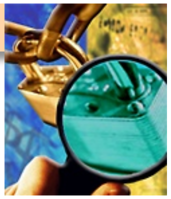
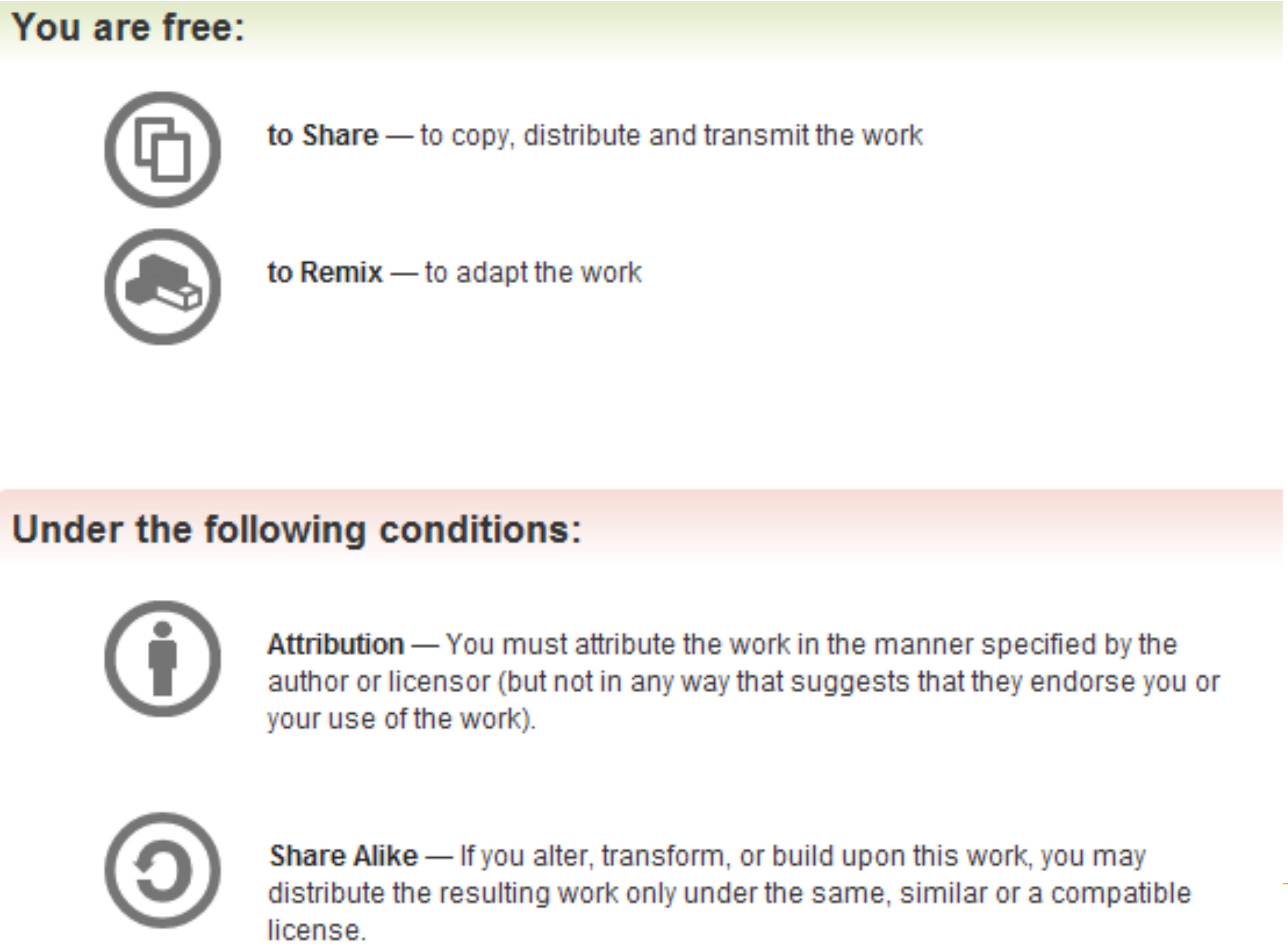
Windows Assessment

Vulnerability Assessment Course



All materials are licensed under a Creative Commons “Share Alike” license.

