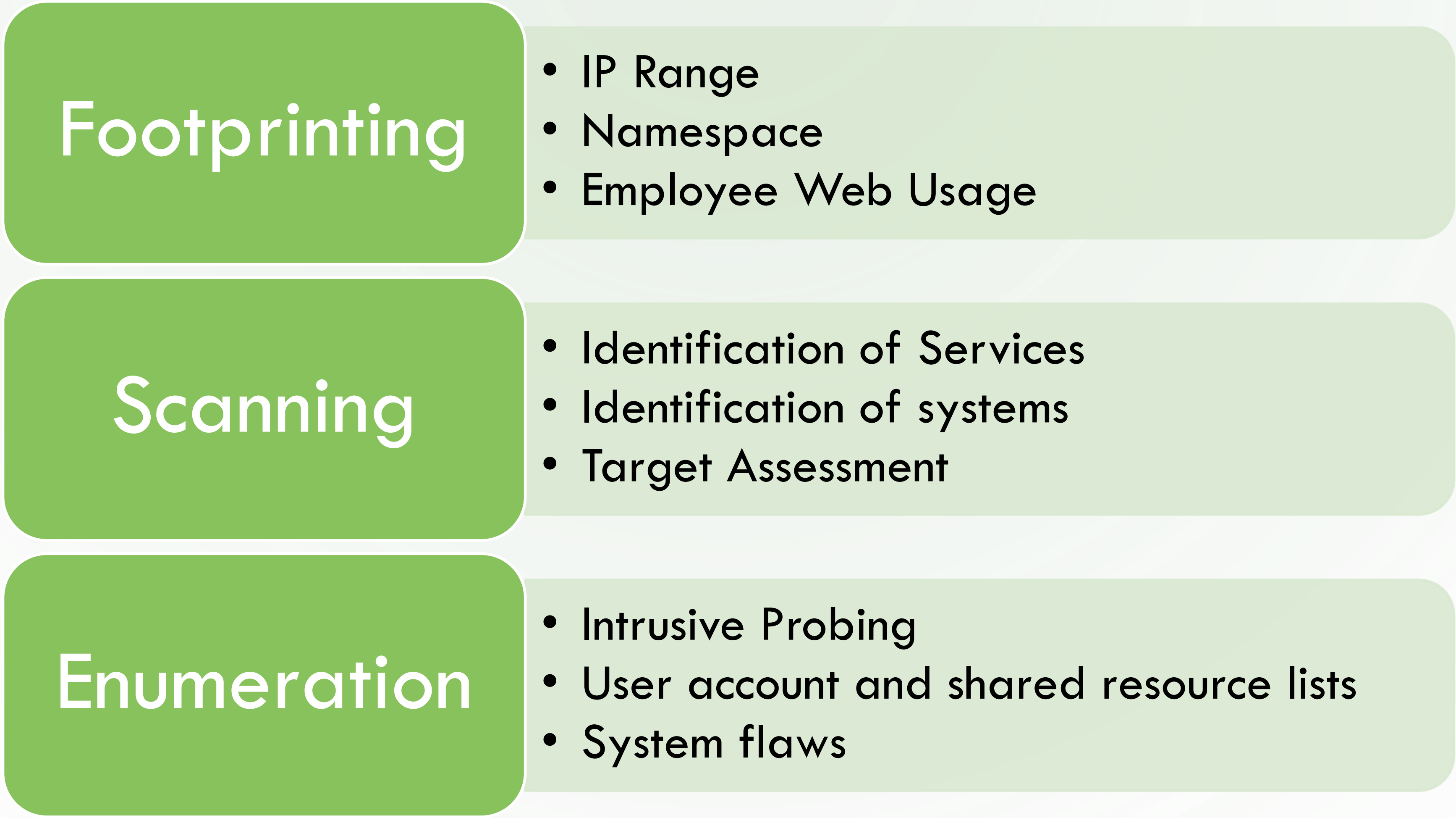
System Hacking

MODULE TOPICS

- Goals of System Hacking
- Password Cracking
  - Techniques
  - The Windows LM Hash
  - Countermeasures
- Exploiting Vulnerabilities
  - CVEs
  - Privilege Escalation

INFORMATION AT HAND AT THIS STAGE



Footprinting

- IP Range
- Namespace
- Employee Web Usage

Scanning

- Identification of Services
- Identification of systems
- Target Assessment

Enumeration

- Intrusive Probing
- User account and shared resource lists
- System flaws

GOALS OF SYSTEM HACKING

Stage	Objective	Tools / Techniques Used
Gaining Access	Collect enough information to gain access	Password eavesdropping Brute forcing
Escalating Privileges	Create a privileged user account	Password cracking Known exploits
Executing Applications	Create and maintain backdoor access	Trojans
Hiding Files	Hide malicious files	Rootkits
Clearing Tracks	Hide signs of hacking	Clearing logs

Password Cracking

PASSWORD CRACKING

- Technique to recover passwords from computer systems
- Used by attackers to gain unauthorized access to a system
- Mostly successful due to
  - Weak passwords

    "The Internet's 25 Worst Passwords 2014"
  - Default passwords

    "Cirt.net Default Password Database"

PASSWORD CRACKING TECHNIQUES

- Dictionary Attack
- Brute Force Attack
- Hybrid
- Syllabus Based Attack
- Rule Based Attack

PASSWORD CRACKING TECHNIQUES

- Dictionary attacks
  - A dictionary file (text file containing dictionary words) is loaded into a password cracking application
  - Will not work in systems that uses passphrases
  - String manipulation can improve the attack
  - Must contain a variety of dictionaries (e.g. technical, foreign language)

PASSWORD CRACKING TECHNIQUE

- Brute force attacks
  - Exhaustive search for the correct key by trying all possible combinations in the keyspace
  - Must have enough processing power
- Hybrid attack
  - Uses the dictionary attack but adding numbers or other characters
  - This is due to the fact some users just add numbers to their password when changing them

