full control	✓	□
Modify	✓	□
Read & execute	✓	□
List folder contents	✓	□
Read	✓	□
Write	✓	□

Learn about access control and permissions

SMB/CIFS and null sessions

- NetBEUI and NetBIOS
- net use \\<IP-address>\IPC$ “” /u:””
  - net view \\<IP-address>
- Works with pre-vista
- Net* Win32 API
- Enum
- DumpSec
- User2sid
- Sid2user
- GetAcct
- Winfo
- Winfingerprint
- Etc.



Applications

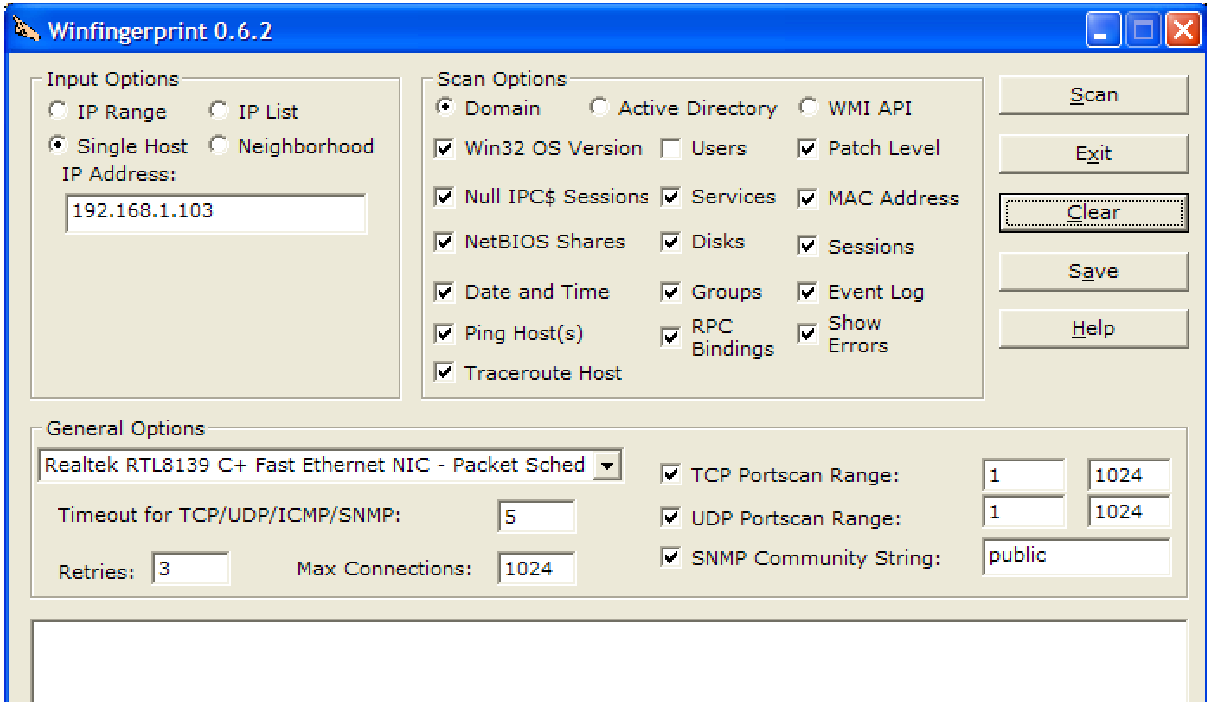
SMB

NetBIOS on TCP/IP | NetBeui | NetBIOS on IPX

PPP, 802.x

Token Ring, Ethernet, Serial

NetBIOS API



Winfingerprint 0.6.2

Input Options

○ IP Range ○ IP List

● Single Host ○ Neighborhood

IP Address: 192.168.1.103

Scan Options

● Domain ○ Active Directory ○ WMI API

☑ Win32 OS Version □ Users ☑ Patch Level

☑ Null IPC$ Sessions ☑ Services ☑ MAC Address

☑ NetBIOS Shares ☑ Disks ☑ Sessions

☑ Date and Time ☑ Groups ☑ Event Log

☑ Ping Host(s) ☑ RPC Bindings ☑ Show Errors

☑ Traceroute Host

General Options

Realtek RTL8139 C+ Fast Ethernet NIC - Packet Sched

Timeout for TCP/UDP/ICMP/SNMP: 5

Retries: 3 Max Connections: 1024

☑ TCP Portscan Range: 1 1024

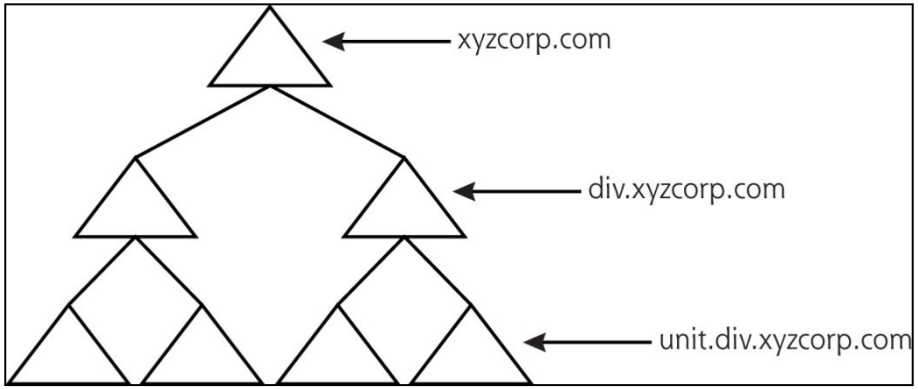
☑ UDP Portscan Range: 1 1024

☑ SNMP Community String: public

Windows 2000+

- Difference Windows 2K+ vs. older Windows
  - – Lots of new functions and security features
  - – Size, resource usage and complexity…++
  - – MS implementation of Kerberos
  - – MS implementation of IPSec
  - – L2TP, EFS, SSPI etc. …
  - – Native and mixed (compability) mode
  - – Active Directory
  - – Trust
    - Tree or forest
    - All authoritative
  - – No PDC/BDC
  - – LDAP