- http://creativecommons.org/licenses/by-sa/3.0/



You are free:

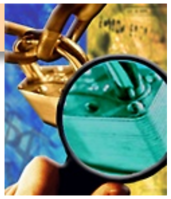
to Share — to copy, distribute and transmit the work

to Remix — to adapt the work

Under the following conditions:

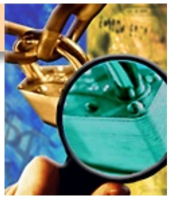
Attribution — You must attribute the work in the manner specified by the author or licensor (but not in any way that suggests that they endorse you or your use of the work).

Share Alike — If you alter, transform, or build upon this work, you may distribute the resulting work only under the same, similar or a compatible license.



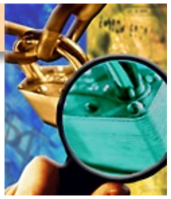
Agenda

- Windows Security Overview
- Active Directory
- Computers and Their Role in the Network
- Built-in tools
- Exercise
- Sources of secure configuration information
- Analysis Tools
- Secure Host Configuration
- Other Sources of Vulnerabilities



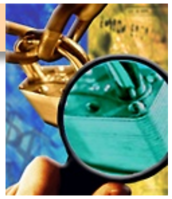
Windows Security Overview

- Local Security Authority (LSA)
- Security Account Manager (SAM)
- Security Reference Monitor (SRM)



SAM and Active Directory

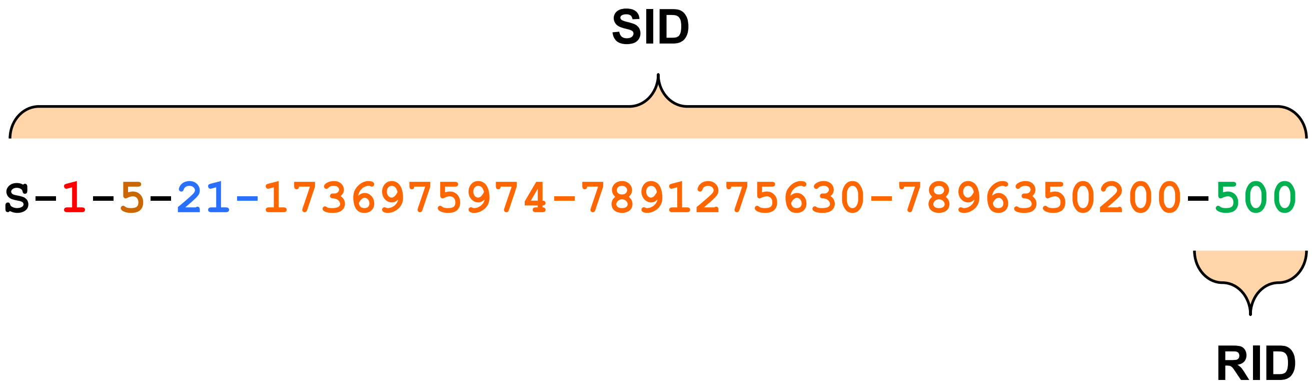
- On Windows 2K, 2K3, and 2K8 Domain Controllers the user account and hashes are stored in Active Directory
  - Uses Kerberos for authentication
- In Windows NT/2K-2K8/XP/Vista/Windows 7 non-domain hosts all user names and hashes are kept in the SAM
  - Early versions of Windows (pre-NT) have LAN Manager (NLM) Hash weaknesses that make password retrieval trivial
  - Legacy protocol support for backward compatibility in later versions of Windows
  - New Technology (NT) LM Hash version 2 in NT 4 Service Pack 4
  - NTLM does not support any federal compliant cryptographic methods (AES or SHA-256)
  - NTLM still widely used for non-AD networks
  - As of Windows Vista, the protocol is disabled by default