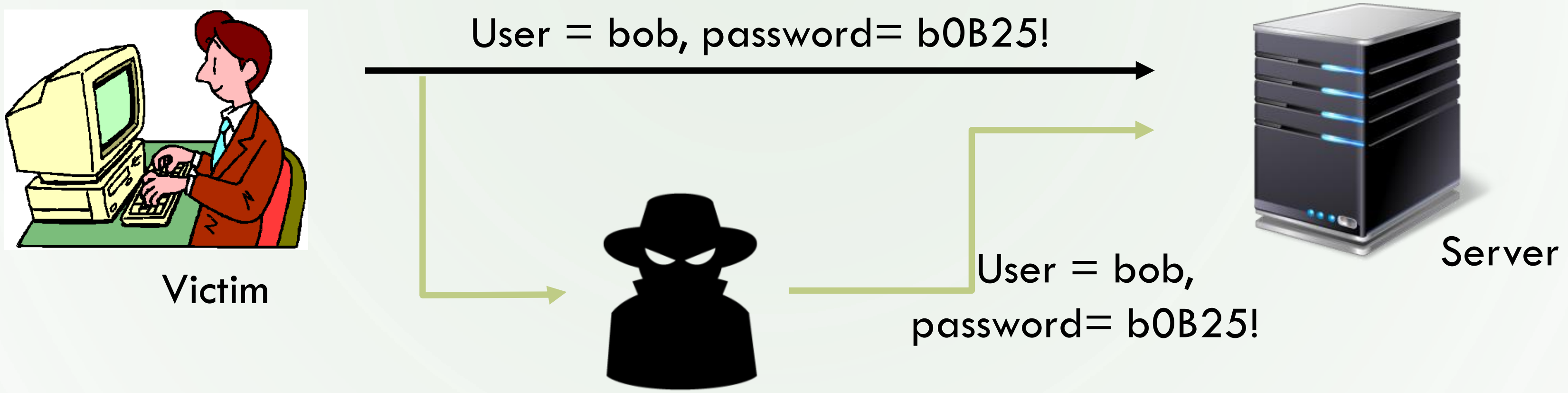
PASSWORD CRACKING TECHNIQUE

- Syllable attack
  - Combination of dictionary and brute force attack
  - For passwords that are not an existing word
  - Trying combinations of several dictionary words
- Rule-based attack
  - Requires some information / clues about the password to use specific techniques
  - Shortens cracking time
  - Combination of Dictionary, Brute Force and Syllable attack

TYPES OF PASSWORD ATTACKS

- Passive Online
  - Password hacking without communicating with the authorizing party
- Active Online
  - Try list of passwords against the victim
- Offline
  - Copy password file and attempt to crack on your own system in a different location
- Non-electronic
  - No need to possess technical knowledge

PASSIVE ONLINE ATTACK



- Monitors and collects data from the communications channel
- Relatively hard to do
- Examples: Wire sniffing, Man-in-the-middle, Replay Attacks

ACTIVE ONLINE ATTACK

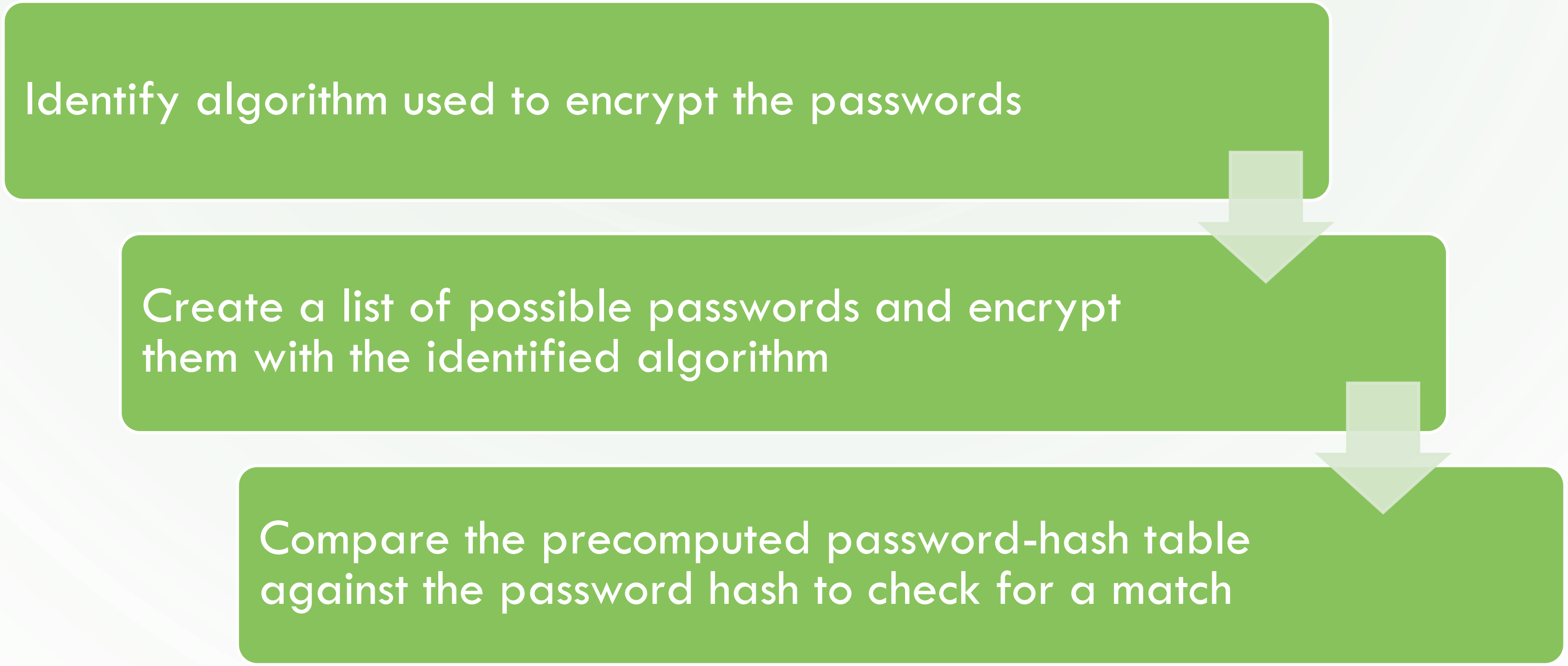
- Password Guessing
  - Time consuming and Easily detected
  - Needs bandwidth
  - Tool: hydra
- Spyware and keyloggers
  - Programs that secretly gather passwords on the victim computer
- Hash Injection
  - Hacker compromises a system and extracts password hashes
  - Hashes are used to log on to a domain controller

