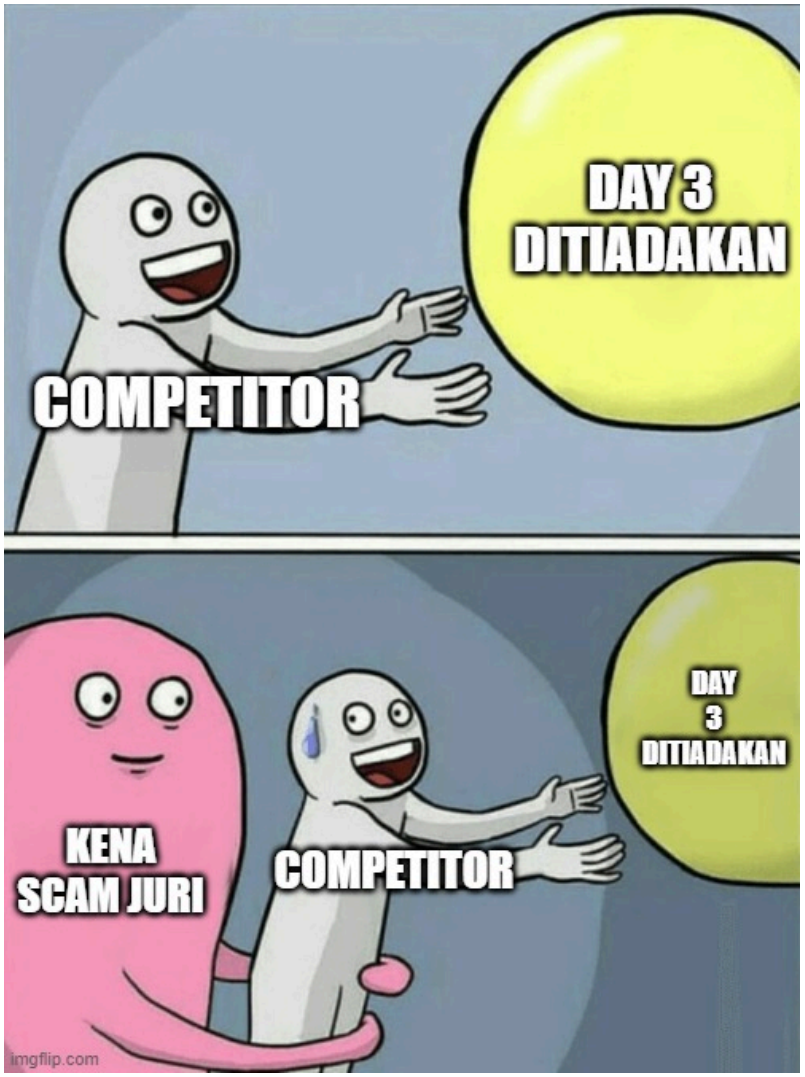
PoC Seleknas WSA Day 3 - Hardening

*The PoC by **shelltatic***



Presented by:

