Cybersecurity

Linde Nouwen

KdG Karel de Grote Hogeschool

CyberSecurity Enumeration

KdG Karel de Grote Hogeschool

Enumeration

- Part of “scanning”
- •=Gathering more information about the target system, usually already exploiting a known weakness
- •= “Digging deeper”
- Before real “exploitation”

Enumeration

- Connection needed
- Higher risk of detection
- Legal Issue = real access to system!
  - –GET PERMISSION!

Enumeration

- Extra information:
  - Machine names
  - User or Group names
  - Shares (Network resources)
  - Applications or services (daemons)
  - Network info:
    - Routing tables
    - SNMP information
    - More DNS details

Enumeration

Windows Basics:

Users/Groups/Machines & SIDs

Enumeration

- Windows: Accounts (Machine & Domain)
  - User Accounts = define access
    - Default user accounts (on almost all systems):
      - Guest
      - Administrator
        - » Disabled by default (other account needed = active)
        - » Can't be deleted. Can't be locked out. Can be renamed.
        - » No restriction (full control + can take ownership of everything)
        - » "elevated permissions"
      - More exist…

https://docs.microsoft.com/en-us/windows/security/identity-protection/access-control/local-accounts#sec-default-accounts

- Default built-in system accounts (used by processes)
  - Local Service (used by service control manager, extensive permissions, acts as computer on the network)
  - Network Service (used by SCM = present computer credentials to remote servers)
  - System (used by OS and Windows Systems)

https://docs.microsoft.com/en-us/windows/security/identity-protection/access-control/local-accounts#sec-localsystem

Account lijsten zijn per OS en type te bekijken!!!

Enumeration

- Windows: Groups (Machine & Domain)
  - (Domain) **Local** groups = give permissions and contain global groups
  - Domain **Global** groups = organize users
  - Domain **Universal** groups = organize users or global groups and can be placed in domain local groups or domain universal groups over domain boundaries (if trusts exists)

Enumeration

- Windows: Predefined Groups (Machine & Domain)
  - Predefined Local Groups
  - Predefined Domain accounts
  - Predefined Domain Local Groups
  - Predefined Domain Global Groups

→All come with specific permissions.

→Too big to list them all (google)

Enumeration

- Windows
  - Computers
    - Also have accounts
    - Can be part of groups

Enumeration

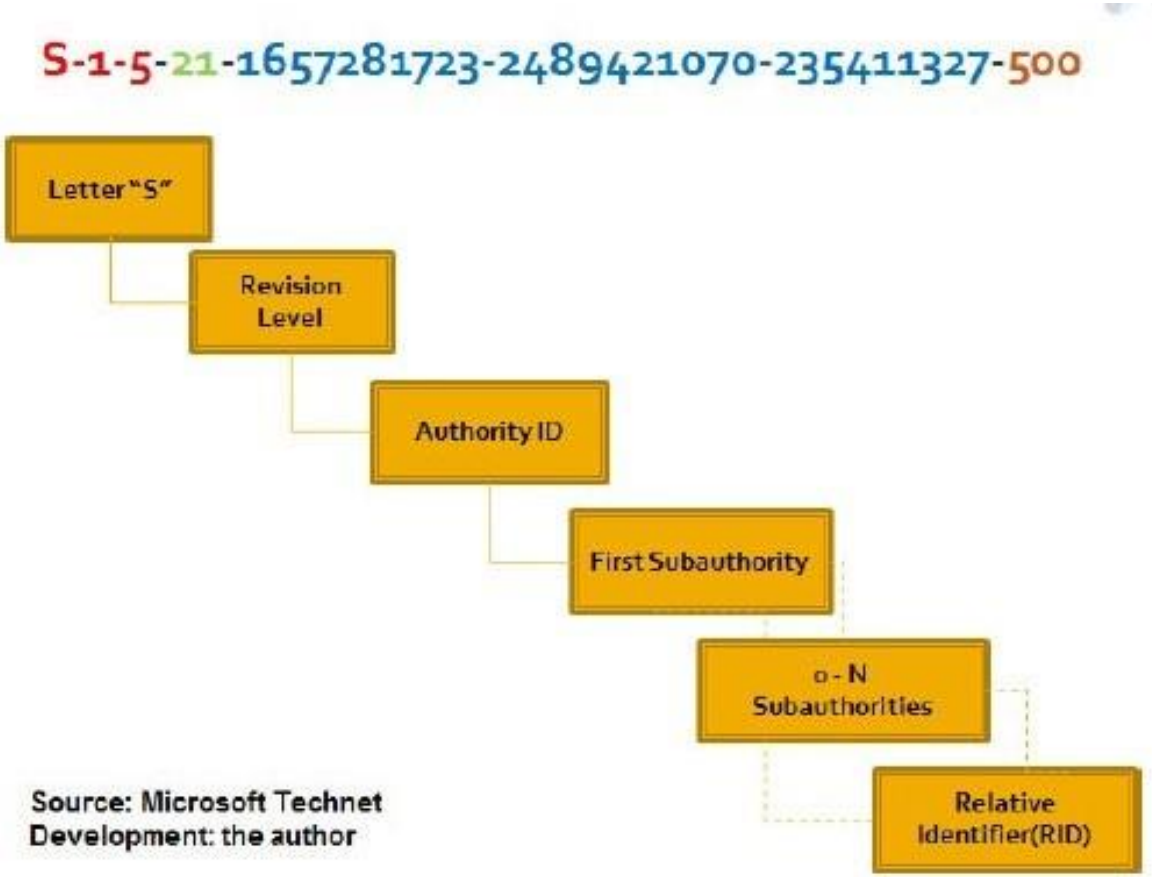
- Windows under the bonnet:
  - Users, Groups, Computers have a:
    - SID (Security Identifier)
      - Unique (User Account); Not Unique (built-in accounts)
      - Assigned by an authority (DC)
      - Variable length
      - S-1-5: universal start
      - Used in:
        - Security descriptors (owner/primary group of object)
        - ACLs (who can access)
        - Access Tokens (Identify user & his/her groups)
      - Creation: S+R+48-bit = authority issued SID + 32-bit = subauthority & RID