OFFLINE ATTACKS

- Attacker observes how passwords are stored
  - If password file is readable- easy to gain access
  - If password file contains encrypted passwords, get file and try to crack
- FYI: Some systems store *hashed* passwords
  - Hashing is a one-way encryption method
- Techniques:
  - Rainbow tables / precomputed hashes
- Tool: John The Ripper

OFFLINE ATTACK: RAINBOW TABLES

- Assumes that the hacker is able to get a copy of the hashed password



Identify algorithm used to encrypt the passwords

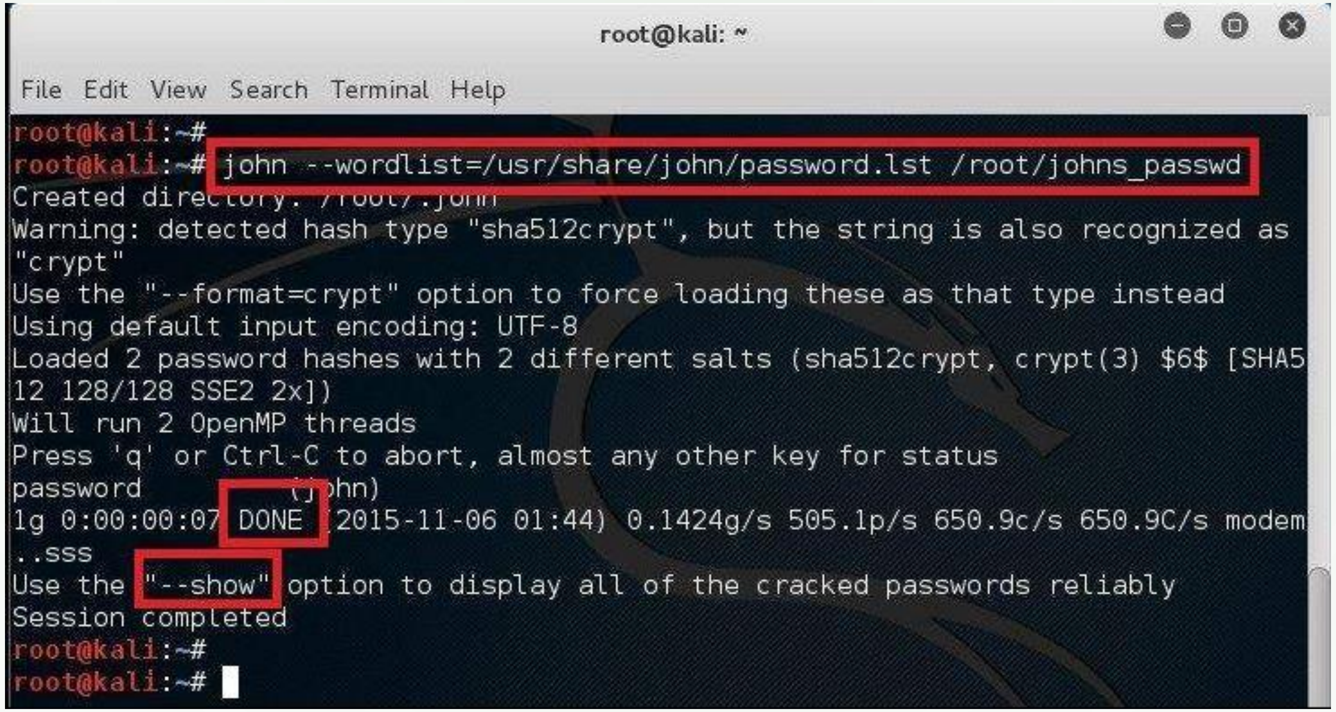
Create a list of possible passwords and encrypt them with the identified algorithm

Compare the precomputed password-hash table against the password hash to check for a match

NON-ELECTRONIC ATTACKS

- Social Engineering
  - Convince the victim to reveal their password
- Shoulder Surfing
  - Observe the victim while he/she is logging into a system
  - PINs are easiest to catch – usually 4 digits long only
- Dumpster Diving
  - Look for account creation documents, Post-It notes

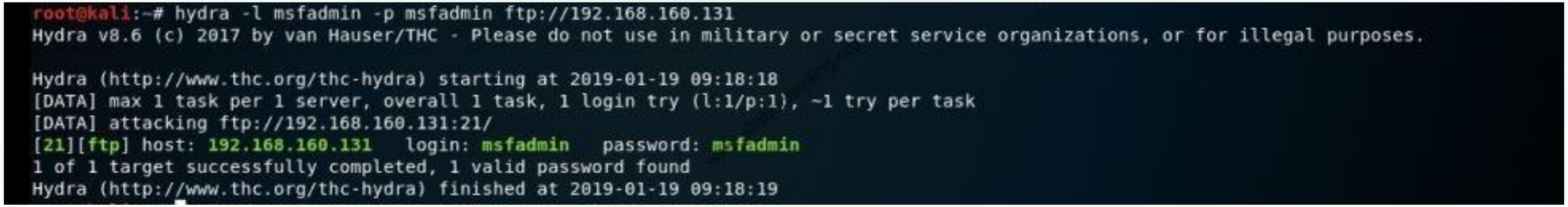
JOHN THE RIPPER



```
root@kali:~#
root@kali:~# john --wordlist=/usr/share/john/password.lst /root/johns_passwd
Created directory: /root/.john
Warning: detected hash type "sha512crypt", but the string is also recognized as
"crypt"
Use the "--format=crypt" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (sha512crypt, crypt(3) $6$ [SHA5
12 128/128 SSE2 2x])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
password         (john)
1g 0:00:00:07 DONE (2015-11-06 01:44) 0.1424g/s 505.1p/s 650.9c/s 650.9C/s modem
..sss
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@kali:~#
root@kali:~#
```

```
john --format=NT -w=/usr/share/wordlists/rockyou.txt hashfile.txt
john --format=zip hash.txt
```