Ardhi Putra Pradana *A.K.A* **rootkids**
Ahmad Idza Anafin *A.K.A* **Idzoyy**

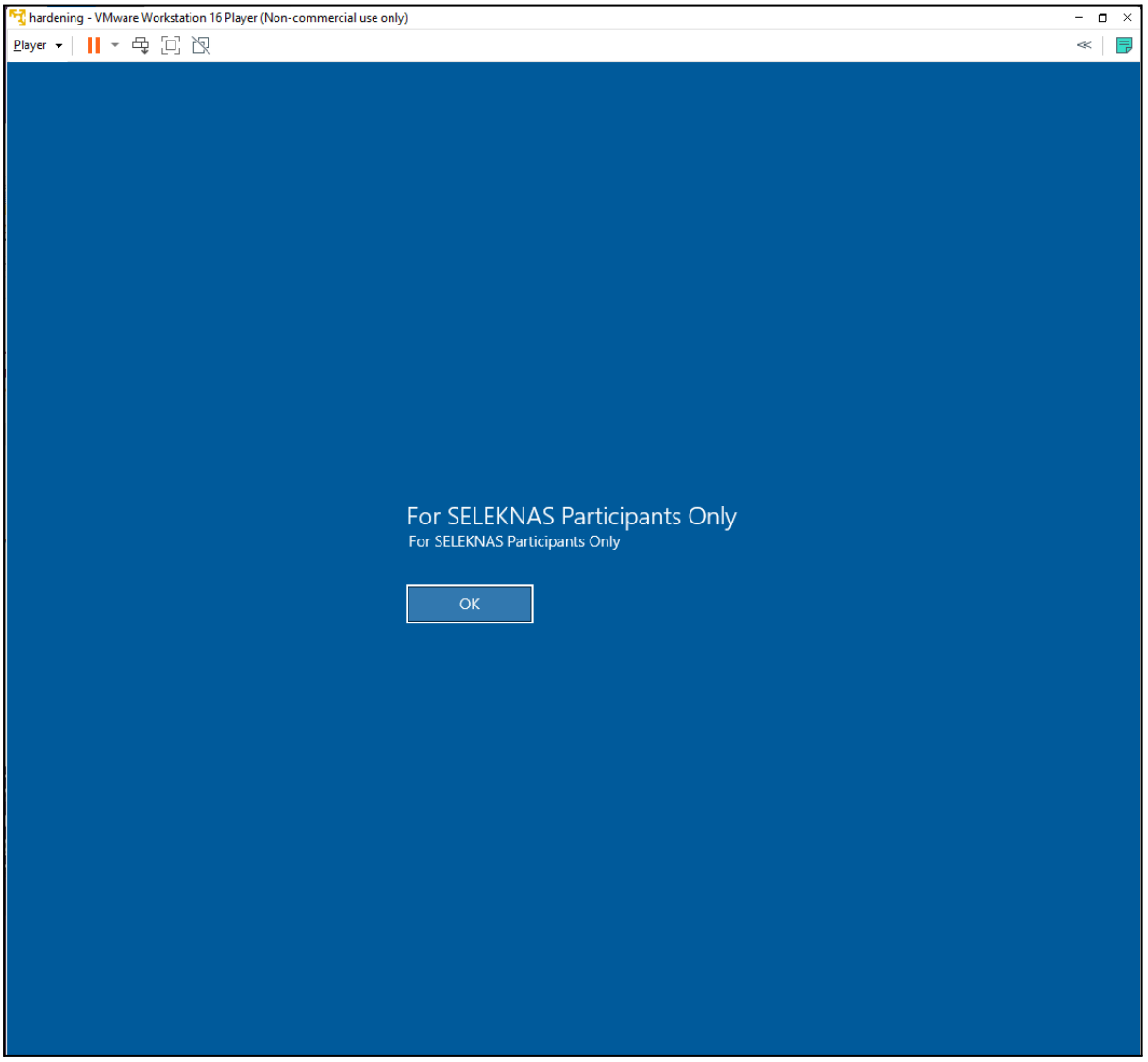
DAFTAR ISI

[WINDOWS]

Restricted banner logon

1. Klik Tools pada server manager dab Masuk ke **Group Policy Management** Console
2. Pada panel kiri terdapat struktur policy management, masuk ke options **“Domain”** dan klik kanan pada domain **“seleknascyber.local”** dan klik **“Create a GPO in this domain, and link it here”**
3. Buat group policy baru dengan nama bebas, example: LOGON BANNER
4. Kemudian klik edit pada policy yang dibuat sebelumnya
5. Kemudian masuk ke **Computer Configuration> Policies > Windows Settings > Security Settings > Local Policies** dan pilih **Security Options**
6. Pada panel sebelah kanan terdapat banyak policy, kemudian pilih
   a. **Interactive Logon: Message text for users attempting to logon** Untuk mengatur pesan banner yang tampil ketika user mencoba login
   b. **Interactive Logon: Message title for users attempting to login** Untuk mengatur title dari banner yang tampil ketika user mencoba login
7. Pada masing masing policy, centang pada checkbox **Define this policy settings in the template,** dan ketik pada kolom text pesan/judul yang ingin ditampilkan (**For SELEKNAS Participants Only**), lalu klik apply dan OK
8. setelah di konfigurasi update group policy melalui administrator command line dengan command

```
gpupdate /force
```