Tree



Lightweight Directory Access Protocol

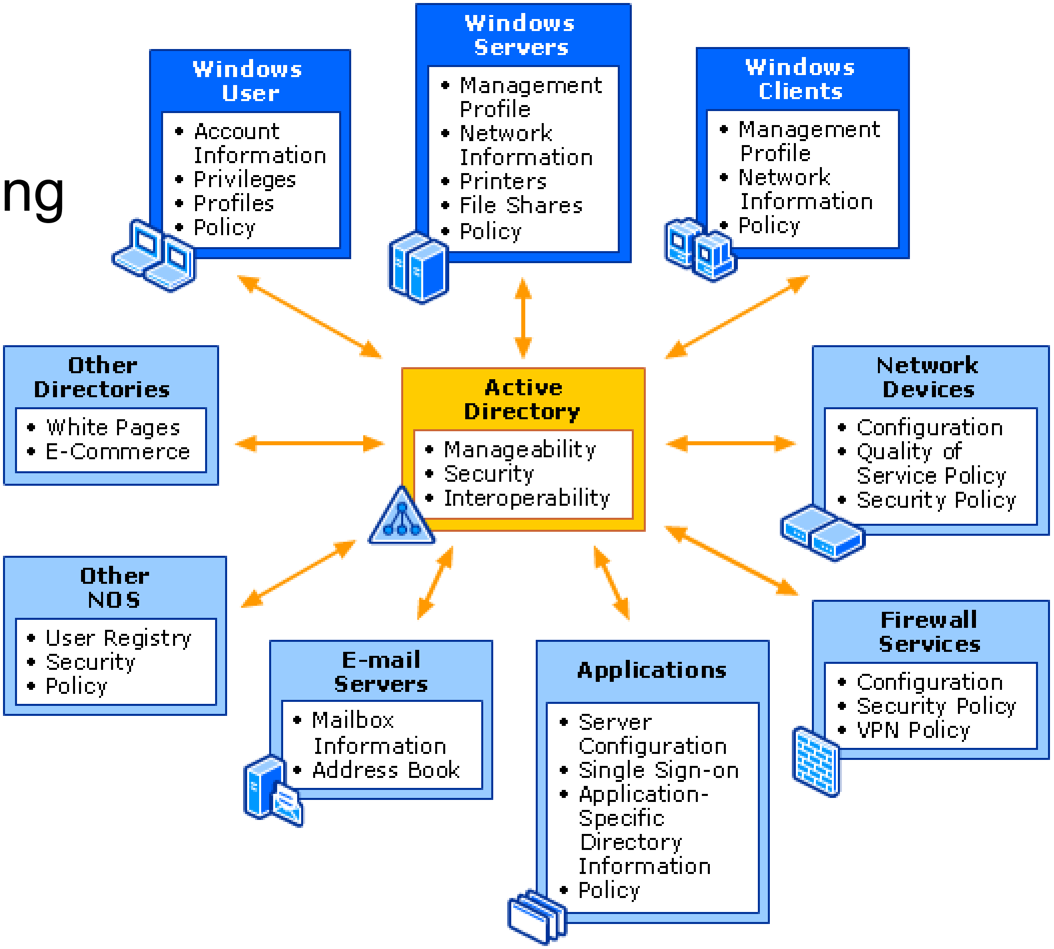
- LDAP is a binary application protocol for accessing and maintaining distributed directory information services over an IP network
- Directory services may provide any organized set of records, often with a hierarchical structure, such as a corporate electronic mail directory
- The protocol accesses LDAP directories, which follow the X.500 model
- A client starts an LDAP session (which may use TLS) by connecting to an LDAP server, called a Directory System Agent (DSA), by default on TCP port 389
    - A directory is a tree of directory entries
    - An entry consists of a set of attributes
    - An attribute has a name (an attribute type or attribute description) and one or more values
    - Each entry has a unique identifier: its Distinguished Name (DN)

```
dn: cn=John Doe,dc=example,dc=com
cn: John Doe
givenName: John
sn: Doe
telephoneNumber: +1 888 555 6789
telephoneNumber: +1 888 555 1232
mail: john@example.com
manager: cn=Barbara Doe,dc=example,dc=com
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: top
```

Example entry represented in LDAP Data Interchange Format (LDIF)

Active Directory in Windows 2000+

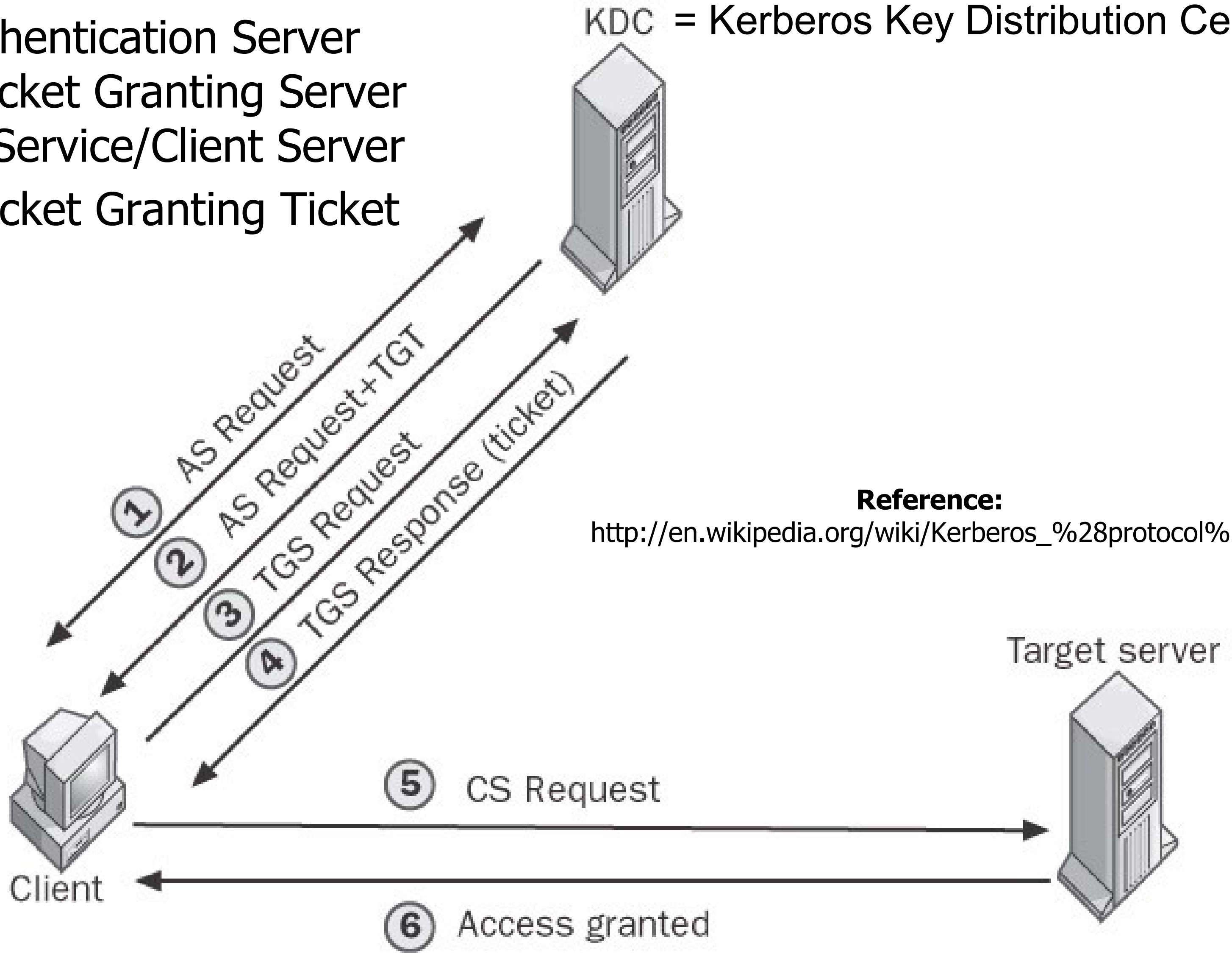
- A directory services DB
- Manage almost everything from one place!
- Uses DNS/DDNS
- Password hashfile
  - ntds.nit
- Correct installation and permissions are critical for secure and working AD!
- Client cache credentials
- MBSA (Microsoft Baseline Security Analyzer)



http://technet.microsoft.com/en-us/security/cc184924.aspx

Kerberos Authentication - 1

- AS = Authentication Server
- TGS = Ticket Granting Server
- (S)CS = Service/Client Server
- TGT = Ticket Granting Ticket



= Kerberos Key Distribution Center

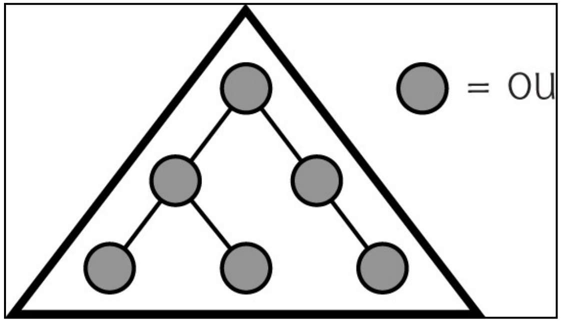
Reference:
http://en.wikipedia.org/wiki/Kerberos_%28protocol%29