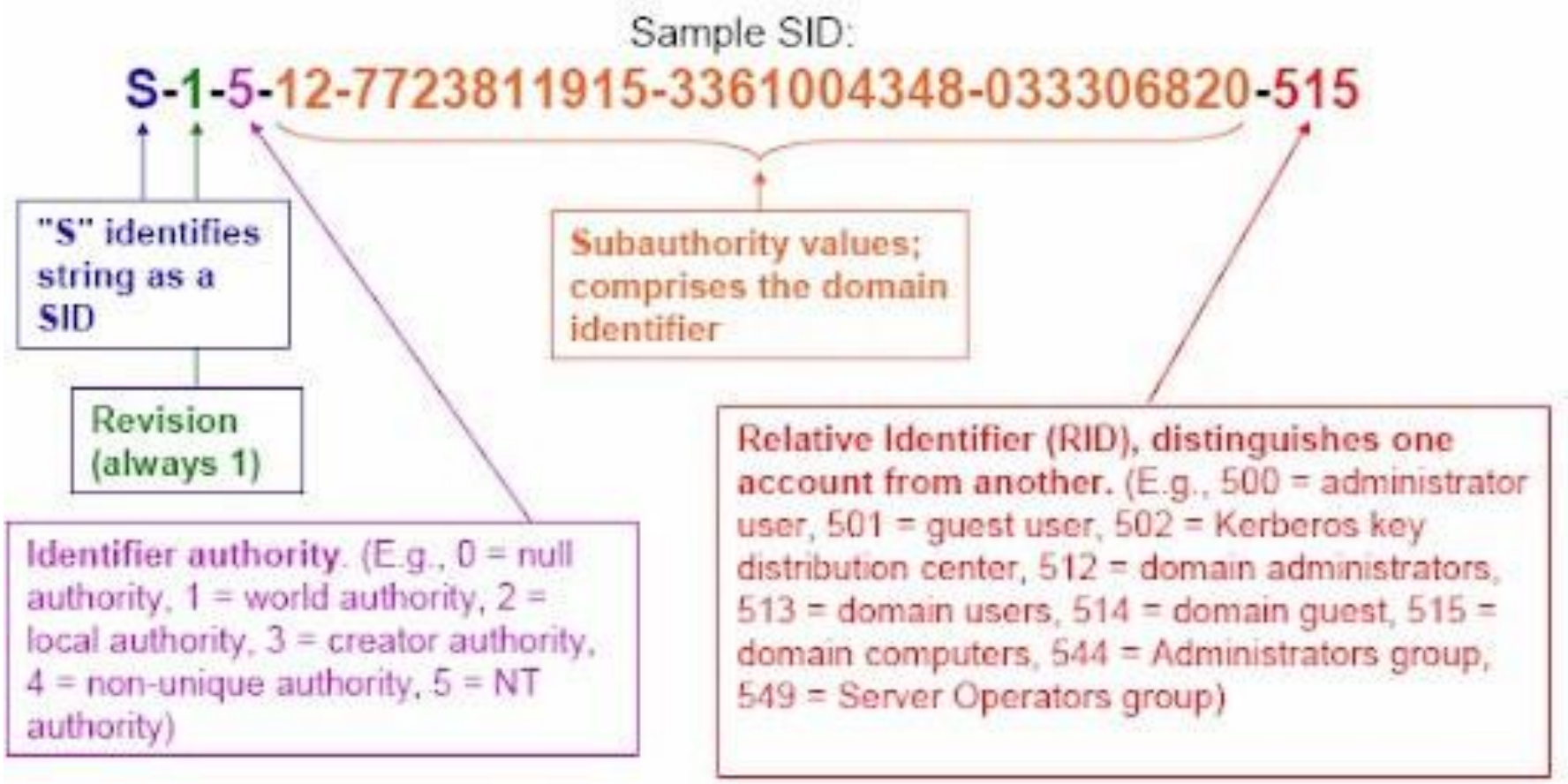
Enumeration

- SID-structure:
  - S-R-X-Y^1-Y^2...-Yn-1 – Yn
    - S -- The string is a SID.
    - R -- The revision level.
    - X -- The identifier authority value.
    - Y^1-Yn-1 -- The series of subauthority values that make up the domain identifier. For all SIDs issued by the same security authority, all the values in this field are the same. On the flip side, the domain identifier differentiates SIDs issued by different domains in your enterprise because no two domains share the same domain identifier.
    - Yn; -- The RID. Remember that this value is what distinguishes one account or security group from all the others issued by the same security authority.
      - the static RID for the Administrators group is always 544
      - the RID for the Everyone group is actually NULL.

Enumeration

- Windows
  - SID (Security Identifier)
  - Structure:




Sample SID:
S-1-5-12-7723811915-3361004348-033306820-515
"S" identifies string as a SID
Revision (always 1)
Identifier authority. (E.g., 0 = null authority, 1 = world authority, 2 = local authority, 3 = creator authority, 4 = non-unique authority, 5 = NT authority)
Subauthority values; comprises the domain identifier
Relative Identifier (RID), distinguishes one account from another. (E.g., 500 = administrator user, 501 = guest user, 502 = Kerberos key distribution center, 512 = domain administrators, 513 = domain users, 514 = domain guest, 515 = domain computers, 544 = Administrators group, 549 = Server Operators group)

Enumeration

- Windows
  - SID (Security Identifier)
  - Details (check web):

Authority ID	Description
0	SECURITY_NULL_SID_AUTHORITY. Used to perform comparisons when the authority ID is unknown.
1	SECURITY_WORLD_SID_AUTHORITY Used to construct SIDs that represent all users.
2	SECURITY_LOCAL_SID_AUTHORITY Used to create SIDs that represent users that login to a local console.
3	SECURITY_CREATOR_SID_AUTHORITY Used to create SIDs that indicate the creator or owner of an object.
5	SECURITY_NT_AUTHORITY Represents the operating system.

Source: Microsoft Technet
Development: the author

Table 6 - Sub-authorities

Sub-Authority ID	Description
5	Used to apply permissions for applications that run under a specific session.
6	Used when a process authenticates as a service.
21	Specifies computer and users SIDs that are not universally unique, it means with local significance.
32	Identifies built-in SIDs.
80	Used to identify services' SIDs.