Setup Password Policy

1. Klik Tools pada server manager dab Masuk ke **Group Policy Management** Console
2. Pada panel kiri terdapat struktur policy management, masuk ke options **"Domain"** dan klik kanan pada domain **"seleknascyber.local"** dan masuk ke **default domain policy**
3. Kemudian masuk ke **Computer Configuration > Policies > Windows Settings > Security Settings > Account Policies**
4. Ada beberapa policy yang harus di konfigurasi
    a. **Enforcing the password complexity**
    Untuk mengatur password complexity, masuk ke **Password Policy** dan **enabled** policy **Password must meet complexity requirements**
    b. **Minimum of password length now shall be 10 instead of 7 digits**
    Untuk mengatur minimal panjang password, masuk ke **Password Policy** dan atur minimal karakter pada policy **Minimum password**

length audit dan **Minimum password length** set menjadi 10 karakter.

c. **Never use a reversible encryption to store passwords**
   Untuk mengatur minimal panjang password, masuk ke **Password Policy** dan disabled policy **Store passwords using reversible encryption**
d. **If any user wants to login as admin to this computer, please locks the account once there are 5 failed attempts. They will be locked out for approximately 1 minute and the counter will be reset after that.**
   Untuk mengatur minimal panjang password, masuk ke **Account Lockout Policy** dan set beberapa policy:
   - **Account lockout duration:** 2 minutes
   - **Account lockout threshold:** 5 (invalid logon attemps)
   - **Reset account lockout counter after:** 1 minutes

```
C:\Users\Administrator>net accounts
Force user logoff how long after time expires?:       Never
Minimum password age (days):                          1
Maximum password age (days):                          42
Minimum password length:                              10
Length of password history maintained:                24
Lockout threshold:                                    5
Lockout duration (minutes):                           30
Lockout observation window (minutes):                 1
Computer role:                                        PRIMARY
The command completed successfully.
```

Create RDP Users

Membuat user baru berikut

Username	Password	command
siahaan	SELEKING_hardeningpw123!	New-ADUser -Name "siahaan" -SamAccountName "siahaan" -AccountPassword (ConvertTo-SecureString -AsPlainText “SELEKING_hardeningpw123!” -Force) -Title "king" -Description "RDP Account Creation" -DisplayName "siahaan" -Enabled $True

enryu	SELEPWNZ_hardeningpw456!	New-ADUser -Name "enryu" -SamAccountName "enryu" -AccountPassword (ConvertTo-SecureString -AsPlainText “SELEPWNZ_hardeningpw456!” -Force) -Title "sepuh pwn" -Description "RDP Account Creation" -DisplayName "enryu" -Enabled $True
prajna	SELECRYPT_hardeningpw1$$	New-ADUser -Name "prajna" -SamAccountName "prajna" -AccountPassword (ConvertTo-SecureString -AsPlainText “SELECRYPT_hardeningpw1$$” -Force) -Title "sepuh kripto" -Description "RDP Account Creation" -DisplayName "prajna" -Enabled $True
faishol	SELE0DAY_hardeningpw23!!	New-ADUser -Name "faishol" -SamAccountName "faishol" -AccountPassword (ConvertTo-SecureString -AsPlainText “SELE0DAY_hardeningpw23!!” -Force) -Title "penimbun 0day" -Description "RDP Account Creation" -DisplayName "faishol" -Enabled $True
aseng	SELENUB_hardeningpw098?!	New-ADUser -Name "aseng" -SamAccountName "aseng" -AccountPassword (ConvertTo-SecureString -AsPlainText