HYDRA



```
root@kali:~# hydra -l msfadmin -p msfadmin ftp://192.168.160.131
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2019-01-19 09:18:18
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking ftp://192.168.160.131:21/
[21][ftp] host: 192.168.160.131   login: msfadmin   password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2019-01-19 09:18:19
```

hydra -L <username_file> -P <password_file> ftp://<Target_IP>

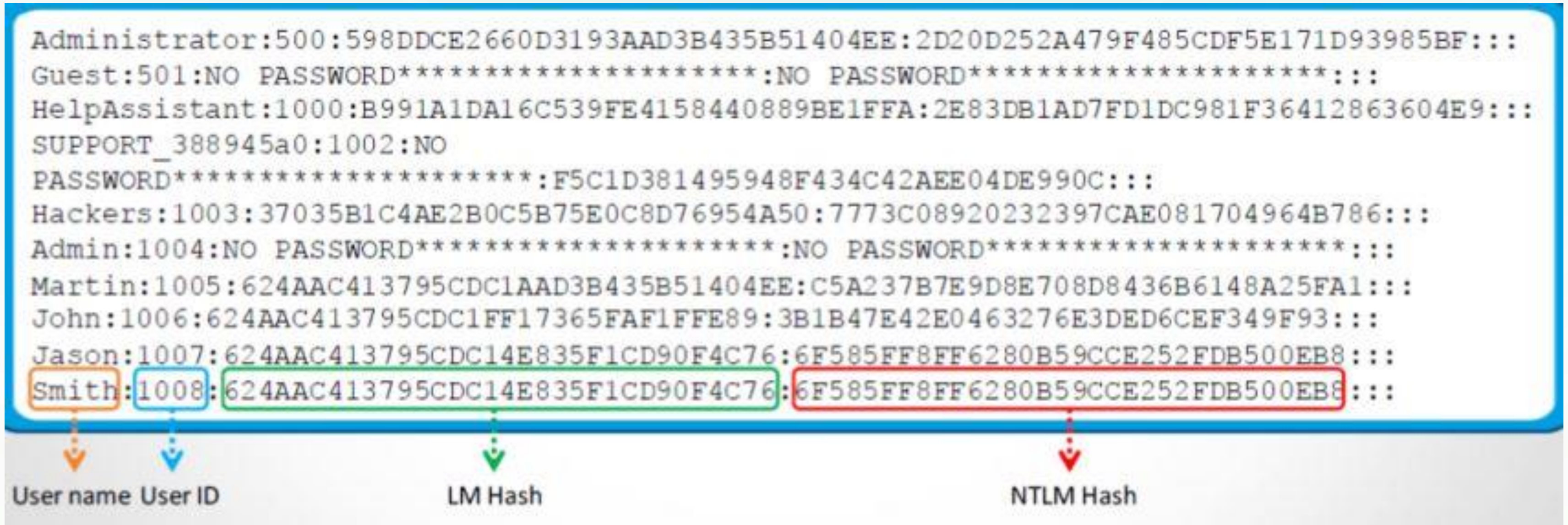
Case Study: Windows Authentication

WINDOWS AUTHENTICATION COMPONENTS

- Security Accounts Manager (SAM) Database
  - Database of hashed user passwords on a Windows system
- NTLM Authentication
  - Protocol used by Microsoft to perform challenge/ response authentication
  - Stores password in the SAM database

SAM PASSWORD STORAGE

- SAM file is located in C:\Windows\System32\config\SAM
- Normally system locked when OS is running



```
Administrator:500:598DDCE2660D3193AAD3B435B51404EE:2D20D252A479F485CDF5E171D93985BF:::
Guest:501:NO PASSWORD*********************:NO PASSWORD*********************:::
HelpAssistant:1000:B991A1DA16C539FE4158440889BE1FFA:2E83DB1AD7FD1DC981F36412863604E9:::
SUPPORT_388945a0:1002:NO
PASSWORD*********************:F5C1D381495948F434C42AEE04DE990C:::
Hackers:1003:37035B1C4AE2B0C5B75E0C8D76954A50:7773C08920232397CAE081704964B786:::
Admin:1004:NO PASSWORD*********************:NO PASSWORD*********************:::
Martin:1005:624AAC413795CDC1AAD3B435B51404EE:C5A237B7E9D8E708D8436B6148A25FA1:::
John:1006:624AAC413795CDC1FF17365FAF1FFE89:3B1B47E42E0463276E3DED6CEF349F93:::
Jason:1007:624AAC413795CDC14E835F1CD90F4C76:6F585FF8FF6280B59CCE252FDB500EB8:::
Smith:1008:624AAC413795CDC14E835F1CD90F4C76:6F585FF8FF6280B59CCE252FDB500EB8:::
```

ACCOUNT IDS

System accounts tracked by their Security IDs

Ex:

S-1-5-21-3623811015-3361044348-30300820-**1013**

- Relative ID at end of SID is recorded in the SAM file and identifies account type
  - RID = 500 is admin account
  - RID = 501 is guest
  - RID >= 1000 is a user account

LAN MANAGER (LM) HASH

- Primary hash format that Windows uses to store user passwords that are up to 14 characters in length
- Enabled by default in versions of Windows prior to Win 7.
- Newer Windows have this feature disabled by default and use a dummy value only in the SAM file

HOW IS THE LM HASH PRODUCED?