Source: Microsoft Technet
Development: the author

Table 7 - Well known RIDs

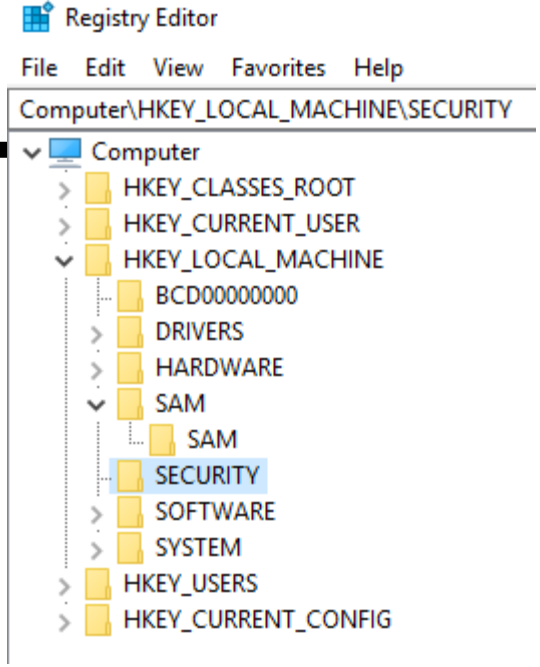
RID	Description
500	Administrator
501	Guest
502	Kerberos
512	Domain Admins

Source: Microsoft Technet
Development: the author

Enumeration

- Well-known SIDs:
  - Guest: ends in 501
  - Administrator: ends in 500
  - S-1-5-18: LocalSystem account
  - S-1-0-0 (Null SID)—This is assigned when the SID value is unknown or for a group without any members.
  - S-1-1-0 (World)—This is a group consisting of every user.
  - S-1-2-0 (Local)—This SID is assigned to users who log on to a local terminal.

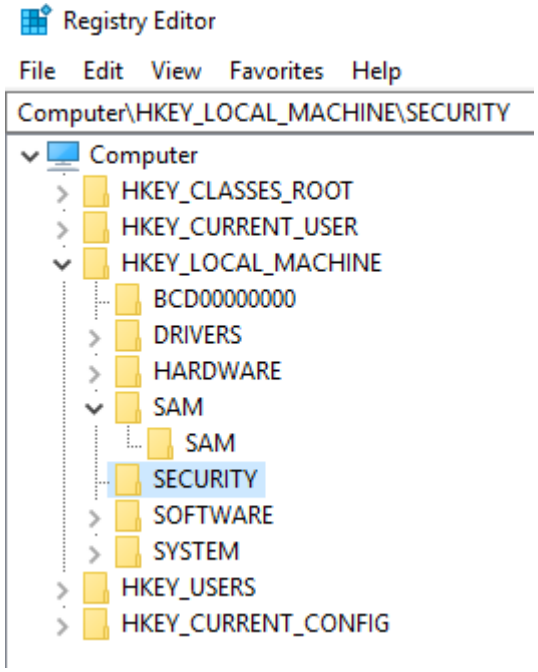
Enumeration



- Windows Security Databases
  - Local
    - SAM (Security Accounts Manager)
      - Database
      - Contains SIDs
      - Part of Windows Registry (\windows\system32\config)
      - UserAccount
        - Info
        - One info = PW (Encrypted hash)
  - Domain (on Domain Controllers)
    - Active Directory
      - Database
      - Contains objects
      - LDAP compatible