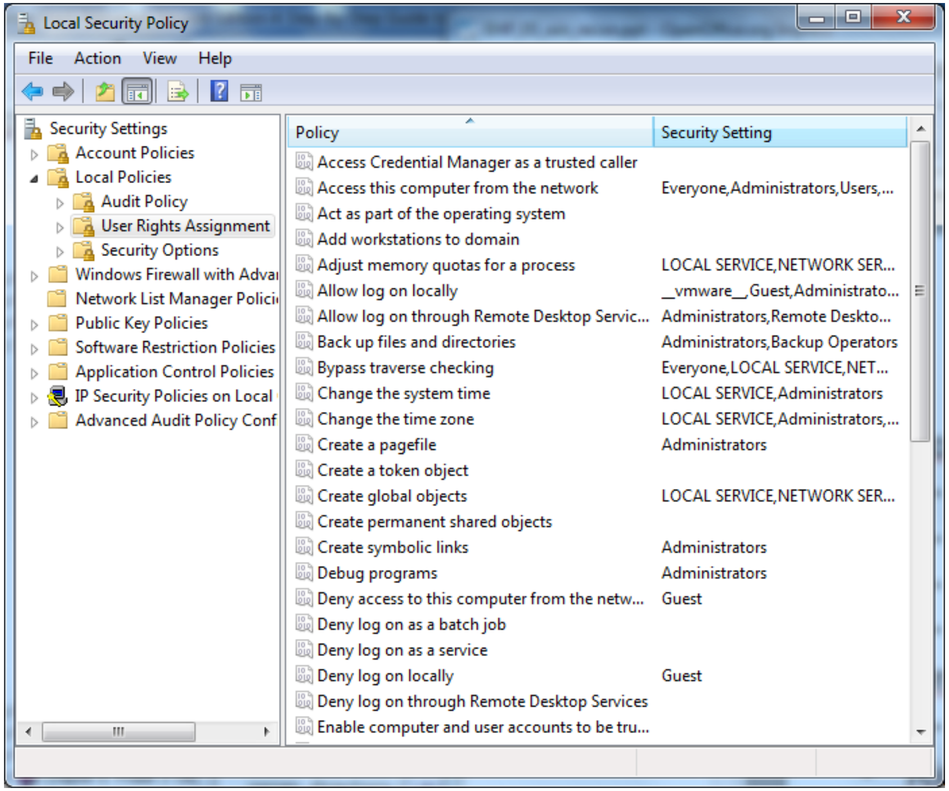
Kerberos Authentication – 2

1. The user’s credentials are entered on the client, which submits a request to the KDC to access the TGS using the AS Exchange protocol. The request includes encrypted proof of the user’s identity.
2. The KDC receives the request, looks up the master key of the user in Active Directory directory service, and decrypts the identify information contained in the request. If the user’s identity is verified, the KDC responds by granting the user a TGT and a session key using the AS Exchange protocol.
3. The client then sends the KDC a TGS request containing the TGT granted earlier and requesting access to some service on a target server using the TGS Exchange protocol.
4. The KDC receives the request, authenticates the user, and responds by granting the user a ticket and a session key for accessing the target server using the TGS Exchange protocol.
5. The client then sends the target server a request containing the ticket granted earlier using the CS Exchange protocol. The server authenticates the ticket, replies with a session key, and the client can now access the server.

Windows 2000+ cont.

- Accounts and groups - as pre-w2k mostly…
  - Default accounts are administrator and guest
  - Power Users is a new default group with high privilege (backward comp.)
  - Universal is a new addition to local and global groups
  - In native mode global groups can be member of other global groups
- Organizational units (OUs)
  - Privilege control etc.
  - Objects into directories
- Rights management
  - No built-in abilities
  - Inheritance of rights

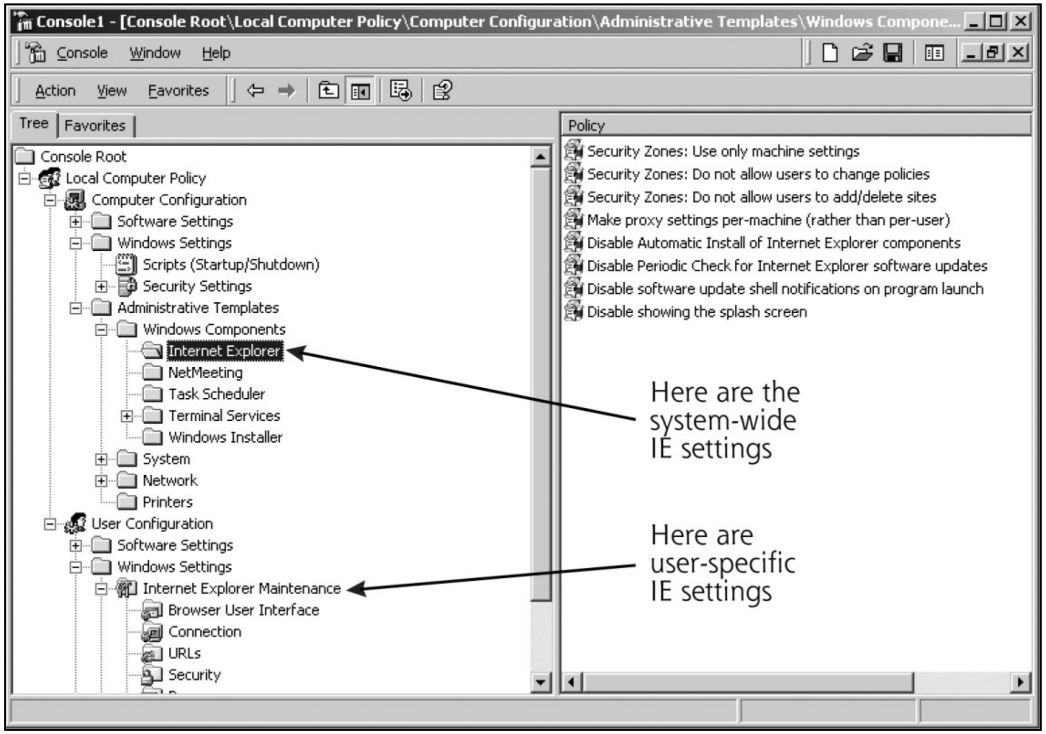



Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Firewall with Advai
Network List Manager Polici
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local
Advanced Audit Policy Conf

Policy	Security Setting
Access Credential Manager as a trusted caller	
Access this computer from the network	Everyone,Administrators,Users,...
Act as part of the operating system	
Add workstations to domain	
Adjust memory quotas for a process	LOCAL SERVICE,NETWORK SER...
Allow log on locally	__vmware__,Guest,Administrato...
Allow log on through Remote Desktop Servic...	Administrators,Remote Deskto...
Back up files and directories	Administrators,Backup Operators
Bypass traverse checking	Everyone,LOCAL SERVICE,NET...
Change the system time	LOCAL SERVICE,Administrators
Change the time zone	LOCAL SERVICE,Administrators,...
Create a pagefile	Administrators
Create a token object	
Create global objects	LOCAL SERVICE,NETWORK SER...
Create permanent shared objects	
Create symbolic links	Administrators
Debug programs	Administrators
Deny access to this computer from the netw...	Guest
Deny log on as a batch job	
Deny log on as a service	
Deny log on locally	Guest
Deny log on through Remote Desktop Services	
Enable computer and user accounts to be tru...	

Windows 2000+ cont.

- RunAs (as sudo http://en.wikipedia.org/wiki/Sudo)
  - GUI version, right click on exe…
- Group Policy objects
  - Start > run > mmc > File > add/remove snap-in. Choose Group policy > click add then finish/ok
- Auditing
  - Nine event categories ++
- Access control permissions
  - Standard (NTFS-5)
    - Full Control
    - Modify
    - Read & execute
    - Read
    - Write
    - List contents (folders)
  - Special permissions
    - 14 different perms.
    - http://www.windowsitlibrary.com/Content/592/toc.html



Console1 - [Console Root\Local Computer Policy\Computer Configuration\Administrative Templates\Windows Compone...

