Google Hacking Database & Windows Hardening

By ComotSec | Ghazz

Table Of Contents :

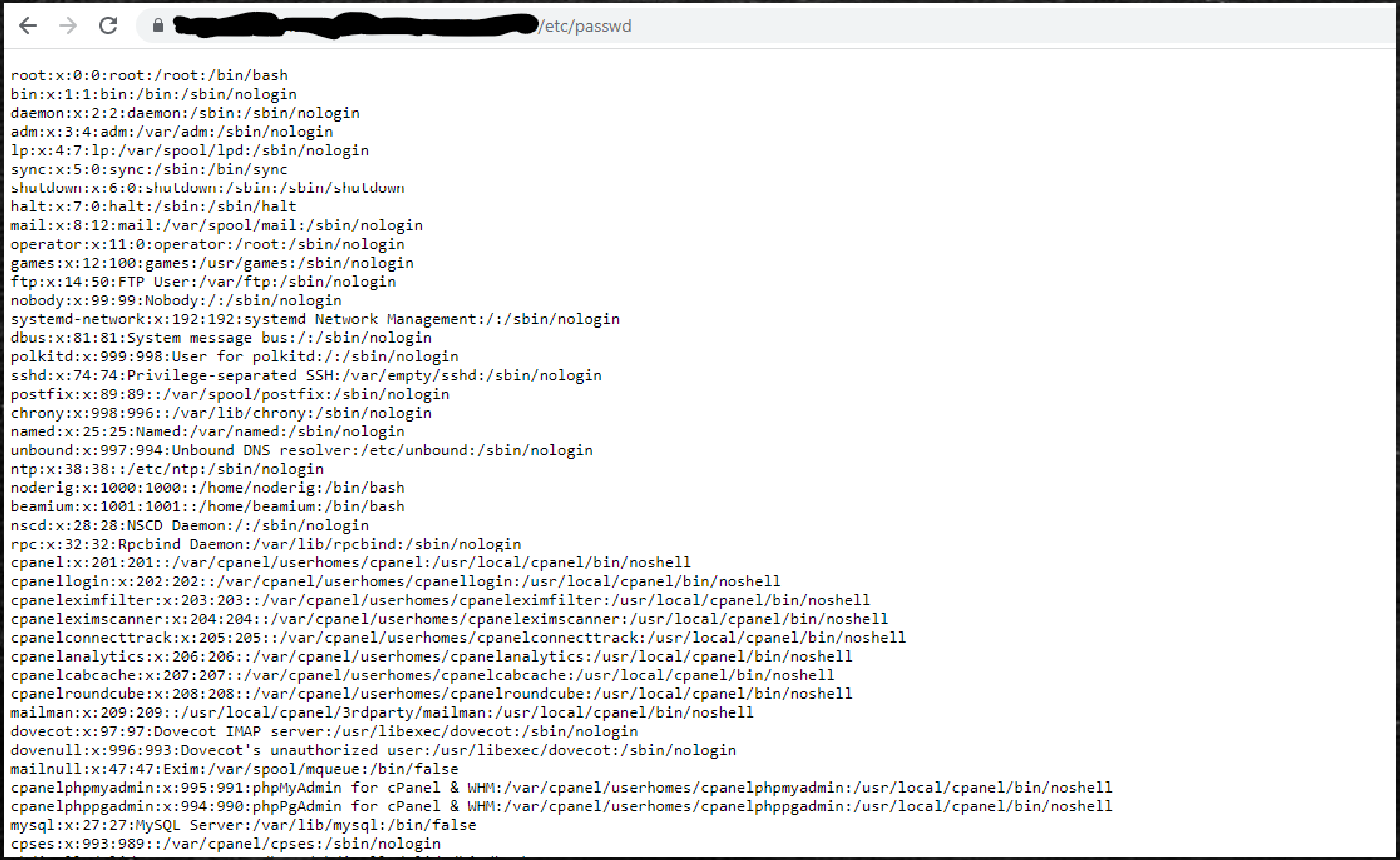
1) Google Hacking Database :

- What is Crawlers ?
- What is Google Dorking ?
- Is Crawlers and Google Dorking Illegal?
- Common Terms in Dorking
- Resources for Google Database Hacking
- Let's Practice !

2) Windows Hardening :

- What is System Hardening?