		“SELENUB_hardeningpw098?!” -Force) -Title "king rev brutal" -Description "RDP Account Creation" -DisplayName "aseng" -Enabled $True

```
PS C:\Users\Administrator> Get-ADUser -Filter * -Properties * | select name,samaccountname,title,description

name          samaccountname title          description
----          -------------- -----          -----------
Administrator Administrator                 Built-in account for administering the computer/domain
Guest         Guest                         Built-in account for guest access to the computer/domain
krbtgt        krbtgt                        Key Distribution Center Service Account
siahaan       siahaan        king           RDP Account Creation
enryu         enryu          sepuh pwn      RDP Account Creation
prajna        prajna         sepuh kripto   RDP Account Creation
faishol       faishol        penimbun 0day  RDP Account Creation
aseng         aseng          king rev brutal RDP Account Creation
```

1. untuk memasukkan ke group remote desktop users, masuk ke tools **Active Directory Users and Computers** lalu masuk ke **seleknascyber.local > Builtin > Remote Desktop Users.**
2. Kemudian pada tab member klik **add > advanced > find now** lalu pilih user yang ingin ditambahkan lalu klik OK
3. Kemudian pada **Group Policy Management** masuk ke domain **“seleknascyber.local”** dan masuk ke **default domain policy** dan masuk ke **Computer Configuration > Policies > Administrative Template > Windows Components > Remote Desktop Service > Connections** lalu **enabled** pada policy **Allow users to connect remotely by using Remote Desktop Services.**
4. Lalu pada **Computer Configuration > Policies > Administrative Template > Windows Components > Remote Desktop Service > Remote Desktop Session Host > Security, enabled** policy Require user authentication for remote connections by using Network Level Authentication
5. setelah di konfigurasi update group policy melalui administrator command line dengan command

```
gpupdate /force
```

Automatically Lock

Untuk mengatur ini sama dengan **setup password policy poin d,** pada policy **Account lockout duration:** 2 minutes

Disable Cached Login

Untuk disable login cache, set policy pada **Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options > Interactive Logon: Number of previous logons to cache** set ke 0

Restrict Guest Logon on Group Users

Untuk membatasi guest logon ke Users Group, **disabled** policy pada **Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options > Accounts: Guest account status**

Always digitally sign communication for Microsoft Network Server

Untuk mengatur digital sign communication ke always, **enabled** policy pada **Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options > Microsoft network client:Digitally sign communications (always)**

Specific Audit Policy

Untuk mengatur audit policy, ceklist policy yang sesuai pada **Computer Configuration > Windows Settings > Security Settings > Local Policies > Audit Policiy** dan set sesuai policy

Enable Firewall

Untuk mengatur firewall, turn on Windows Defender Firewall

[LINUX]

SSH

Config

Disable root login

1. Buka file **/etc/ssh/sshd_config**
2. Ubah bagian **PermitRootLogin** menjadi **no**

```
nano /etc/ssh/sshd_config

# ubah bagian PermitRootLogin seperti menjadi dibawah
PermitRootLogin no
```

```
# Authentication:

#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
```

Set SSH Banner

1. Buat file **/etc/ssh/welcome_banner** dengan isi teks "This is for Staff Seleknas."

   ```
   echo "This is for Staff Seleknas." > /etc/ssh/welcome_banner
   ```

   ```
   root@seleknas:/etc/ssh# ls -la welcome_banner
   -rw-r--r-- 1 root root 28 Nov  8 01:22 welcome_banner
   root@seleknas:/etc/ssh# cat welcome_banner
   This is for Staff Seleknas.
   root@seleknas:/etc/ssh#
   ```