Policy
- Security Zones: Use only machine settings
- Security Zones: Do not allow users to change policies
- Security Zones: Do not allow users to add/delete sites
- Make proxy settings per-machine (rather than per-user)
- Disable Automatic Install of Internet Explorer components
- Disable Periodic Check for Internet Explorer software updates
- Disable software update shell notifications on program launch
- Disable showing the splash screen

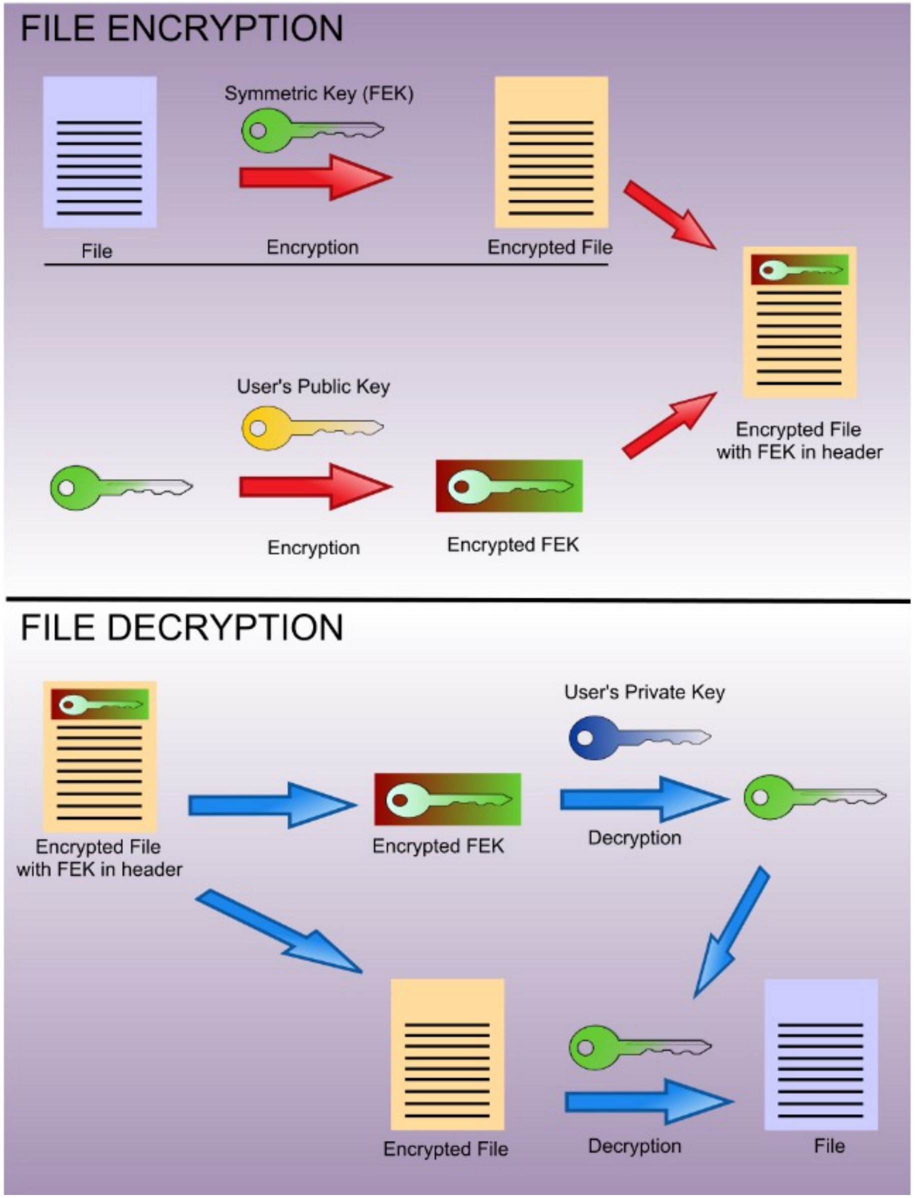
Here are the system-wide IE settings

Here are user-specific IE settings

EFS (Encrypting File System)

http://www.answers.com/topic/encrypting-file-system?cat=technology

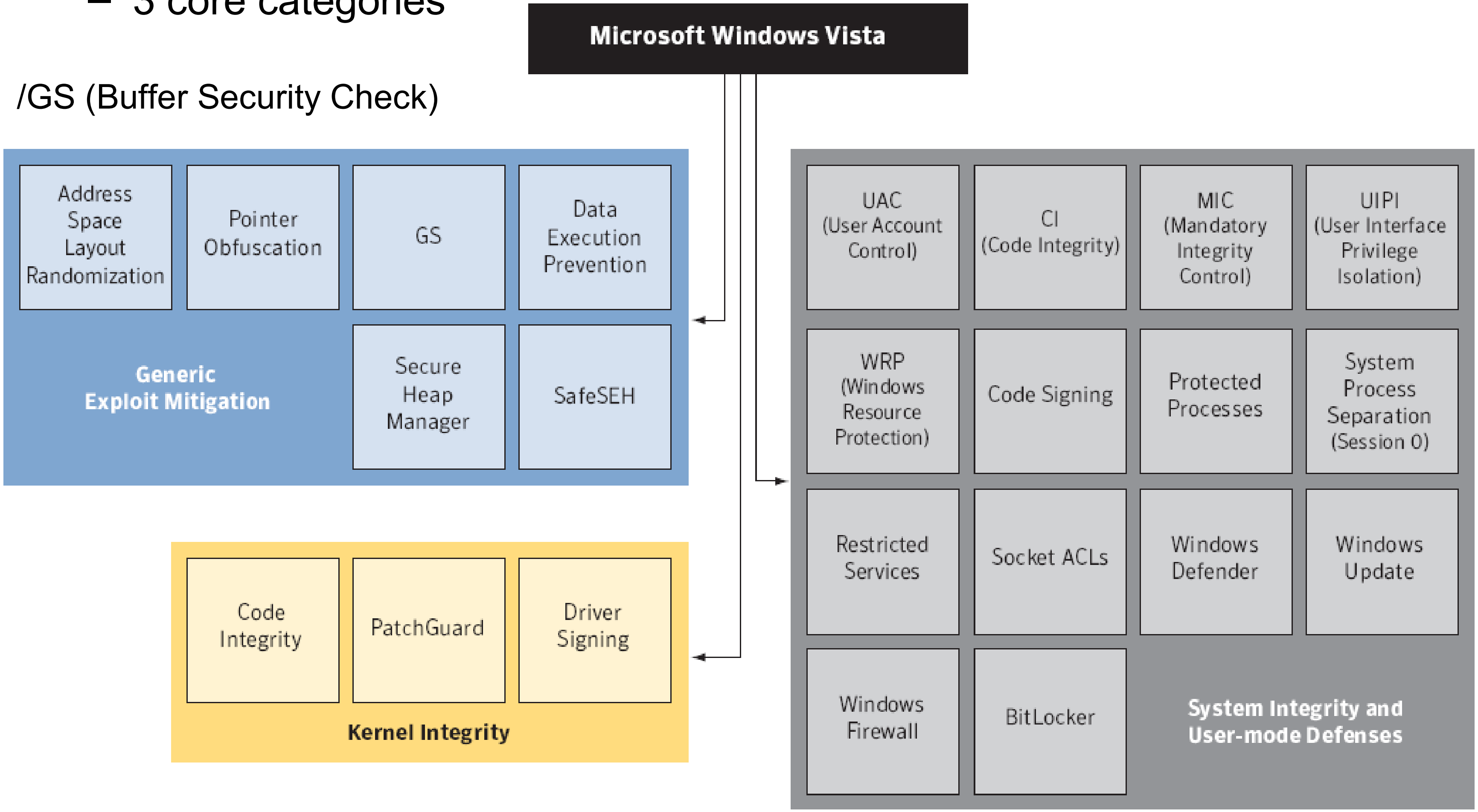
- EFS works by encrypting a file with a random bulk symmetric key, also known as the File Encryption Key (FEK)
- The FEK is then encrypted with a public key that is associated with the user who encrypted the file, and this encrypted FEK is stored in the $EFS alternate data stream of the encrypted file
- To decrypt the file, the EFS component driver uses the private key that matches the EFS digital certificate to decrypt the symmetric key that is stored in the $EFS stream
- The EFS component driver then uses the symmetric key (FEK) to decrypt the file
- Transparent for user



Windows Vista security

- Symantec research – objective analysis - **very good read!**
  - http://www.symantec.com/business/theme.jsp?themeid=vista_research
  - 3 core categories

/GS (Buffer Security Check)