- Windows Server Hardening :
  - Windows User Configuration Guidelines
  - Windows Network Configuration Guidelines
  - Windows Service Configuration Guidelines
  - Network Time Protocol (NTP) Configuration Guidelines
  - Centralized Event Logs

Dorking > Path Traversal > Arbitrary File Read

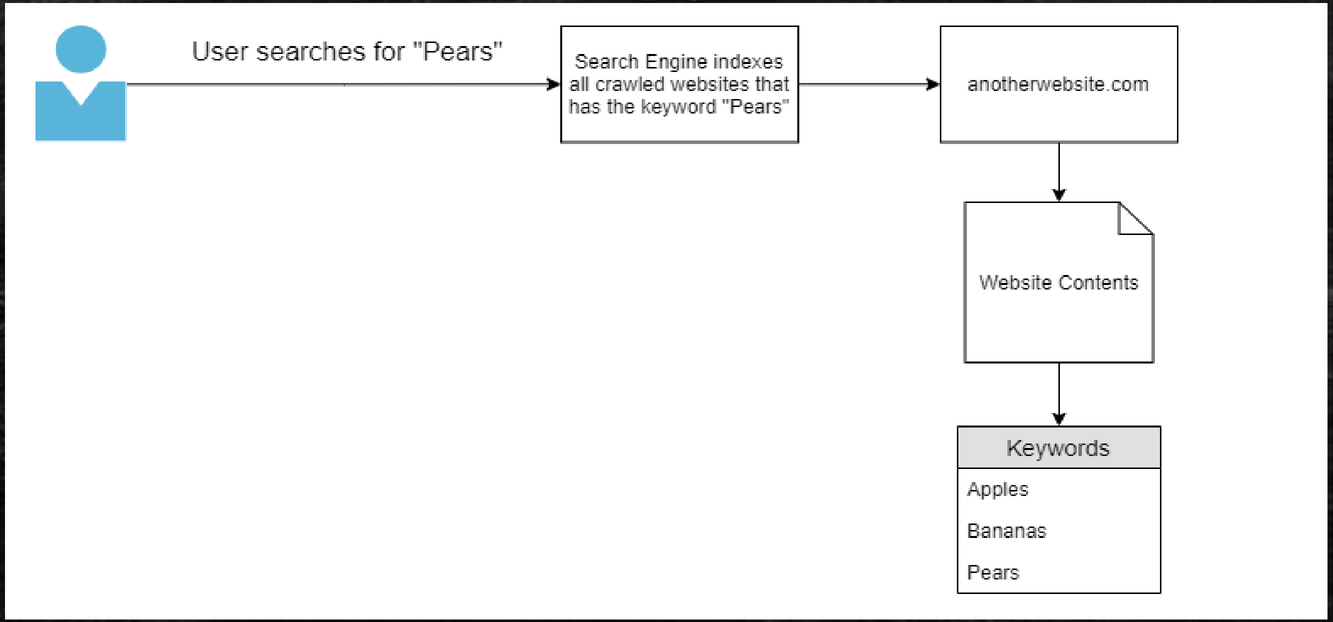


[redacted]/etc/passwd

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
systemd-network:x:192:192:systemd Network Management:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
polkitd:x:999:998:User for polkitd:/:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
chrony:x:998:996::/var/lib/chrony:/sbin/nologin
named:x:25:25:Named:/var/named:/sbin/nologin
unbound:x:997:994:Unbound DNS resolver:/etc/unbound:/sbin/nologin
ntp:x:38:38::/etc/ntp:/sbin/nologin
noderig:x:1000:1000::/home/noderig:/bin/bash
beamium:x:1001:1001::/home/beamium:/bin/bash
nscd:x:28:28:NSCD Daemon:/:/sbin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin
cpanel:x:201:201::/var/cpanel/userhomes/cpanel:/usr/local/cpanel/bin/noshell
cpanellogin:x:202:202::/var/cpanel/userhomes/cpanellogin:/usr/local/cpanel/bin/noshell
cpaneleximfilter:x:203:203::/var/cpanel/userhomes/cpaneleximfilter:/usr/local/cpanel/bin/noshell
cpaneleximscanner:x:204:204::/var/cpanel/userhomes/cpaneleximscanner:/usr/local/cpanel/bin/noshell
cpanelconnecttrack:x:205:205::/var/cpanel/userhomes/cpanelconnecttrack:/usr/local/cpanel/bin/noshell
cpanelanalytics:x:206:206::/var/cpanel/userhomes/cpanelanalytics:/usr/local/cpanel/bin/noshell
cpanelcabcache:x:207:207::/var/cpanel/userhomes/cpanelcabcache:/usr/local/cpanel/bin/noshell
cpanelroundcube:x:208:208::/var/cpanel/userhomes/cpanelroundcube:/usr/local/cpanel/bin/noshell
mailman:x:209:209::/usr/local/cpanel/3rdparty/mailman:/usr/local/cpanel/bin/noshell
dovecot:x:97:97:Dovecot IMAP server:/usr/libexec/dovecot:/sbin/nologin
dovenull:x:996:993:Dovecot's unauthorized user:/usr/libexec/dovecot:/sbin/nologin
mailnull:x:47:47:Exim:/var/spool/mqueue:/bin/false
cpanelphpmyadmin:x:995:991:phpMyAdmin for cPanel & WHM:/var/cpanel/userhomes/cpanelphpmyadmin:/usr/local/cpanel/bin/noshell
cpanelphppgadmin:x:994:990:phpPgAdmin for cPanel & WHM:/var/cpanel/userhomes/cpanelphppgadmin:/usr/local/cpanel/bin/noshell
mysql:x:27:27:MySQL Server:/var/lib/mysql:/bin/false
cpses:x:993:989::/var/cpanel/cpses:/sbin/nologin
```

What Is Crawlers ?