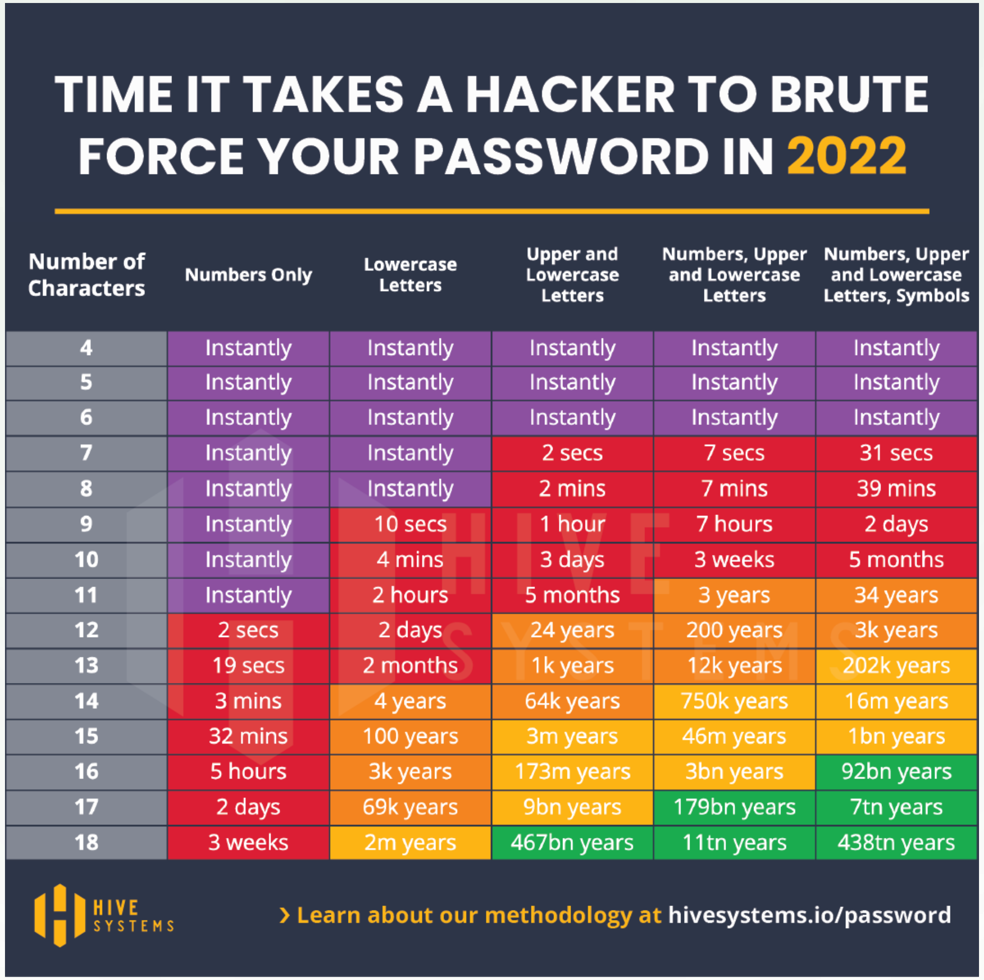
Password = 123456qwerty

1. Convert to uppercase:
    - 123456QWERTY
2. Pad null to make it 14 characters:
    - 123456QWERTY__
3. Split into two:
    - 123456Q and WERTY__
4. Get Hash Value
    - 6BF11E04AFAB197F and F1E9FFDCC75575B15
5. Concatenate the 2 hashes
    - 6BF11E04AFAB197FF1E9FFDCC75575B15

Example from CEH

PASSWORD CRACKING COUNTERMEASURES

USE Password Managers



TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2022

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years

HIVE SYSTEMS

> Learn about our methodology at hivesystems.io/password

PASSWORD CRACKING COUNTERMEASURES (CON'T)

- Follow password best practices
  - No sharing
  - Don't reuse a password when asked to change
  - Don't use dictionary words
  - Avoid unencrypted protocols
  - Don't leave system passwords at default
- Enforce account lockouts for successive wrong password attempts
- Use systems that are capable of password salting

PASSWORD SALTING

- Salting is the method of adding random characters to a password before it is hashed
- Prevents passwords from being cracked even if the password file is compromised
- Same passwords produce different hashes when done with salting
- Defeats the rainbow table technique

Linux System

LINUX PASSWORDS

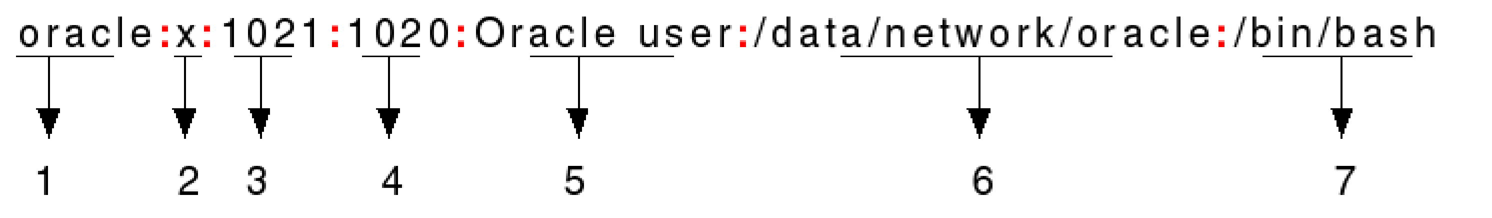
- Linux / Unix user account are stored in
  - /etc/passwd
- The hashed password is stored in
  - /etc/shadow
- Example entry
  - passwd entry

```
root:x:0:0:root:/root:/bin/bash
```

  - shadow entry

```
root:$6$yh0x1DO.$Mbaq4fbkALdEiZvzCG9pz/Rdz5sFeSCFimzyAGwKciTgUqG.6mw0SImN.H
nas8uWUkbxgboGp2RYa4ed12Ln1:16083:0:99999:7:::
```

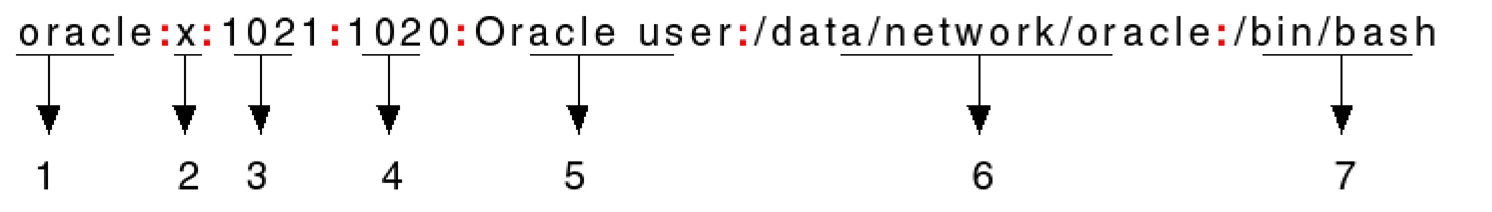
USER ACCOUNT ENTRY



```
oracle:x:1021:1020:Oracle user:/data/network/oracle:/bin/bash
```

1.Username: It is used when user logs in. It should be between 1 and 32 characters in length.
2.Password: An x character indicates that encrypted password is stored in /etc/shadow file. Please note that you need to use the passwd command to computes the hash of a password typed at the CLI or to store/update the hash of the password in /etc/shadow file.
3.User ID (UID): Each user must be assigned a user ID (UID). UID 0 (zero) is reserved for root and UIDs 1-99 are reserved for other predefined accounts. Further UID 100-999 are reserved by system for administrative and system accounts/groups.