Microsoft Windows Vista
Address Space Layout Randomization
Pointer Obfuscation
GS
Data Execution Prevention
Generic Exploit Mitigation
Secure Heap Manager
SafeSEH
Code Integrity
PatchGuard
Driver Signing
Kernel Integrity
UAC (User Account Control)
CI (Code Integrity)
MIC (Mandatory Integrity Control)
UIPI (User Interface Privilege Isolation)
WRP (Windows Resource Protection)
Code Signing
Protected Processes
System Process Separation (Session 0)
Restricted Services
Socket ACLs
Windows Defender
Windows Update
Windows Firewall
BitLocker
System Integrity and User-mode Defenses

Windsows wrap up

- Security in Windows is anything but easy!
  - Backward compability
    - Example: avoid LM Passwords
  - Complex
- IIS (Internet Information Service)
  - Large number of security threats over the years
- Security templates and hardening guides
  - www.cisecurity.org, www.sans.org, www.securityforum.org
- Vista/7 brings: security evolution not revolution
  - Most of tech in XP SP2 but disabled, now enabled and enhanced
  - Attackers have already moved on to apps on top of OS
  - Vista/7 user mode services
    - Paper: http://go.microsoft.com/fwlink/?LinkId=71280
    - Limiting access to services by user applications
    - "Hardening" services to limit the ability of a compromised service to damage a system
    - Restricted Network Access

Windows 8 security

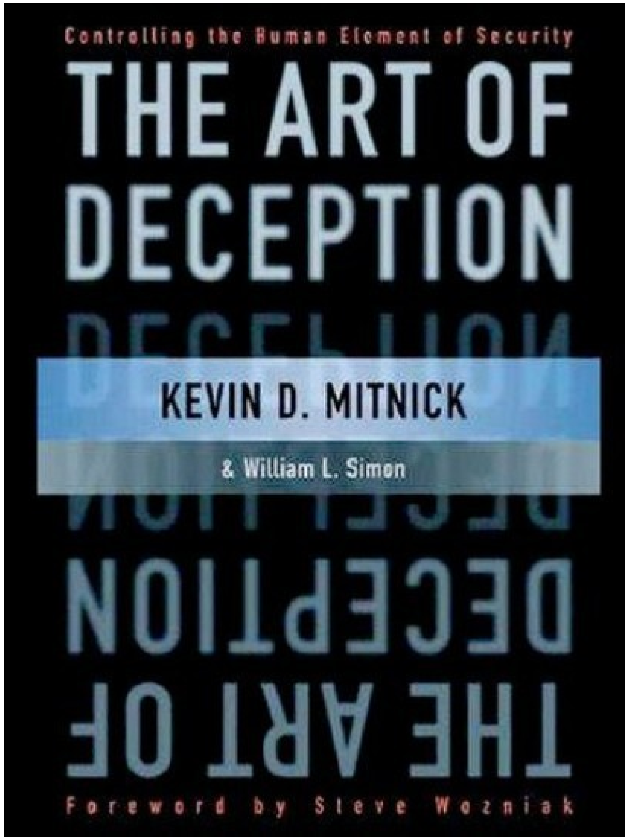
- 8 new security functions in Windows 8 and server 2012

1. Secure Boot – UEFI (Unified Extensible Firmware Interface) is a modern BIOS which only allow signed software in the boot sequence
2. Early Launch Anti-Malware – AV agent start before malware
3. Smartscreen – keep track of (dangerous) web sites and files ”reputation”
4. Dynamic access control – more fine grained
5. PC Refresh och Reset – reinstall of OS keeping user data or full reset
6. Appcontainer – isolate applications in sandboxes with permission control
7. Windows Defender – the new MS Security Essentials
8. Pictures as passwords – make a certain pattern on the picture

- Read more: Åtta viktiga funktioner > http://computersweden.idg.se/2.2683/1.490829/atta-viktiga-funktioner
- SMEP (Supervisor Mode Execution Prevention) kernel buffer overflow protection for the ones with a Intel Ivy Bridge CPU
- Read more: http://blog.ptsecurity.com/2012/09/intel-smep-overview-and-partial-bypass.html

Reconnaissance

- Social engineering
  - Password stealing
    - Kevin Mitnick – The art of Deception
  - Caller ID spoofing
    - In-house phone number
  - Reverse social engineering
- Physical break-in
- Dumpster Diving
- Defense
  - Awareness
  - Policies
  - Locking equipment and encryption
  - Destroying (or erasing) equipment correct


Controlling the Human Element of Security
THE ART OF DECEPTION
KEVIN D. MITNICK
& William L. Simon
Foreword by Steve Wozniak

Google hacking (applies for other search engines as well) - 4 important elements

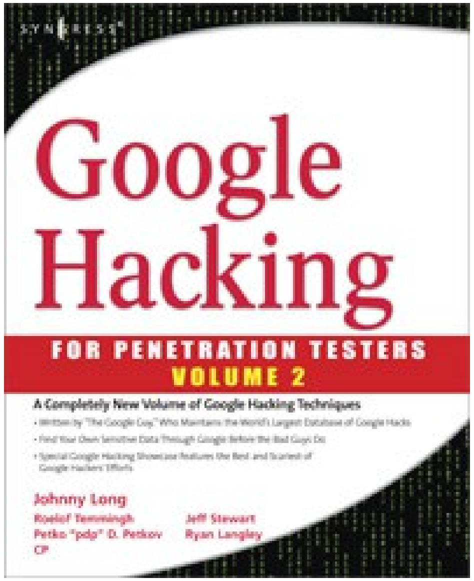
- Google bots
  - Crawls all websites on Internet every 24h!
- Google index
  - THE INDEX, 8 billion (2006) web sites/pages, now 45+ billion
  - http://www.worldwidewebsize.com/
  - Algorithm - PageRank
    - http://infolab.stanford.edu/~backrub/google.html

WorldWideWebSize.com
DAILY ESTIMATED SIZE OF THE WORLD WIDE WEB

- Google cache
  - Copy of Internet (not all ☺), large docs indexed (first 101kB)
  - Text but not images or code are cached?
- Google API:s (Google code)
  - https://developers.google.com/
  - My Google Maps API examples: www.du.se/~hjo/lbs
  - Using Google API needs a Google API key
    - https://code.google.com/apis/console

Google
Developers

Google hacking 1


SYNGRESS
Google Hacking
FOR PENETRATION TESTERS
VOLUME 2
A Completely New Volume of Google Hacking Techniques
• Written by "The Google Guy" Who Maintains the World's Largest Database of Google Hacks
• Find Your Own Sensitive Data Through Google Before the Bad Guys Do
• Special Google Hacking Showcase Features the Best and Scariest of Google Hackers' Efforts
Johnny Long
Roelof Temmingh
Petko "pdp" D. Petkov
CP
Jeff Stewart
Ryan Langley

- Books are written in this subject
  - Google Hacking for Penetration Testers by Johnny Long etc.
- Google Advanced search (graphical)
- Number of results is max 1000
  - Not enough for data mining
- Important tips
  - Searches are always case insensitive
  - When using directive as ”site:” do not use white space between directive and search term
  - Max 10 search terms (including directive)

Google hacking 2

http://www.google.com/help/operators.html

- site:[domain]
  - Only search on this domain, site:.se is also possible
- link:[web page]
  - Shows all sites linked to a given web page
- intitle:[term(s)]
  - Finds pages with given search title
- related:[site]
  - Similar pages to given search page
- cache:[page url] (highlighted search terms)
  - Display a page from the Google cache
  - Example: cache:http://users.du.se/~hjo/ hans jones
- inurl:[term(s)]
  - Restrict the results to documents containing that word in the url

Google hacking 3

http://www.google.com/help/operators.html

- filetype:[suffix]
  - Only search files of given type
- rphonebook:[name and city/state]
  - Only US residents just now
- bphonebook:[name and city/state]
  - Only US business just now
- phonebook:[name and city/state]
  - Both above combined
- Literal matches (”search terms”)
  - Search is done on whole string in given order
- Not (-term)
  - Filters out web pages with given term
- Plus (+term)
  - Filters in web pages with given term that Google normally will filter out, +the, +how…