A web crawler, or spider, is a type of bot that is typically operated by search engines like Google and Bing. Their purpose is **to index the content of websites all across the Internet so that those websites can appear in search engine results**.



User searches for "Pears"
Search Engine indexes all crawled websites that has the keyword "Pears"
anotherwebsite.com
Website Contents
Keywords
Apples
Bananas
Pears

**What is Index ?*

An index is another name for the database used by a search engine. Indexes contain the information on all the websites that Google (or any other search engine) was able to find

What Is Google Dorking ?

It is basically a search string that uses advanced search query to find information that are not easily available on the websites.

Attackers will combine some of the keywords or use filters to find privacy information.

This will gained the attackers many useful information and use it for illegal purposes.

Google dorking is also known as passive reconnaissance (gain information about the target without actively enganging the systems)

Is Crawlers and Google Dorking Illegal?

Law Enforcement About Hacking or Computer Abused in Malaysia :

1. Akta Tandatangan Digital 1997
2. Akta Jenayah Komputer 1997
3. Akta Teleperubatan 1997
4. Akta Komunikasi & Multimedia 1998

As long as you don't misused the knowledge, so it is still legal. Remember, use it for awareness and benefit the community.

Understanding Common Terms in Dorking

Terms	Meaning
Intitle:	Find Document that have the title we want
Inurl:	Find specified terms in url
Filetype:	Find the filetype
Ext:	Find the extension of a file
Site:	We use this to limit the site that we want
Intext:	Find the words that have in the text
Cache:	Find google archive of the website

Resources For Google Hacking Database

- https://www.exploit-db.com/google-hacking-database
- https://home.ubalt.edu/abento/753/footscan/googlehacking.html
- https://www.objectivity.co.uk/blog/google-hacking-how-to-find-vulnerable-data-using-nothing-but-google-search-engine/
- https://securitytrails.com/blog/google-hacking-techniques
- https://tryhackme.com/room/googledorking
- https://pentest-tools.com/information-gathering/google-hacking

LET'S DO SOME PRACTICAL !

What is System Hardening?

According to National Institute of Standards & Technology (NIST), system hardening is process intended to eliminate a means of attack by patching vulnerabilities and turning off non-essential services.