2. Buka file **/etc/ssh/sshd_config**

   ```
   nano /etc/ssh/sshd_config
   ```

3. Tambahkan properties baru di **/etc/ssh/sshd_config** dengan value **Banner /etc/ssh/welcome_banner**

```
Banner /etc/ssh/welcome_banner
```

4. Restart service SSH

```
systemctl restart sshd
```

Proof

FTP

Config

Disable anonymous login

1. Buka file config **/etc/vsftpd.conf**

```
nano /etc/vsftpd.conf
```

2. Ubah bagian **anonymous_enable** menjadi **NO**

```
anonymous_enable=NO
```

```
# Allow anonymous FTP? (Disabled by default).
anonymous_enable=NO
#
```

3. Restart service ftp

```
systemctl restart vsftpd
```

```
root@seleknas:/etc# systemctl restart vsftpd
root@seleknas:/etc# systemctl status vsftpd
● vsftpd.service - vsftpd FTP server
     Loaded: loaded (/usr/lib/systemd/system/vsftpd.service; enabled; preset: enabled)
     Active: active (running) since Fri 2024-11-08 02:53:57 UTC; 3s ago
    Process: 2974 ExecStartPre=/bin/mkdir -p /var/run/vsftpd/empty (code=exited, status=0/SUCCESS)
   Main PID: 2977 (vsftpd)
      Tasks: 1 (limit: 2276)
     Memory: 1.0M (peak: 1.5M)
        CPU: 10ms
     CGroup: /system.slice/vsftpd.service
             └─2977 /usr/sbin/vsftpd /etc/vsftpd.conf

Nov 08 02:53:57 seleknas systemd[1]: Starting vsftpd.service - vsftpd FTP server...
Nov 08 02:53:57 seleknas systemd[1]: Started vsftpd.service - vsftpd FTP server.
root@seleknas:/etc#
```

Enable TLS/SSL connection

1. Buat folder baru **/etc/ssl/private**

```
mkdir -p /etc/ssl/private
```

2. Generate certificate dengan openssl

```
openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout
/etc/ssl/private/vsftpd.pem -out /etc/ssl/private/vsftpd.pem
```

3. Buka file **/etc/vsftpd.conf**

```
nano /etc/vsftpd.conf
```

4. Tambahkan konfigurasi SSL/TLS di file **/etc/vsftpd.conf**

```
rsa_cert_file=/etc/ssl/private/vsftpd.pem
rsa_private_key_file=/etc/ssl/private/vsftpd.pem
ssl_enable=YES
```

5. Restart service ftp

```
systemctl restart vsftpd
```

Encapsulate filesystem

1. Buka file **/etc/vsftpd.conf**

```
nano /etc/vsftpd.conf
```

2. Uncomment atau tambahkan property **chroot_local_users** dengan value **YES**

```
chroot_local_users=YES
```

```
# You may restrict local users to their home directories.  See the FAQ for
# the possible risks in this before using chroot_local_user or
# chroot_list_enable below.
chroot_local_user=YES
```

3. Tambahkan property untuk default **ftp folder** pada config

```
user_sub_token=$USER
local_root=/home/$USER/ftp
```

```
user_sub_token=$USER
local_root=/home/$USER/ftp
```

4. Restart service ftp

```
systemctl restart vsftpd
```

```
root@seleknas:/etc# systemctl restart vsftpd
root@seleknas:/etc# systemctl status vsftpd
● vsftpd.service - vsftpd FTP server
     Loaded: loaded (/usr/lib/systemd/system/vsftpd.service; enabled; preset: enabled)
     Active: active (running) since Fri 2024-11-08 02:53:57 UTC; 3s ago
    Process: 2974 ExecStartPre=/bin/mkdir -p /var/run/vsftpd/empty (code=exited, status=0/SUCCESS)
   Main PID: 2977 (vsftpd)
      Tasks: 1 (limit: 2276)
     Memory: 1.0M (peak: 1.5M)
        CPU: 10ms
     CGroup: /system.slice/vsftpd.service
             └─2977 /usr/sbin/vsftpd /etc/vsftpd.conf

Nov 08 02:53:57 seleknas systemd[1]: Starting vsftpd.service - vsftpd FTP server...
Nov 08 02:53:57 seleknas systemd[1]: Started vsftpd.service - vsftpd FTP server.
root@seleknas:/etc#
```