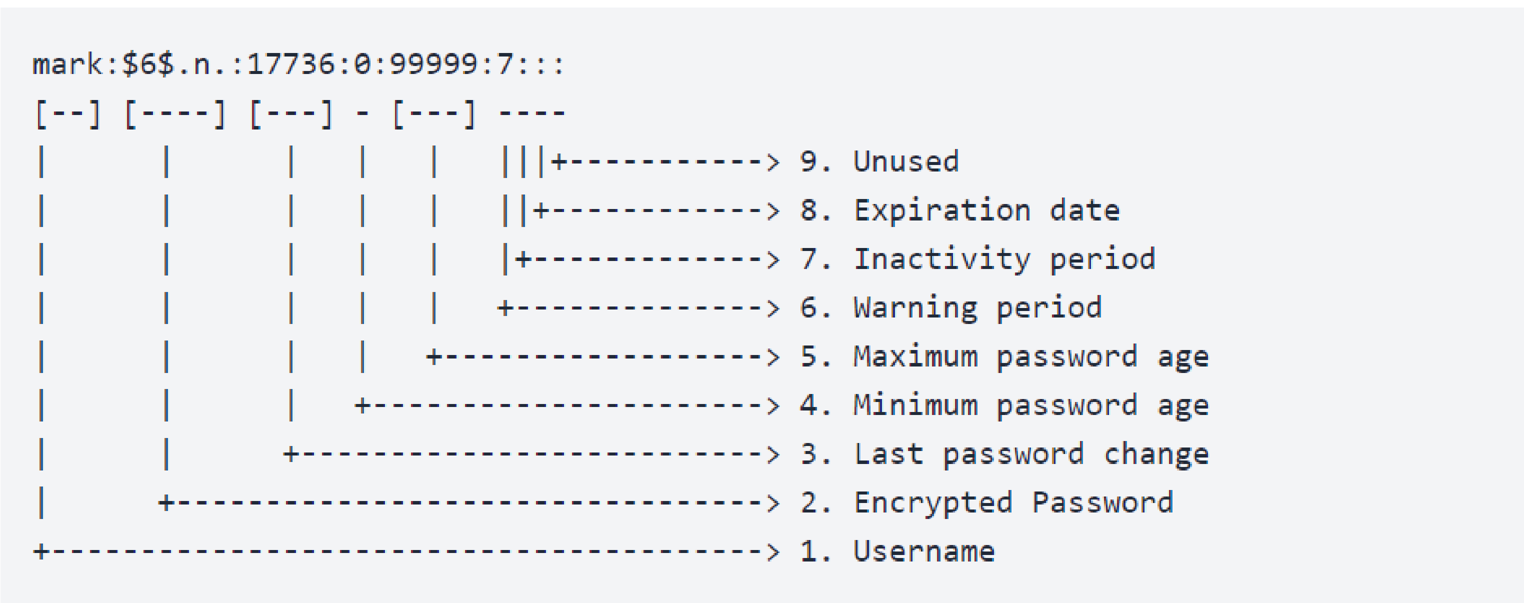
USER ACCOUNT ENTRY



```
oracle:x:1021:1020:Oracle user:/data/network/oracle:/bin/bash
```

4.Group ID (GID): The primary group ID (stored in /etc/group file)
5.User ID Info (GECOS): The comment field. It allow you to add extra information about the users such as user's full name, phone number etc. This field use by finger command.
6.Home directory: The absolute path to the directory the user will be in when they log in. If this directory does not exists then users directory becomes /
7.Command/shell: The absolute path of a command or shell (/bin/bash). Typically, this is a shell. Please note that it does not have to be a shell. For example, sysadmin can use the nologin shell, which acts as a replacement shell for the user accounts. If shell set to /sbin/nologin and the user tries to log in to the Linux system directly, the /sbin/nologin shell closes the connection.

SHADOW PASSWORD ENTRY



```
mark:$6$.n.:17736:0:99999:7:::
[--] [----] [---] - [---] ----
|      |      |   |   |   |||+-----------> 9. Unused
|      |      |   |   |   ||+------------> 8. Expiration date
|      |      |   |   |   |+-------------> 7. Inactivity period
|      |      |   |   |   +--------------> 6. Warning period
|      |      |   |   +------------------> 5. Maximum password age
|      |      |   +----------------------> 4. Minimum password age
|      |      +--------------------------> 3. Last password change
|      +---------------------------------> 2. Encrypted Password
+----------------------------------------> 1. Username
```

SHADOW PASSWORD ENTRY

1.Username. The string you type when you log into the system. The user account that exist on the system.
2.Encrypted Password. The password is using the $type$salt$hashed format. $type is the method cryptographic hash algorithm and can have the following values:

- $1$ – MD5
- $2a$ – Blowfish
- $2y$ – Eksblowfish
- $5$ – SHA-256
- $6$ – SHA-512

If the password field contains an asterisk (*) or exclamation point (!), the user will not be able to login to the system using password authentication. Other login methods like key-based authentication or switching to the user are still allowed.

In older Linux systems, the user’s encrypted password was stored in the /etc/passwd file.

3.Last password change. This is the date when the password was last changed. The number of days is counted since January 1, 1970 (epoch date).

SHADOW PASSWORD ENTRY

4.Minimum password age. The number of days that must pass before the user password can be changed. Typically it is set to zero, which means that there is no minimum password age.
5.Maximum password age. The number of days after the user password must be changed. By default, this number is set to 99999.
6.Warning period. The number of days before the password expires during which the user is warned that the password must be changed.
7.Inactivity period. The number of days after the user password expires before the user account is disabled. Typically this field is empty.
8.Expiration date. The date when the account was disabled. It is represented as an epoch date.
9.Unused. This field is ignored. It is reserved for future use.
The /etc/shadow file should not be edited by hand unless you know what you are doing. Always use a command that is designed for the purpose. For example, to change a user password, use the passwd command, and to change the password aging information, use the chage command.