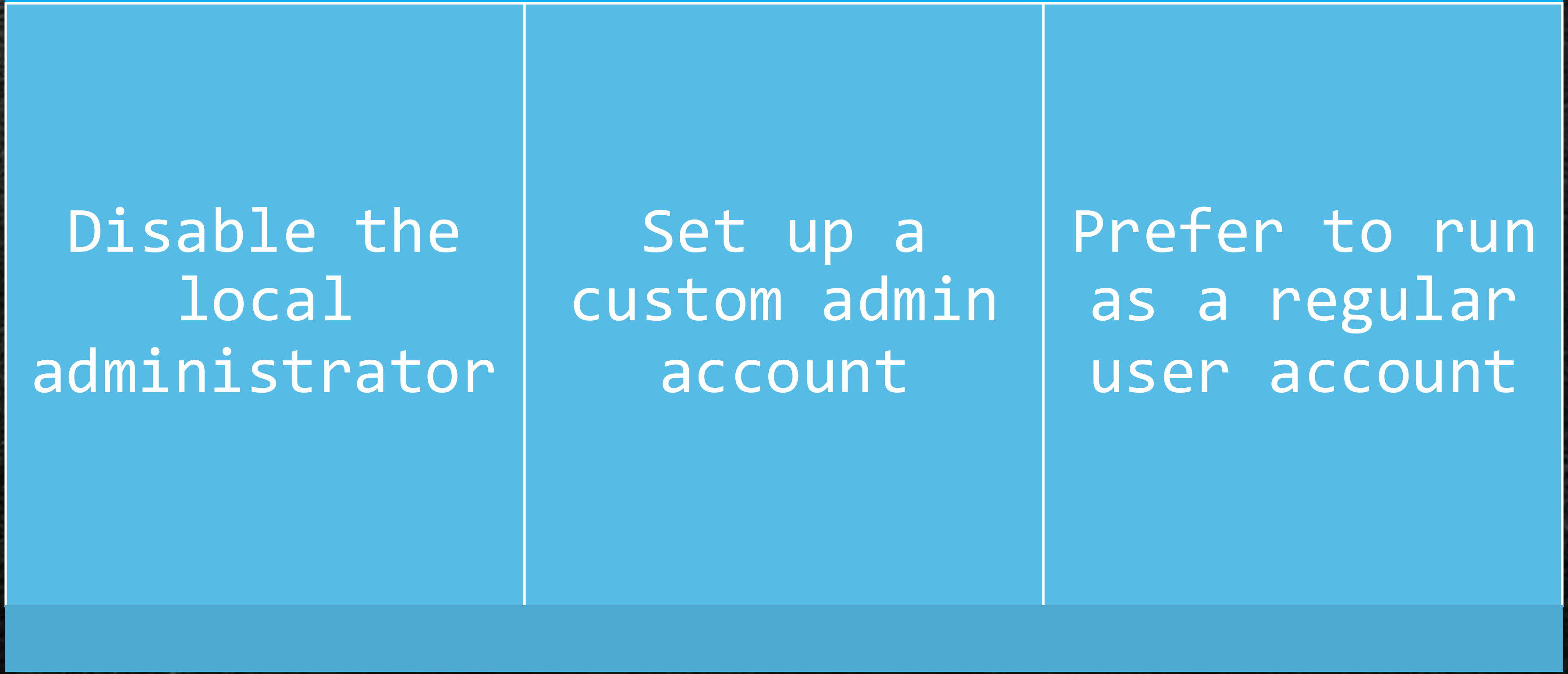
Types of System hardening :

- ✓ Server hardening
- ✓ Network hardening
- ✓ Operating System hardening
- ✓ Software hardening
- ✓ Database hardening

Windows Server Hardening

1. Windows User Configuration
2. Windows Network Configuration
3. Windows Service Configuration
4. Network Time Protocol (NTP) Configuration
5. Centralized Event Logs

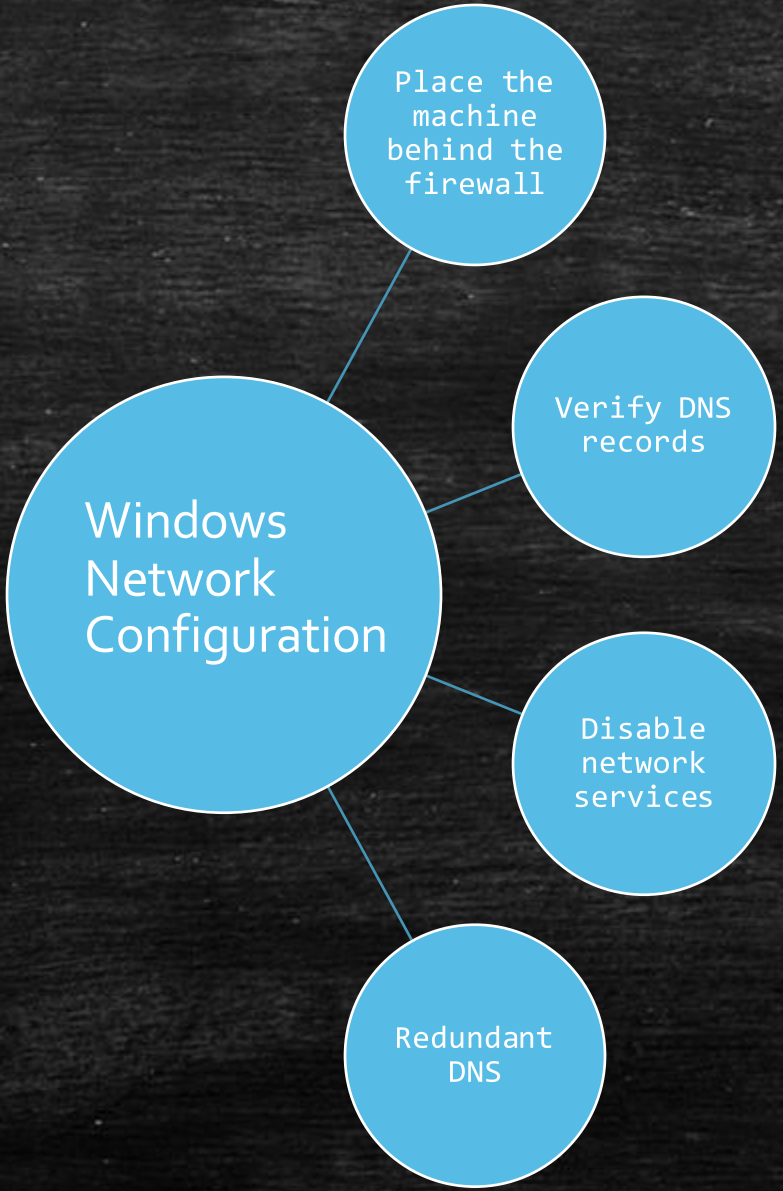
Windows User Configuration



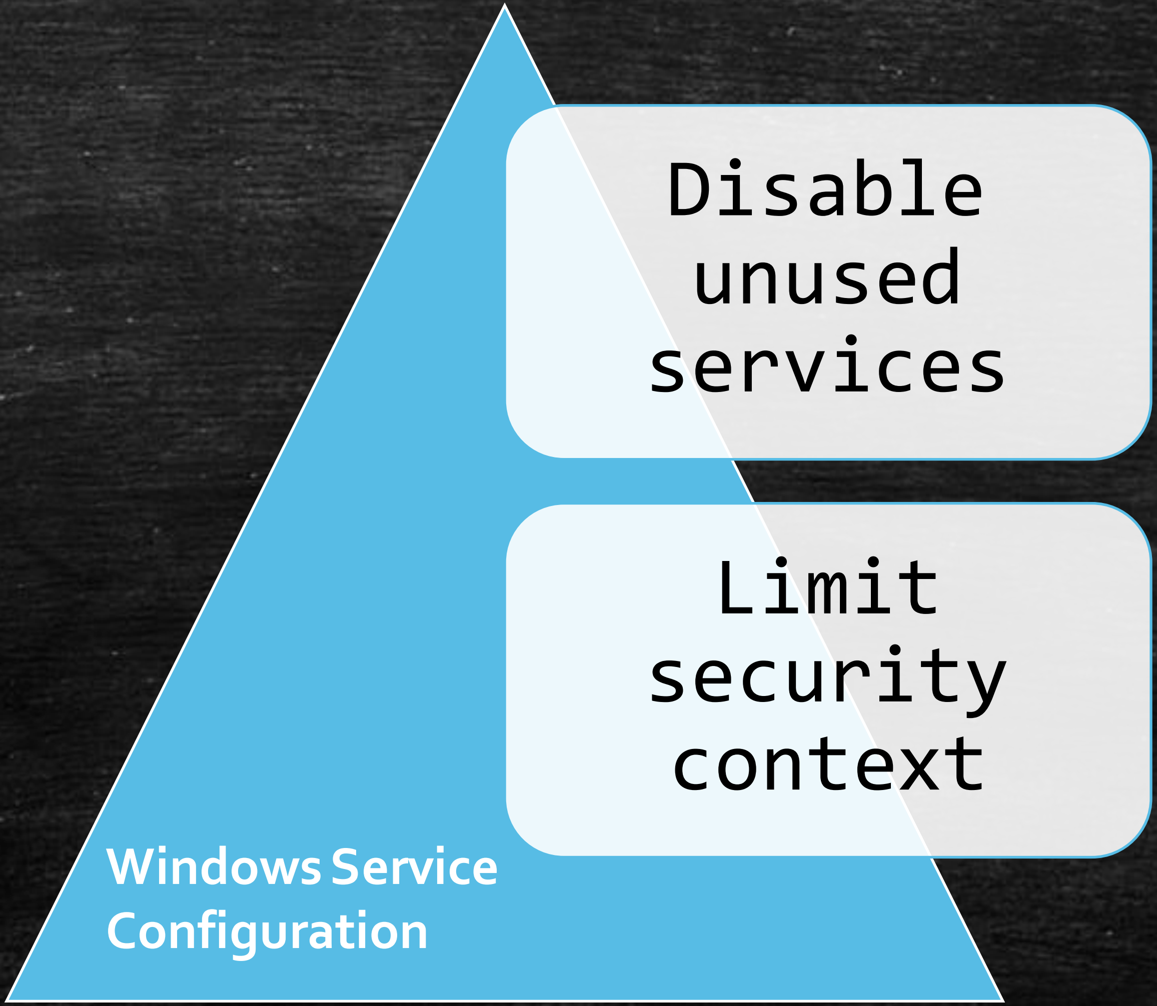
Disable the local administrator

Set up a custom admin account