Enumeration

- Windows Security Databases
  - Local: SAM



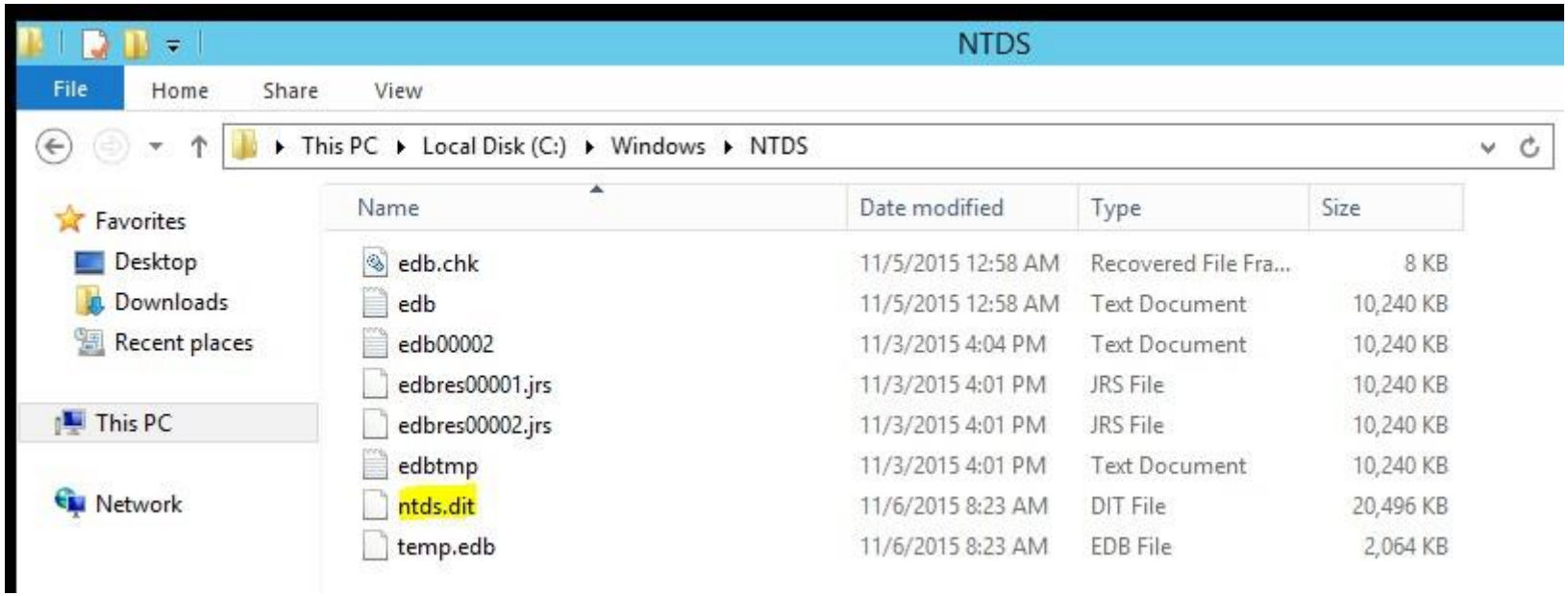

```
C:\Windows\System32\config>dir
 Volume in drive C is Windows
 Volume Serial Number is 6E41-EA45

 Directory of C:\Windows\System32\config

24/09/2019  12:39    <DIR>          .
24/09/2019  12:39    <DIR>          ..
24/09/2019  12:35           524 288 BBI
20/09/2018  12:01    <DIR>          bbimigrate
20/09/2018  12:03            28 672 BCD-Template
24/09/2019  12:39        59 768 832 COMPONENTS
24/09/2019  12:35         1 310 720 DEFAULT
24/09/2019  10:01         6 230 016 DRIVERS
23/09/2019  08:31           131 072 ELAM
29/09/2017  15:46    <DIR>          Journal
24/09/2019  09:26               336 netlogon.ftl
23/09/2019  08:41    <DIR>          RegBack
20/09/2018  12:01            73 728 SAM
24/09/2019  12:35            65 536 SECURITY
24/09/2019  12:35       172 752 896 SOFTWARE
24/09/2019  12:35        26 738 688 SYSTEM
29/09/2017  15:46    <DIR>          systemprofile
29/09/2017  15:46    <DIR>          TxR
20/09/2018  10:38             8 192 userdiff
29/09/2017  15:44             4 096 VSMIDK
              13 File(s)    267 637 072 bytes
               7 Dir(s)  24 139 902 976 bytes free
```

Enumeration

- Windows Security Databases
  - Domain: ntds.dit



Enumeration

Windows Basics:

Null-Sessions

Prevention

Enumeration

- Windows
  - Note: null sessions were created (in earlier versions of Windows) to create trust relationships between domains. Null sessions allowed…:
    - For the SYSTEM account to be authenticated to list system resources.
    - For trusted domains to enumerate resources.
    - For non-domain computers to authenticate and enumerate users.
  - Since Windows Vista & 2008: security settings were “hardened”.

Enumeration

- Windows
  - Netbios (CIFS/SMB) weakness: possibility to create "null sessions"
    - Connection to \\IP or Name\ipc$ without user/pw.
      - \\192.168.1.60\ipc$
  - Ports to check for:

Service name	Port
Naming service	137 TCP/UDP
Datagram distribution (error detection and recovery)	138 UDP
Session service	139 TCP
Sharing files and printers SMB (*)	445 TCP

Note (*): In previous versions of *Windows*, SMB (Service Message Block) required to be transported over NetBT (NetBIOS over TCP / IP), but now it does it directly on TCP/IP.