Only allow ftp users to login

1. Buka file **/etc/vsftpd.conf**

```
nano /etc/vsftpd.conf
```

2. Tambahkan config berikut agar hanya user yang ditambahkan ke ftp users yang dapat login

```
userlist_enable=YES
userlist_file=/etc/vsftpd.userlist
userlist_deny=NO
```

```
userlist_enable=YES
userlist_file=/etc/vsftpd.userlist
userlist_deny=NO
```

3. Buat file **/etc/vsftpd.userlist** dan tambahkan user **ftp_user**

```
echo “ftp_user” > /etc/vsftpd.userlist
```

```
root@seleknas:/etc# cat vsftpd.userlist
ftp_user
root@seleknas:/etc#
```

4. Buat folder ftp di home **ftp_user**

```
mkdir -p /home/ftp_user/ftp
```

5. Restart service ftp

```
systemctl restart vsftpd
```

```
root@seleknas:/etc# systemctl restart vsftpd
root@seleknas:/etc# systemctl status vsftpd
● vsftpd.service - vsftpd FTP server
     Loaded: loaded (/usr/lib/systemd/system/vsftpd.service; enabled; preset: enabled)
     Active: active (running) since Fri 2024-11-08 02:53:57 UTC; 3s ago
    Process: 2974 ExecStartPre=/bin/mkdir -p /var/run/vsftpd/empty (code=exited, status=0/SUCCESS)
   Main PID: 2977 (vsftpd)
      Tasks: 1 (limit: 2276)
     Memory: 1.0M (peak: 1.5M)
        CPU: 10ms
     CGroup: /system.slice/vsftpd.service
             └─2977 /usr/sbin/vsftpd /etc/vsftpd.conf

Nov 08 02:53:57 seleknas systemd[1]: Starting vsftpd.service - vsftpd FTP server...
Nov 08 02:53:57 seleknas systemd[1]: Started vsftpd.service - vsftpd FTP server.
root@seleknas:/etc#
```

Proof

```
admin_seleknas@seleknas:~$ ftp localhost
Connected to localhost.
220 (vsFTPd 3.0.5)
Name (localhost:admin_seleknas): anonymous
530 Permission denied.
ftp: Login failed
ftp> _
```

```
root@seleknas:/home/admin_seleknas# ftp localhost
Connected to localhost.
220 (vsFTPd 3.0.5)
Name (localhost:admin_seleknas): staff_user
530 Permission denied.
ftp: Login failed
ftp>
```

```
root@seleknas:/home/admin_seleknas# ftp localhost
Connected to localhost.
220 (vsFTPd 3.0.5)
Name (localhost:admin_seleknas): ftp_user
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> _
```

Web

Config

SSL/TLS Connection

1. Melakukan generate key certificate menggunakan openssl

```
sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout
/etc/ssl/private/nginx-selfsigned.key -out
/etc/ssl/certs/nginx-selfsigned.crt
```

2. Override default site setting dan simpan file aslinya ke backup

```
cp /etc/nginx/site-available/default
/etc/nginx/site-available/default.bak
```