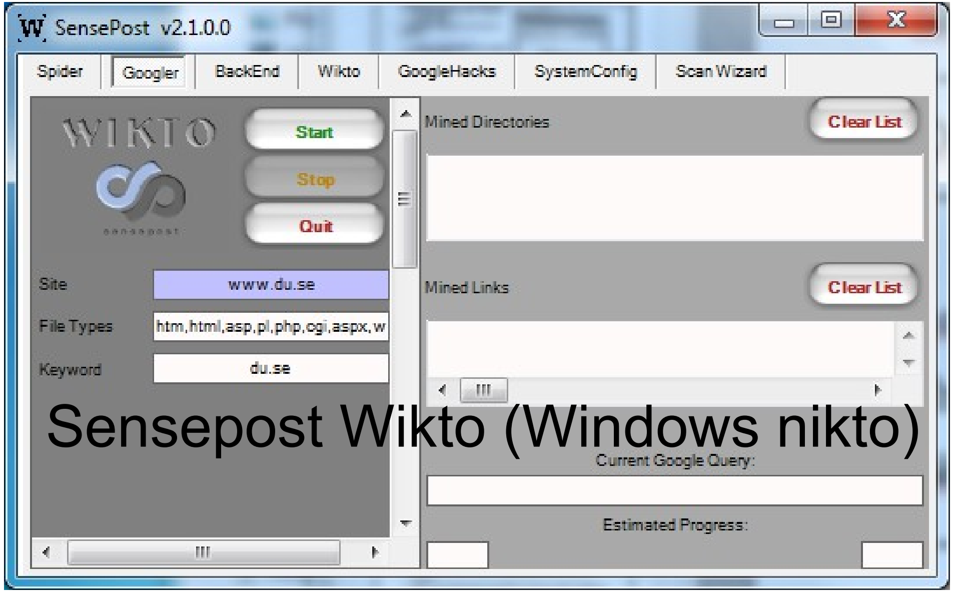
Google hacking 4 - nasty examples

- site:swedbank.se filetype:xls account -filetype:pdf
- kickstart filetype:cfg
  - Finds Redhat Linux unattended installations which may contain intresting info as password hashes!
- mysql dump filetype:sql
  - This search reveals all the exposed MySQL backups taken on a system which have been subjected (indexed) to Google, often these dumps contain juicy information like usernames, passwords, emails, credit card numbers etc.
- There are hundreds of interesting searches that can be made, and most of them are (were?) listed in Johnny Longs website: http://johnny.ihackstuff.com/
- Alternate resources: http://jwebnet.net/advancedgooglesearch.html
- http://safecomputing.umich.edu/events/download/brashars_sumit_05.pdf
- Johnny's presentation from Blackhat 2005
  - http://www.blackhat.com/presentations/bh-usa-05/bh-us-05-long.pdf

Google hacking 5

Google API allows for interesting automated recon software tools to be created as: http://www.sensepost.com/labs/tools/pentest/wikto

```
#!/usr/bin/python
import google
google.setLicense('XXXXXXXXXXXXXX')
data = google.doGoogleSearch('0day attack')
i = 1
for result in data.results:
    print "Result", i, "of", len(data.results)
    print "  URL: ", result.URL
    print "           Title: ", result.title
    i = i + 1
```

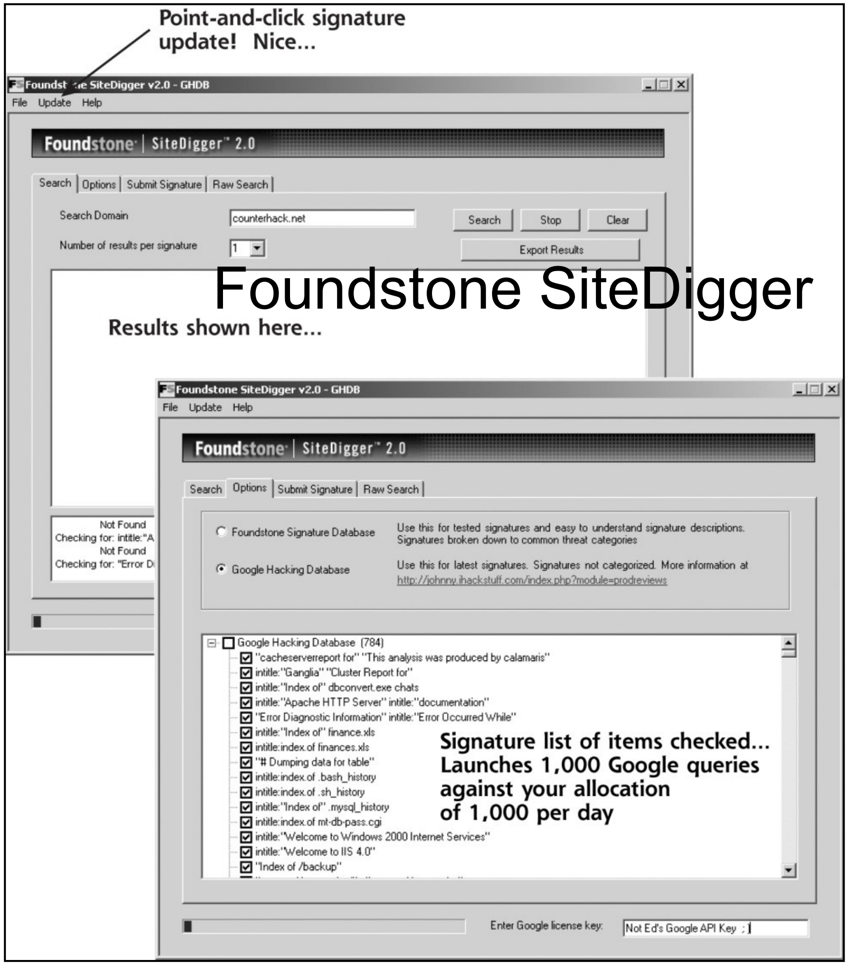


Site: www.du.se

File Types: htm,html,asp,pl,php,cgi,aspx,w

Keyword: du.se

Sensepost Wikto (Windows nikto)



Point-and-click signature update! Nice...

Search Domain: counterhack.net

Number of results per signature: 1

Foundstone SiteDigger

Results shown here...

Not Found
Checking for: intitle:"A
Not Found
Checking for: "Error Di

○ Foundstone Signature Database — Use this for tested signatures and easy to understand signature descriptions. Signatures broken down to common threat categories

● Google Hacking Database — Use this for latest signatures. Signatures not categorized. More information at http://johnny.ihackstuff.com/index.php?module=prodreviews

- □ Google Hacking Database (784)
  - ☑ "cacheserverreport for" "This analysis was produced by calamaris"
  - ☑ intitle:"Ganglia" "Cluster Report for"
  - ☑ intitle:"Index of" dbconvert.exe chats
  - ☑ intitle:"Apache HTTP Server" intitle:"documentation"
  - ☑ "Error Diagnostic Information" intitle:"Error Occurred While"
  - ☑ intitle:"Index of" finance.xls
  - ☑ intitle:index.of finances.xls
  - ☑ "# Dumping data for table"
  - ☑ intitle:index.of .bash_history
  - ☑ intitle:index.of .sh_history
  - ☑ intitle:"Index of" .mysql_history
  - ☑ intitle:index.of mt-db-pass.cgi
  - ☑ intitle:"Welcome to Windows 2000 Internet Services"
  - ☑ intitle:"Welcome to IIS 4.0"
  - ☑ "Index of /backup"

Signature list of items checked... Launches 1,000 Google queries against your allocation of 1,000 per day

Enter Google license key: Not Ed's Google API Key ;)