Security Identifiers (SIDs)

- Used to identify a security principal or security group
- Known SIDs are generic groups or users
- Known Relative Identifiers (RIDs)

500	Administrator
501	Guest
1000	First User Created



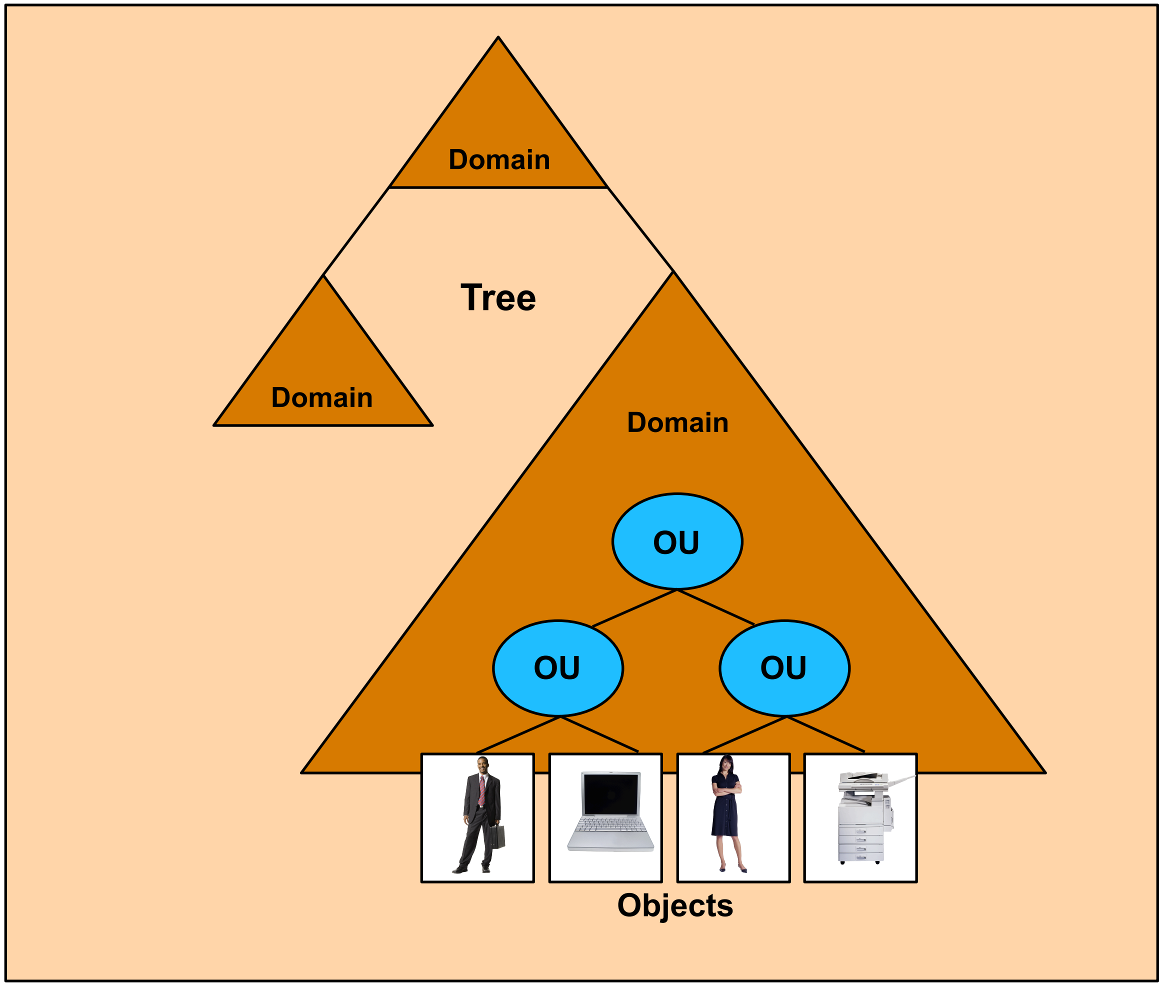
SID

S-1-5-21-1736975974-7891275630-7896350200-500

RID

Active Directory Structure

Forest



Forest

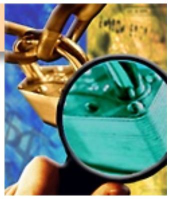
Contains domains. Used to define the scope of authority for administrators.