Exploiting Vulnerabilities

USING VULNERABILITIES

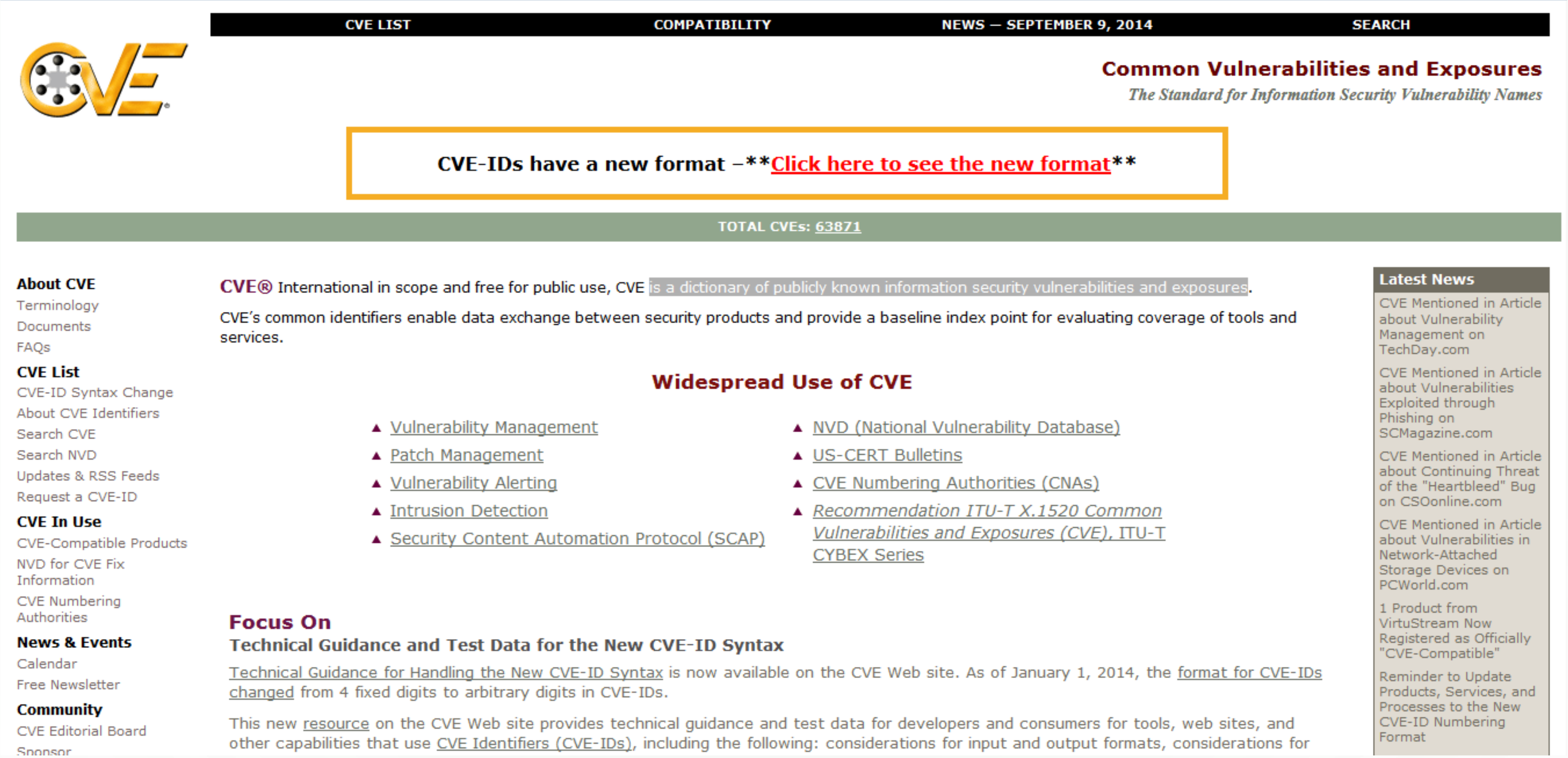
- Using information acquired through scanning and enumeration, find things to exploit. (e.g. services, software)
- Example: In windows, vulnerabilities often exist in:
  - MSRPC
  - NetBIOS + SMB
  - IIS

WHAT IS A CVE?

- Stands for Common Vulnerability and Exploit
- It also a dictionary of publicly known information security vulnerabilities and exposures
- The website https://cve.mitre.org host the list of CVEs
- CVE ID syntax

CVE prefix + Year + Arbitrary Digits

CVE WEBSITE



CVE LIST | COMPATIBILITY | NEWS — SEPTEMBER 9, 2014 | SEARCH

Common Vulnerabilities and Exposures

The Standard for Information Security Vulnerability Names

CVE-IDs have a new format –**Click here to see the new format**

TOTAL CVEs: 63871

About CVE
Terminology
Documents
FAQs

CVE List
CVE-ID Syntax Change
About CVE Identifiers
Search CVE
Search NVD
Updates & RSS Feeds
Request a CVE-ID

CVE In Use
CVE-Compatible Products
NVD for CVE Fix Information
CVE Numbering Authorities

News & Events
Calendar
Free Newsletter

Community
CVE Editorial Board
Sponsor

CVE® International in scope and free for public use, CVE is a dictionary of publicly known information security vulnerabilities and exposures.

CVE's common identifiers enable data exchange between security products and provide a baseline index point for evaluating coverage of tools and services.

Widespread Use of CVE

- Vulnerability Management
- Patch Management
- Vulnerability Alerting
- Intrusion Detection
- Security Content Automation Protocol (SCAP)
- NVD (National Vulnerability Database)
- US-CERT Bulletins
- CVE Numbering Authorities (CNAs)
- *Recommendation ITU-T X.1520 Common Vulnerabilities and Exposures (CVE)*, ITU-T CYBEX Series

Focus On

Technical Guidance and Test Data for the New CVE-ID Syntax

Technical Guidance for Handling the New CVE-ID Syntax is now available on the CVE Web site. As of January 1, 2014, the format for CVE-IDs changed from 4 fixed digits to arbitrary digits in CVE-IDs.