Other recon sites

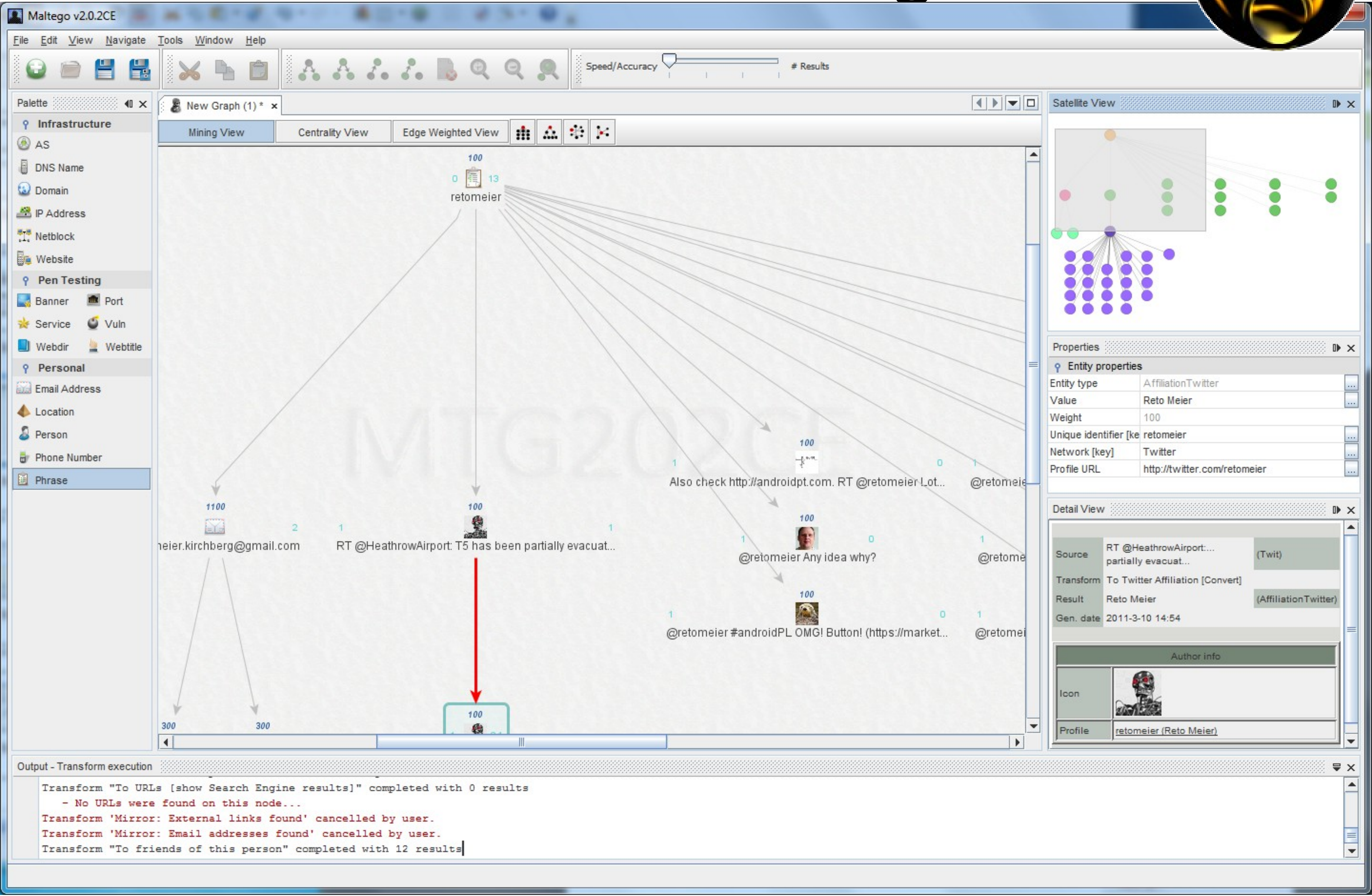
- The organizations web sites
  - Contact info, myriad of clues about tech, buisiness partners, open jobs etc.
- Newsgroups
  - Usenet, Yahoo and Google groups, ..., etc.
- Social media
  - Social networking, blogs, microblogging, ..., etc.
- Use other search engines

  http://www.searchengineshowdown.com/features/
- Netcraft.com
  - Internet exploration/monitoring and data mining
  - Netcraft can be used to indirectly find out information about web servers on the internet, including the underlying operating system, web server version, uptime graphs, etc.

Web hacking

- Email harvesting from web pages is an effective way of finding out possible emails (and possibly usernames) belonging to an organization
  - [server] /pen-test/python/goog-mail.py <domain-name>
  - When done harvesting, back tracing a specific user can reveal specific job titles as IT-admins etc.
- Finding vulnerable web application servers
  - Search for new vulnerabilities using Google yourself
  - Use GHDB (Google Hacking Database), Johhny L.
    - http://www.hackersforcharity.org/ghdb/
- Scraping (filter out vulnerabilities)
  - Compare search engines against each other
  - Yahoo, Bing, …
- Wayback machine, the Internet archive
  - Cached webpages over the years
  - http://www.archive.org

Paterva Maltego



Entity properties

Entity type	AffiliationTwitter
Value	Reto Meier
Weight	100
Unique identifier [ke	retomeier
Network [key]	Twitter
Profile URL	http://twitter.com/retomeier

Source	RT @HeathrowAirport:... partially evacuat...	(Twit)
Transform	To Twitter Affiliation [Convert]	
Result	Reto Meier	(AffiliationTwitter)
Gen. date	2011-3-10 14:54	

Author info

Icon	
Profile	retomeier (Reto Meier)

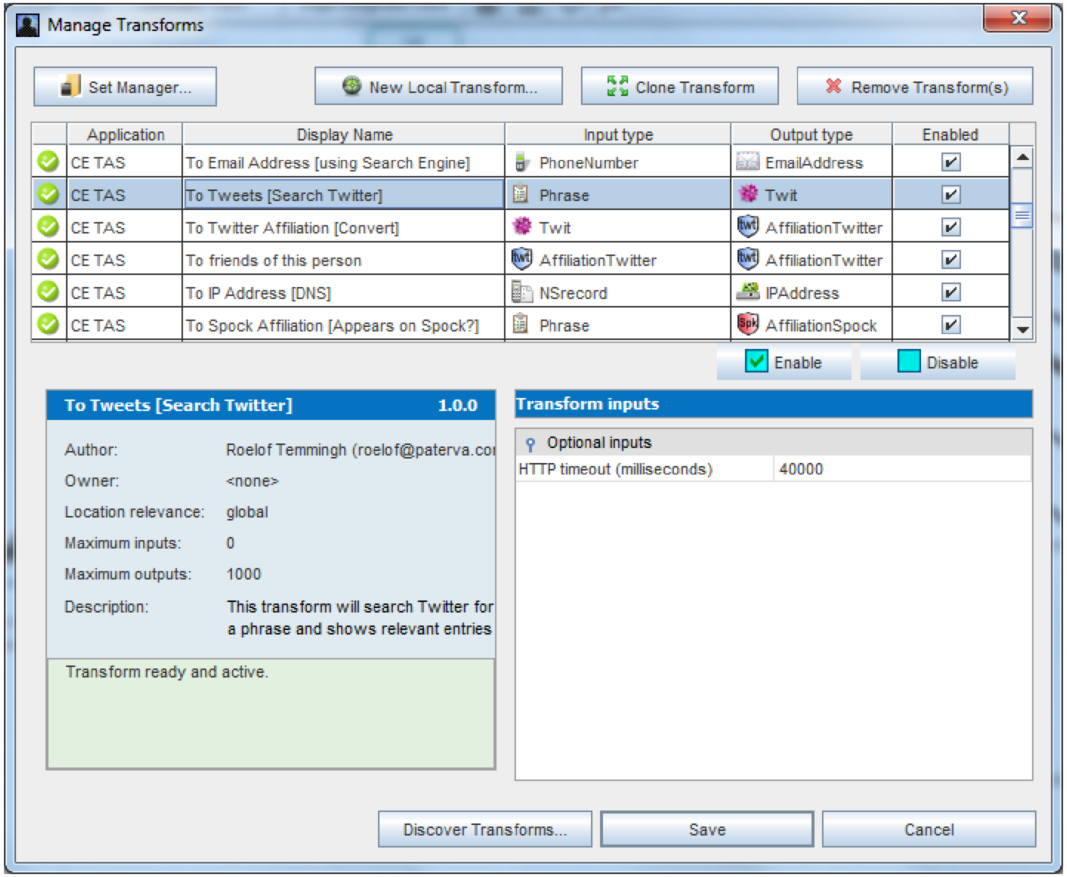
```
Transform "To URLs [show Search Engine results]" completed with 0 results
   - No URLs were found on this node...
Transform 'Mirror: External links found' cancelled by user.
Transform 'Mirror: Email addresses found' cancelled by user.
Transform "To friends of this person" completed with 12 results
```

What is Maltego?