Domain

Contains OUs. Used to partition the directory data structure and control replication.

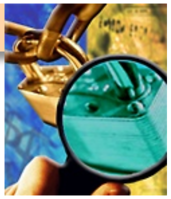
Organizational Unit (OU)

Contains users, computer accounts, and resources. Used to delegate control and apply policies.



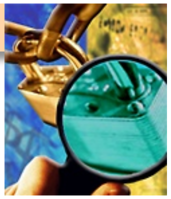
Key Active Directory Attributes

- Trusts between domains
  - NT
  - Active Directory
- Domain Name Service (DNS)
- Security group nesting strategies – AGDLP
- Local versus Group Policy



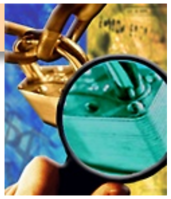
Security Features of Windows 2008 R2 and Windows 7

- More secure settings by default
- Improved User Account Control (UAC)
- Managed service accounts
  - Provides service isolation at the cost of ease of administration
- Stronger NTLM authentication
- Windows 2008 enhanced audit
  - 10 versus 9 audit categories
  - 55 granular audit settings
- Improved host-based firewall implementation



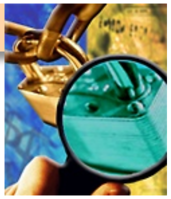
Methodology

- Phase 1 – Planning
- **Phase 2 – Information Collection**
- **Phase 3 – Enumeration**
- Phase 4 – Testing and Evaluation
- Phase 5 – Reporting



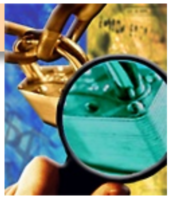
Computers and Their Roles

- Find what hosts are connected to the network and their purpose in the environment
- Examples
  - Domain Name Service (DNS)
  - Dynamic Host Control Protocol (DHCP)
  - Windows Internet Name Service (WINS)
  - Lightweight Directory Access Protocol (LDAP)
  - Domain Controllers
  - Internet Information Services (IIS)
  - Exchange
  - File and Print Services
  - Others (Certificate, SQL, SharePoint)
- Many tools needed for this are already included in your system (i.e., ‘net’ command)



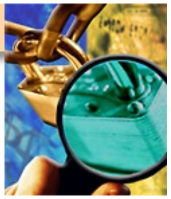
What hosts are in the domain?

- Find what domains are available on the network
  - net view /domain
- List computers in a domain
  - net view /domain:*DOMAIN-NAME*
- You can get the same information from the Windows Explorer but…



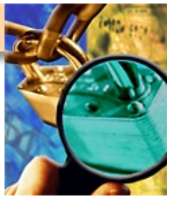
What other hosts do I know about?

- Find out which other computers and networks a computer knows about
  - nbtstat –a *Computer-Name*
  - nbtstat –A *IP-Address*
- Found on every Windows based computer
- The biggest drawbacks to nbtstat is that it operates on a single computer at a time



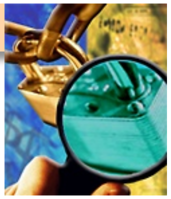
NLTEST

- A command-line utility included in the NT resource kit
- Used to test trust relationships and the state of domain controller replication
  - nltest /dclist:DOMAIN
  - nltest /whowill:DOMAIN USER
  - nltest /finduser:USER
  - nltest /server:SERVER /trusted_domains



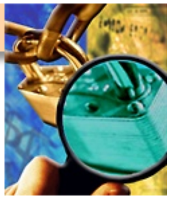
NBTSCAN

- A command-line tool that scans for open NETBIOS nameservers on a network
- Based on functionality of standard Windows tool nbtstat, but operates on a range of addresses instead of just one
  - nbtscan 10.0.0.0/24 – scan all class C network
  - nbtscan –v 10.0.0.24-35 – scan all addresses from 24-35 and displays verbose output



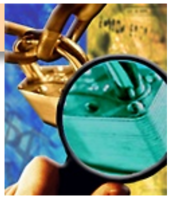
Exercise

- Identify all Windows hosts in the LAB
  - Hint: NET VIEW ?