Enumeration

- Windows: prevention techniques
  - Usually through registry keys (configuration settings)
  - Examples:
    - Restrict Anonymous Enumeration of SAM Accounts and Shares
      - **HKLM\SYSTEM\CurrentControlSet\Control\LSA\RestrictAnonymous**
        - 0 = None (based on default permissions)
        - 1 = Anonymous users restriction (enumeration of SAM database is not permitted)
        - 2 = No access without explicit credentials
      - **+ RestrictAnonymousSAM (Restricts SAM enumerations only, so not shares.)**

Enumeration

➢ Windows: prevention techniques

- ❖ Policies:
  - Pre-configured configuration (registry) settings to be applied to users, groups, machines etc… (GPO = group policy objects = set of policies)
  - Configure through GPMC (Group Policy Management Console)
  - Local
  - Domain

Enumeration

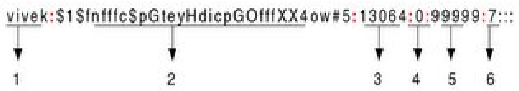
Linux Basics

Enumeration

- Linux
  - Users
    - Account to Logon
    - Properties:
      - Username and user ID (UID)
      - Password
      - Primary group name and group ID (GID)
      - Secondary group names and group IDs
      - Location of the home directory
      - Preferred shell
    - Stored in:
      - Etc/passwd (old = all info in only place, also pw)
        - » username:password:UID:GID:name:home directory:shell
      - Etc/shadow (new = pw & account-info)
        - » Username:hashtype$passwordhash:last:min:max:warn:inactive:expire
      - Both files need to be combined to get all info. Kali has "unshadow" tool.

Enumeration

/etc/shadow file fields



(Fig.01: /etc/shadow file fields)

1. **Username** : It is your login name.
2. **Password** : It is your encrypted password. The password should be minimum 8-12 characters long including special characters, digits, lower case alphabetic and more. Usually password format is set to `$id$salt$hashed`, The `$id` is the algorithm used On GNU/Linux as follows:
   1. **1** is MD5
   2. **$2a$** is Blowfish
   3. **$2y$** is Blowfish
   4. **5** is SHA-256
   5. **6** is SHA-512
3. **Last password change (lastchanged)** : Days since Jan 1, 1970 that password was last changed
4. **Minimum** : The minimum number of days required between password changes i.e. the number of days left before the user is allowed to change his/her password
5. **Maximum** : The maximum number of days the password is valid (after that user is forced to change his/her password)
6. **Warn** : The number of days before password is to expire that user is warned that his/her password must be changed
7. **Inactive** : The number of days after password expires that account is disabled
8. **Expire** : days since Jan 1, 1970 that account is disabled i.e. an absolute date specifying when the login may no longer be used.

- Linux
  - Users
    - Account to Logon
    - Properties:
      - Username and user
      - Password
      - Primary group nam
      - Secondary group na
      - Location of the hom
      - Preferred shell
    - Stored in:
      - Etc/passwd (old = a
        - » username:passwo
      - Etc/shadow (new =
        - » Username:hashtype ire
      - Both files need to b tool.

xp

"

Enumeration

Extra on UID:

- UID 0 (zero) is reserved for the root.
- UIDs 1–99 are reserved for other predefined accounts.
- UID 100–999 are reserved by system for administrative and system accounts/groups.
- UID 1000–10000 are occupied by applications account.
- UID 10000+ are used for user accounts.

Enumeration

Extra on PW:

- Administrators often use the /etc/passwd file to hold local user account information but store the encrypted password in the /etc/shadow file, which is readable only by root. When this method is used, the passwd file entry has an x in the password field.
- When the user logs in by entering a username and password, Linux takes the entered password, encrypts it, and then compares the encrypted value to the value of the password stored in the user account. If the entered value is the same as the value stored in the password field on the computer, the user is granted access.

Enumeration

Groups:

- administer and organize user accounts.
- unique name
- Unique id identification number (GID)
- user has a designated primary (or default) group and can also belong to additional groups called secondary groups.
  - Secondary groups for each user are listed as entries in /etc/group on the computer itself.
- When users create files or launch programs, those files and programs are associated with one group as the owner. A user can access files and programs if they are a member of the group with permissions to allow access. The group can be the user's primary group or any of their secondary groups.
- all user accounts that are part of the group receive the group's rights and permissions.
- the primary GID and group name are stored as entries in the /etc/passwd file on the computer itself.