Prefer to run as a regular user account



Windows Network Configuration
Place the machine behind the firewall
Verify DNS records
Disable network services
Redundant DNS



Disable unused services

Limit security context

Windows Service Configuration

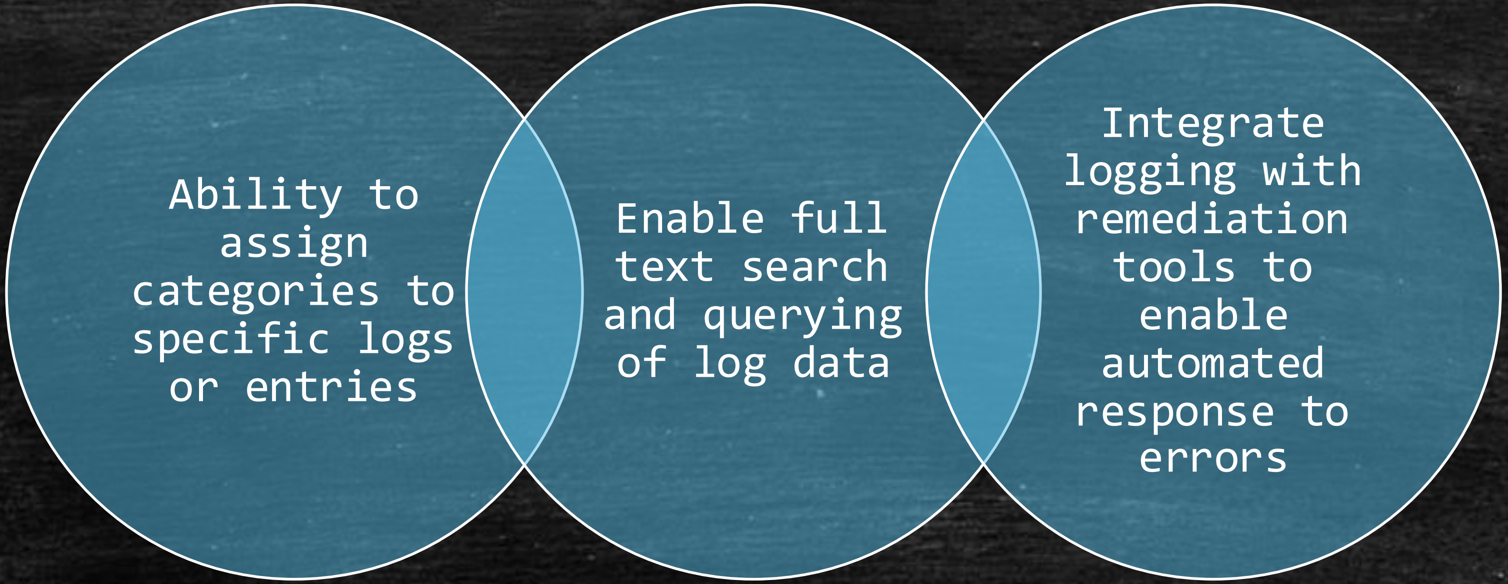
Network Time Protocol (NTP) Configuration

Servers within domains automatically sync time with the domain controller

Standalone servers sync with an external time source

Domain controllers sync with a time server on an ongoing basis

Centralized Event Logs



Ability to assign categories to specific logs or entries

Enable full text search and querying of log data

Integrate logging with remediation tools to enable automated response to errors

Windows Hardening Resources

- https://www.hysolate.com/learn/os-isolation/windows-hardening-checklist-for-windows-server-windows-10/
- https://www.trentonsystems.com/blog/system-hardening-overview
- https://github.com/decalage2/awesome-security-hardening#windows

Thank You For Your Attention

" Hacking Involves a different way of looking at problems that no one's thought of "
- Walter O'Brien -