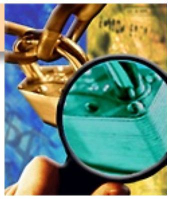
Methodology

- Phase 1 – Planning
- Phase 2 – Information Collection
- Phase 3 – Enumeration
- Phase 4 – Testing and Evaluation
- Phase 5 – Reporting



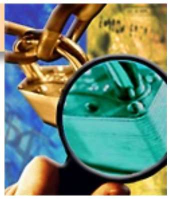
Sources of Secure Configuration Policy

- System Owner Policy
- Center for Internet Security Configuration Guides (http://www.cisecurity.com/)
- NSA's Configuration Guides (http://www.nsa.gov/snac/)
- MS Security Central (http://www.microsoft.com/security)
- MS Security Bulletin Search (http://www.microsoft.com/technet/security/current.aspx)
- BugTraq (http://www.securityfocus.com/)



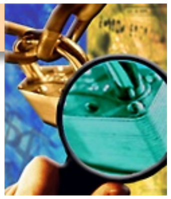
Useful Analysis Tools

- Utilities
  - WinGrep
    - http://www.wingrep.com/
  - GNU Grep for Windows
    - http://gnuwin32.sourceforge.net/packages/grep.htm
  - WinDiff Utility
    - XP CD-ROM in the Support\Tools folder
    - http://www.microsoft.com/downloads/details.aspx?familyid=3E972E9A-E08A-49A2-9D3A-C0519479E85A&displaylang=en
  - GNU DiffUtils for Windows
    - http://gnuwin32.sourceforge.net/packages/diffutils.htm
  - WinMerge
    - http://winmerge.org/downloads/
- Checklists



Secure Host Configurations

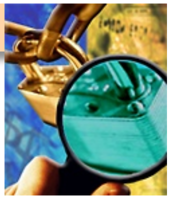
- What do we look for?
  - Service Packs, Hot Fixes, open ports, processes, IP settings, installed software
  - Disk information - using NTFS
  - Shares and permissions
  - Accounts – password settings
  - Users – Name of Administrator and Guest, password required and expiration for users
  - Groups
  - Rights
  - Registry security settings
  - Services – Host-based security applications (AV, HIDS, firewall)
  - Audit settings
  - File ACL and auditing
  - Registry ACL and auditing



Other Sources of Vulnerabilities

- Network diagrams
  - Relationship between systems and network segments
- Nessus reports
  - Scanners lie
- Interviews
  - You get to ask the admin any clarification about what you have seen
- The rest of your team

Questions



Port Scans

- Interesting Windows Ports
  - 25 SMTP
  - 20,21 FTP
  - 23 TELNET
  - 53 DNS
  - 80, 8080, 8088 HTTP
  - 88 Kerberos
  - 135 RPC/DCE Endpoint mapper
  - 137 NetBIOS Name Service
  - 138 NetBIOS Datagram Service
  - 139 NetBIOS Session Service (SMB/CIFS over NetBIOS)
  - 161 SNMP
  - 389 LDAP
  - 443 HTTPS
  - 445 Direct Host
  - 464 Kerberos kpasswd
  - 500 Inet Key Exch, IKE (IPSec)
  - 593 HTTP RPC Endpoint Mapper
  - 636 LDAP over SSL/TLS
  - 1433 MS-SQL Server
  - 1434 MS-SQL Monitor
  - 3268 AD Global Catalog
  - 3269 AD Global Catalog over SSL
  - 3389 Windows Terminal Server
  - 1243, 6711, 6776, 1349, 12345, 12346, 31337 – Trojan Ports *