Enumeration

Groups:

- Extra:
  - GID 0 (zero) is reserved for the root group.
  - GID 1–99 are reserved for the system and application use.
  - GID 100+ allocated for the user's group.

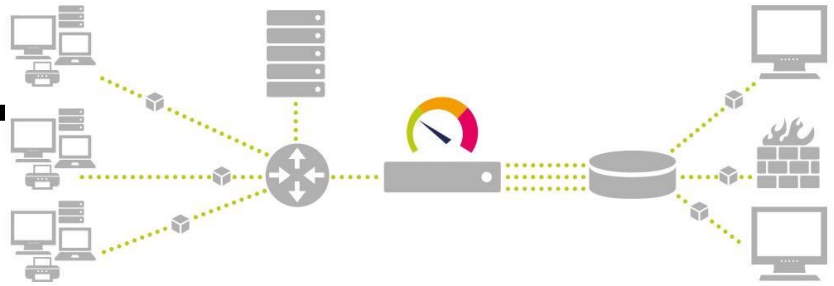
Enumeration

Network Enumeration

Enumeration

- DNS
  - DNS transfer
    - Nslookup (ls –d)
    - Dig (axfr)
- Routing information
  - Switch protocols: CDP (and LLDP)
  - Routing protocols: OSPF, EIGRP, …
    - Neighbour info