- Maltego is an information gathering tool that allows you to visually see relationships. Maltego allows you to enumerate network and domain information like
  - Domain Names, Whois Information, DNS Names
  - Netblocks, IP Addresses
- Maltego also allows you to enumerate People information like
  - Email addresses associated with a person's name
  - Web sites associated with a person's name
  - Phone numbers associated with a person's name
  - Social groups that are associated with a person's name
  - Companies and organizations associated with a person's name
- Maltego also allows you to
  - Do simple verification of email addresses
  - Search blogs for tags and phrases
  - Identify incoming links for websites
  - Extract metadata from files from target domains

Maltego

- All the information gathering "processes" that Maltego does are called "Transforms," and unfortunately not all of them are documented. But different transforms query different types of information. The full list is here:
  - http://ctas.paterva.com/view/Category:Transforms



	Application	Display Name	Input type	Output type	Enabled
✓	CE TAS	To Email Address [using Search Engine]	PhoneNumber	EmailAddress	☑
✓	CE TAS	To Tweets [Search Twitter]	Phrase	Twit	☑
✓	CE TAS	To Twitter Affiliation [Convert]	Twit	AffiliationTwitter	☑
✓	CE TAS	To friends of this person	AffiliationTwitter	AffiliationTwitter	☑
✓	CE TAS	To IP Address [DNS]	NSrecord	IPAddress	☑
✓	CE TAS	To Spock Affiliation [Appears on Spock?]	Phrase	AffiliationSpock	☑

To Tweets [Search Twitter] 1.0.0

Author:	Roelof Temmingh (roelof@paterva.co
Owner:	<none>
Location relevance:	global
Maximum inputs:	0
Maximum outputs:	1000
Description:	This transform will search Twitter for a phrase and shows relevant entries

Transform ready and active.

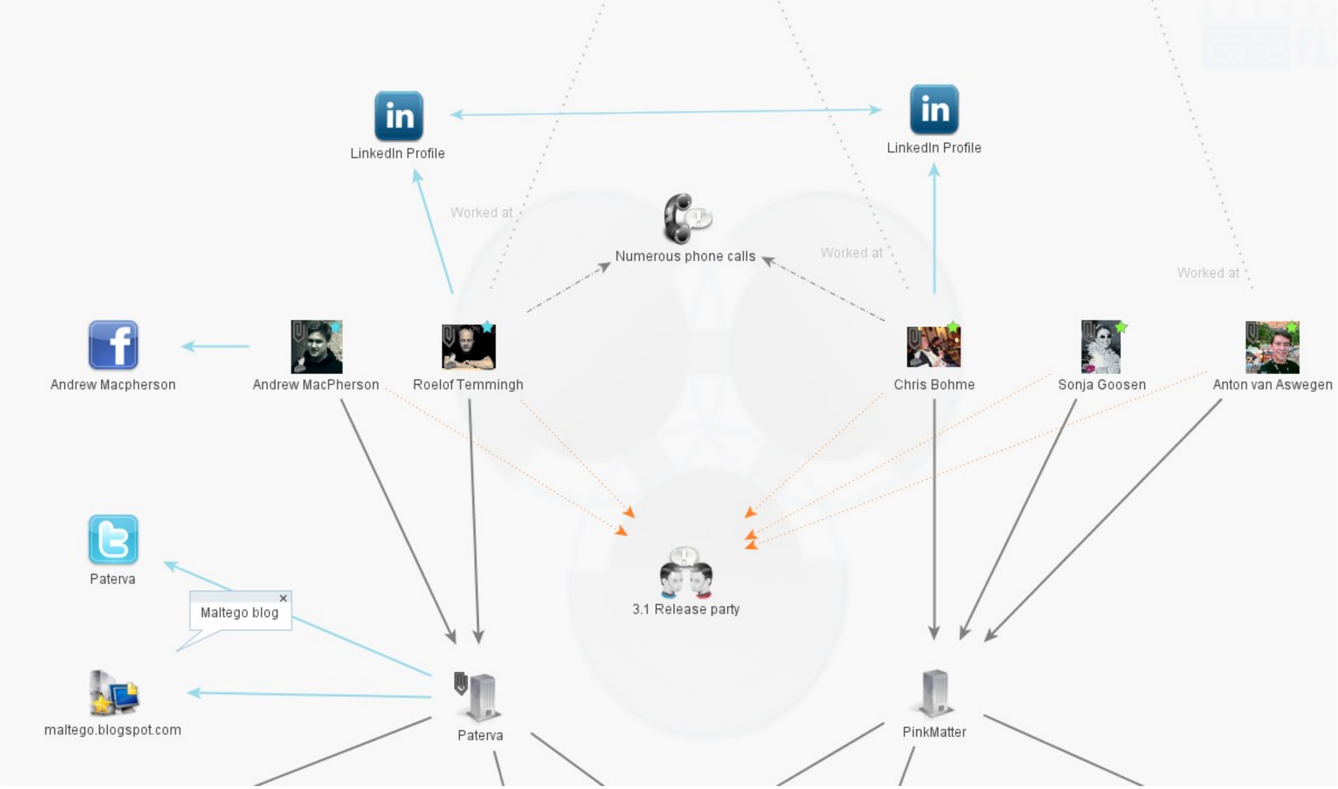
Transform inputs

Optional inputs

HTTP timeout (milliseconds)	40000

Maltego CaseFile

- Maltegos little brother which targets 'offline' analysts (manual input)
- A visual intelligence application that can be used to determine the relationships and real world links between hundreds of different types of information
- CaseFile can be used for the information gathering, analytics and intelligence phases of almost all types of investigates, from IT Security, Law enforcement and any data driven work



Paterva/Maltego resources

- Maltego Part I - Intro and Personal Recon
  - http://www.ethicalhacker.net/content/view/202/24/
- Maltego Part II - Infrastructure Enumeration
  - http://www.ethicalhacker.net/content/view/251/24/
- Data Mining Tony Hawk’s Twitter Hunt with Maltego
  - http://www.securityg33k.com/blog/?p=180
- Maltego: Transform & Correlate
  - https://www.issa.org/Library/Journals/2009/December/McRee-toolsmith.pdf
- Maltego
  - **Well documented now!**
  - http://www.paterva.com

Defenses

- Policies for content of web site
- Policies for employees use of Internet, i.e. web, newsgroups, blogs, social media etc.
- Monitor whats ”out there”
- Have Google (or other search engine) remove certain info (not index or cache it) from your site
  - Add a robots.txt file in web root dir
  - Use certain meta tags that tell well behaved crawlers to not index your web page
  - Order the Google web bot crawlers to recrawl you
  - Double edged sword since it is readable
  - More info
    - http://www.robotstxt.org
    - http://www.free-seo-news.com/all-about-robots-txt.htm

Password reset/recovery with physical access in Windows

Google search “reset password windows”

12 ways how to reset the Windows administrator password – Windows 7, Vista, Windows XP

http://4sysops.com/archives/three-ways-to-reset-a-windows-vista-admin-password/

Forgot your Windows NT/2k/XP/Vista/Win7 admin password?

http://pogostick.net/~pnh/ntpasswd/

I Forgot My Administrator Password!

http://pubs.logicalexpressions.com/Pub0009/LPMArticle.asp?ID=305