3. Buka file config nginx **/etc/nginx/site-enabled/default** dan ubah semua isinya dengan config berikut

```
server {
    listen 443 ssl default_server;
    listen [::]:443 ssl default_server;
    ssl_certificate /etc/ssl/certs/web-service.crt;
    ssl_certificate_key /etc/ssl/private/web-service.key;
    ssl_protocols TLSv1.3;
    ssl_prefer_server_ciphers on;
    ssl_dhparam /etc/nginx/dhparam.pem;
    ssl_ciphers EECDH+AESGCM:EDH+AESGCM;
    ssl_ecdh_curve secp384r1;
    ssl_session_timeout  10m;
    ssl_session_cache shared:SSL:10m;
    ssl_session_tickets off;
    ssl_stapling on;
    ssl_stapling_verify on;
    resolver 8.8.8.8 8.8.4.4 valid=300s;
    resolver_timeout 5s;


    root /var/www/html;
    index index.html index.htm index.nginx-debian.html;

    server_name _;
    location / {
        try_files $uri $uri/ =404;
    }
}
```

4. Restart **nginx** service

```
systemctl restart nginx
```

```
root@seleknas:/etc# systemctl restart nginx
root@seleknas:/etc# systemctl status nginx
● nginx.service - A high performance web server and a reverse proxy server
     Loaded: loaded (/usr/lib/systemd/system/nginx.service; enabled; preset: enabled)
     Active: active (running) since Fri 2024-11-08 03:01:06 UTC; 3s ago
       Docs: man:nginx(8)
    Process: 3025 ExecStartPre=/usr/sbin/nginx -t -q -g daemon on; master_process on; (code=exited, status=0/SUCCESS)
    Process: 3027 ExecStart=/usr/sbin/nginx -g daemon on; master_process on; (code=exited, status=0/SUCCESS)
   Main PID: 3028 (nginx)
      Tasks: 2 (limit: 2276)
     Memory: 2.1M (peak: 2.3M)
        CPU: 13ms
     CGroup: /system.slice/nginx.service
             ├─3028 "nginx: master process /usr/sbin/nginx -g daemon on; master_process on;"
             └─3030 "nginx: worker process"

Nov 08 03:01:06 seleknas systemd[1]: Starting nginx.service - A high performance web server and a reverse proxy server...
Nov 08 03:01:06 seleknas systemd[1]: Started nginx.service - A high performance web server and a reverse proxy server.
root@seleknas:/etc#
```

Redirect all traffic to HTTPS

1. Buka file config nginx **/etc/nginx/site-available/default** dan tambahkan dipaling bawah config berikut

```
server {
    listen 80;
    listen [::]:80;

    server_name _;

    return 302 https://$host$request_uri;
}
```

2. Restart nginx service

```
systemctl restart nginx
```

```
root@seleknas:/etc# systemctl restart nginx
root@seleknas:/etc# systemctl status nginx
● nginx.service - A high performance web server and a reverse proxy server
     Loaded: loaded (/usr/lib/systemd/system/nginx.service; enabled; preset: enabled)
     Active: active (running) since Fri 2024-11-08 03:01:06 UTC; 3s ago
       Docs: man:nginx(8)
    Process: 3025 ExecStartPre=/usr/sbin/nginx -t -q -g daemon on; master_process on; (code=exited, status=0/SUCCESS)
    Process: 3027 ExecStart=/usr/sbin/nginx -g daemon on; master_process on; (code=exited, status=0/SUCCESS)
   Main PID: 3028 (nginx)
      Tasks: 2 (limit: 2276)
     Memory: 2.1M (peak: 2.3M)
        CPU: 13ms
     CGroup: /system.slice/nginx.service
             ├─3028 "nginx: master process /usr/sbin/nginx -g daemon on; master_process on;"
             └─3030 "nginx: worker process"

Nov 08 03:01:06 seleknas systemd[1]: Starting nginx.service - A high performance web server and a reverse proxy server...
Nov 08 03:01:06 seleknas systemd[1]: Started nginx.service - A high performance web server and a reverse proxy server.
root@seleknas:/etc#
```