Enumeration

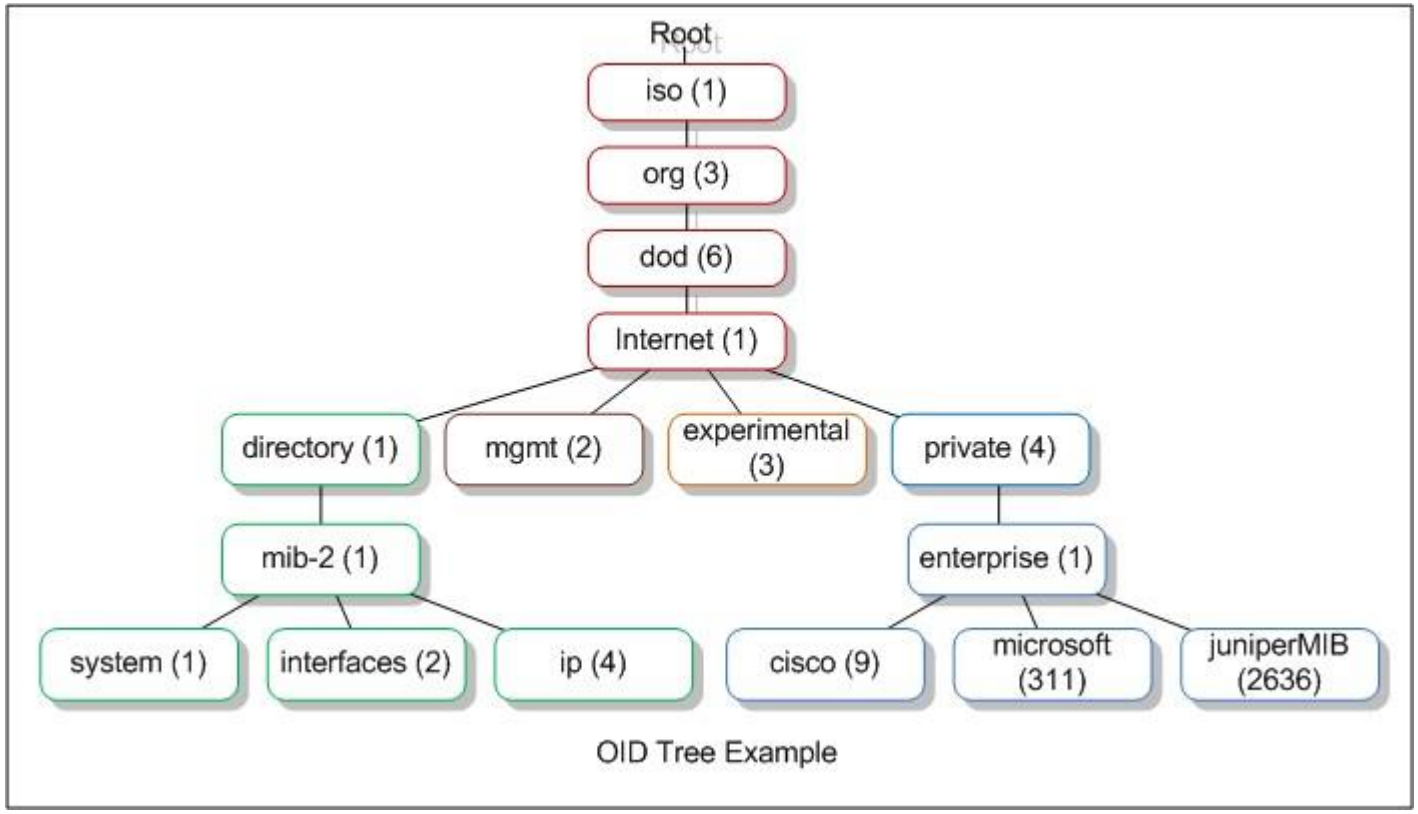


➢ SNMP

- ❖ Network monitoring (UDP or TCP)
- ❖ Port 161 (agent) , 162 (manager)
- ❖ Community (public) Note: v2
- ❖ Operations: Get, GetNext, Set, Trap
- ❖ MIB = Management Information Base
  - Hiërarchically organized information
  - Vendor provides product-database
- ❖ OID = Object Identifier
  - ID of object in a MIB
  - OID repositories = provided by manufacturer
- ❖ Example:
  - 1.3.6.1.4.868.2.4.1.2.1.1.1.3.3562.3
  - Iso(1).org(3).dod(6).internet(1).private(4).transition(868).products(2).chassis(4).card(1).slotCps(2)-cpsSlotSummary(1).cpsModuleTable(1).cpsModuleEntry(1).cpsModuleModel(3).3562.3

Enumeration

- SNMP



Enumeration

- SNMPv1
  - Community
    - default “public”
    - sent in clear text
  - Counters
    - Only 32 bit

Enumeration

- SNMPv2
  - **SNMPv2c**,SNMPv2u, SNMPv2
  - Counters
    - 64 bit
  - New Commands
    - GetBulk
    - Inform (=traps + confirm of manager)
  - More Security
    - Same “community” security as v1
    - No encryption
    - ACLs needed

Enumeration

- SNMPv3
  - Security
    - Authentication
    - Encryption
    - Extra elements
      - SNMP View
        - Restrict view of information a user can access per group
      - SNMP Groups
        - Defines security
        - RO or RW access
      - SNMP User
        - Needs to be added to group for access
        - Username + password + authentication level + encryption