This new resource on the CVE Web site provides technical guidance and test data for developers and consumers for tools, web sites, and other capabilities that use CVE Identifiers (CVE-IDs), including the following: considerations for input and output formats, considerations for

Latest News

CVE Mentioned in Article about Vulnerability Management on TechDay.com

CVE Mentioned in Article about Vulnerabilities Exploited through Phishing on SCMagazine.com

CVE Mentioned in Article about Continuing Threat of the "Heartbleed" Bug on CSOonline.com

CVE Mentioned in Article about Vulnerabilities in Network-Attached Storage Devices on PCWorld.com

1 Product from VirtuStream Now Registered as Officially "CVE-Compatible"

Reminder to Update Products, Services, and Processes to the New CVE-ID Numbering Format

VULNERABILITY

- A mistake in software that can be directly used by a hacker to gain access to a system or network
- Allows an attacker to use it to violate a reasonable security policy for that system
  - Execute commands as another user
  - Access data that is contrary to the specified access restrictions for that data
  - Pose as another entity
  - Conduct a denial of service

https://cve.mitre.org/about/terminology.html

EXPOSURE

- A system configuration issue or a mistake in software that allows access to information or capabilities that can be used by a hacker as a stepping-stone into a system or network
- Does not directly allow compromise but could be an important component of a successful attack
  - Allows information gathering activities
  - Allows hiding activities
  - Primary point of entry that an attacker may attempt to use to gain access to the system or data
  - Is considered a problem according to some reasonable security policy

https://cve.mitre.org/about/terminology.html

WHERE TO USE CVES?

- Vulnerability Management
- Patch Management
- Vulnerability Alerting
- Intrusion Detection
- Security Content Automation Protocol
- National Vulnerability Database
- US-CERT Bulletins
- CVE Numbering Authorities

Privilege Escalation

PRIVILEGE ESCALATION

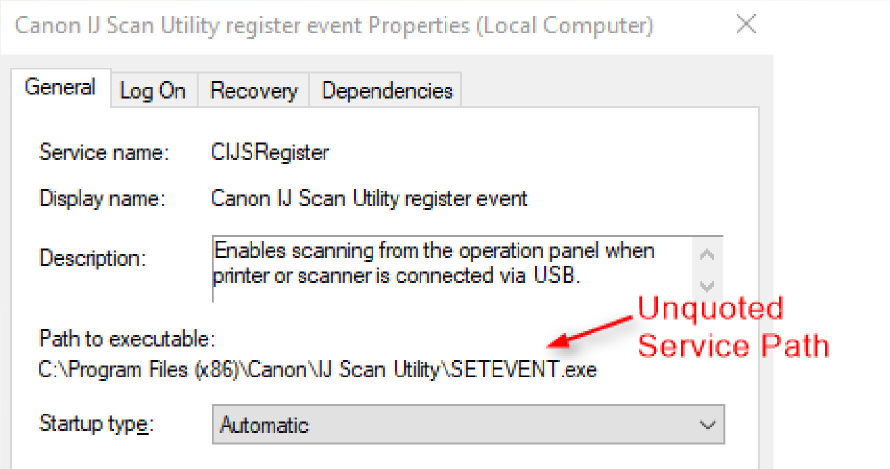
- Attacker can gain access to using a non-admin account
- Need to gain privileges of another account to execute programs or access files
- Types of escalation
  - Vertical – Get higher level access (e.g. admin)
  - Horizontal – Assume identity of another user with similar privileges

PRIVILEGE ESCALATION TASKS

- Assuming you gain access as an unprivileged account
  - Reset passwords of other accounts
  - Steal the SAM file (if you can) and crack password hashes

UNQUOTED SERVICE PATHS

- With Unquoted Service Paths vulnerabilities, we're able to abuse the way that Windows searches for executables belonging to a service.
- In many cases, we can abuse this "search order" to obtain persistence to a system as the currently logged-on user, or escalate our privileges to SYSTEM.
- The issue arises when a Windows service has been configured with a **path** to a service binary **which is unquoted**, and additionally, contains spaces in its path.



Canon IJ Scan Utility register event Properties (Local Computer)

Service name: CIJSRegister

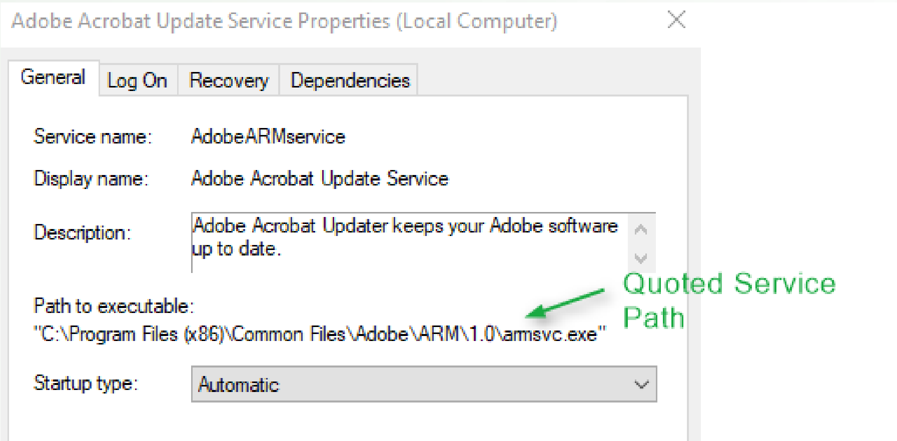
Display name: Canon IJ Scan Utility register event

Description: Enables scanning from the operation panel when printer or scanner is connected via USB.

Path to executable:
C:\Program Files (x86)\Canon\IJ Scan Utility\SETEVENT.exe

Startup type: Automatic

Unquoted Service Path



Adobe Acrobat Update Service Properties (Local Computer)

Service name: AdobeARMservice

Display name: Adobe Acrobat Update Service

Description: Adobe Acrobat Updater keeps your Adobe software up to date.

Path to executable:
"C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\armsvc.exe"

Startup type: Automatic

Quoted Service Path

https://medium.com/@SumitVerma101/windows-privilege-escalation-part-1-unquoted-service-path-c7a011a8d8ae