Proof


root@seleknas:/etc# curl http://localhost -I
HTTP/1.1 302 Moved Temporarily
Server: nginx/1.24.0 (Ubuntu)
Date: Fri, 08 Nov 2024 03:35:49 GMT
Content-Type: text/html
Content-Length: 154
Connection: keep-alive
Location: https://localhost/
root@seleknas:/etc# curl https://localhost -Ik
HTTP/1.1 200 OK
Server: nginx/1.24.0 (Ubuntu)
Date: Fri, 08 Nov 2024 03:35:52 GMT
Content-Type: text/html
Content-Length: 14638
Last-Modified: Tue, 29 Oct 2024 12:07:22 GMT
Connection: keep-alive
ETag: "6720cffa-392e"
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Accept-Ranges: bytes
root@seleknas:/etc# _

User

Config

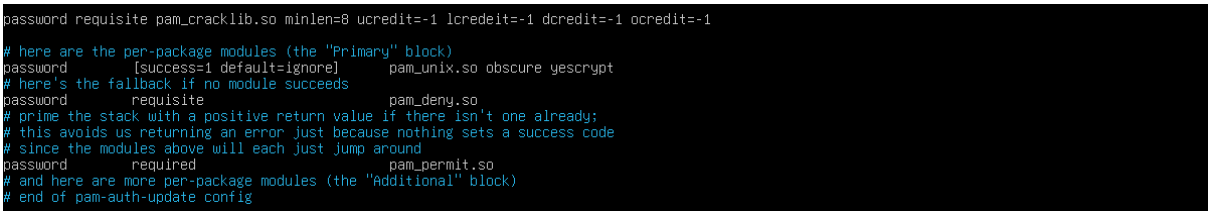
Enforce strong password policy

1. Buka file **/etc/pam.d/common-password**

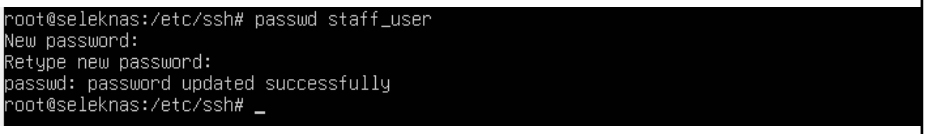
```
nano /etc/pam.d/common-password
```

2. Lalu masukkan config berikut sebelum line dengan kata **pam_unix.so**

```
password requisite pam_cracklib.so minlen=8 ucredit=-1 lcredit=-1
dcredit=-1  ocredit=-1
```



Replace any default passwords user, meet the strong password policy

staff_user	password: SeleknasGac0r? 
staff_guest	password: 1nginJuara! 
ftp_user	password: FTPuhuy* 
admin_seleknas	password: M1minSangar#

	root@seleknas:/etc/ssh# passwd admin_seleknas New password: Retype new password: passwd: password updated successfully root@seleknas:/etc/ssh#

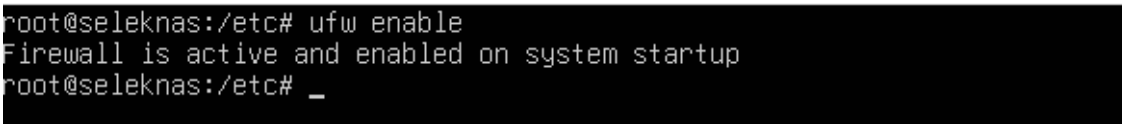
Firewall

Config

Enable firewall

1. Gunakan **ufw** untuk melakukan enable firewall

```
ufw enable
```



Firewall policy

1. Default deny all incoming and outgoing connections

```
ufw default deny incoming
ufw default deny outgoing
```

2. Allow specific services

SSH	ufw allow 22
FTP	ufw allow 21 ufw allow 20
HTTP	ufw allow 80 ufw allow 443
Nginx Resolver	ufw allow out to 8.8.8.8 ufw allow out to 8.8.4.4

Proof

```
root@seleknas:/etc# ufw show added
Added user rules (see 'ufw status' for running firewall):
ufw allow 22
ufw allow 20
ufw allow 21
ufw allow 80
ufw allow 443
ufw allow out to 8.8.8.8
ufw allow out to 8.8.4.4
root@seleknas:/etc#
```