  - No manager/agent
    - SNMP Entities: SNMP Engine (agent) + multiple SNMP Applications (manager)

Enumeration

- SNMPv2 vs SNMPv3

	SNMPv2	SNMPv3
Primary Standards	RFC- 1901	RFC-3412, RFC-3414, RFC-3415, RFC-3417
Allowed Operations	Get, GetNext, Set, Trap, GetBulk, Inform, Response	Get, GetNext, Set, Trap, GetBulk, Inform, Response with PDU message format
Authentication	Community based	User & Group based
Plain text community strings	Yes	No
Data Encryption	None	DES / SHA / MD5 / AES
Device Identification	Request / response protocol	EngineID uniquely identifies each SNMP entity
MIB	Defines general framework for definition and construction of MIB	Configures permissions based on user for differing levels of MIB access
Default/known passwords	Yes	No
Data tampering protection	No	Yes
Eavesdropping protection	No	Yes
Unauthorized access protection	Limited based on locally defined ACLs	Yes
Best for	Internal networks	Public / internet-facing networks

Enumeration

Defense…

Enumeration

➢ DEFENSE:

- ❖ The only secure network is a disconnected network
  - Separate network traffic (vlans, fw, …)
  - Aren't you happy you know VLANs?
- ❖ "Harden" your systems, apps and services
  - Change default passwords
  - Disable not-used or known accounts
  - Only install needed applications
  - Enable automatic patching
  - Keep support contracts at hand
- ❖ Use an IPS
- ❖ Periodically perform your own vulnerability analysis & correct them