1 - Specs and Details

spek :

- name: windows-server 2019
- os: windows
- ram: 2048mb / 2GB an
- cpu: 1core
- memory: 30GB

first issue - virtualbox VM

- error msg: windows cannot find the microsoft software license terms make sure the installation source are valid virtualbox

Solve with :

- pertama create new vm di vbox nya, jangan masukin ISO
- kalau udah buat spek2 nya juga, yang penting ga masuk
- ke settings di vm vbox nya, ke storage
- empty klik, baru tambahin iso nya disitu, yg gambar CD floppy disk
- and run, nanti bisa

step to install

- di windows setup, select OS yg : Windows Server Standard (Evaluation) Desktop experience (biar ga full CLI)
- lalu pilih: custom install windows only (advanced)
- partisi: di drive full, new aja, sampai ada system dan primary, 500mb buat system
- kalau error primary 2 2 nya, delete 2 2 nya sampai unallocated semua, baru ulang new
- set creds -> Administrator:lon3w0lf_f0r3ver
- nah pas open kunci ctrl + alt + del:
- jangan dari keyboard lgsg di vbox ke input -> keyboards -> ctrl alt del nanti ada disitu

server setup

- ganti computer name nya dulu, search aja computername and rename jadi: LIMBO-DC
- di server manager
- manage -> add roles and feature -> next2 in aja -> tambahin ini :

- web server IIS
- AD DS (active directory domain services)

2 - Services

- set web server IIS doang, gausah macem2 next2 aja semuanya terus install
- include IIS management console nya juga

after setup

- ke IIS management, search aja, klik nama hostnya LIMBO-DC
- klik directory browsing -> open feature -> enable
- fungsinya biar dia bisa nge fuzz ke secret dir lain2

get web page source code

- di windows server ke path /administrator/desktop
- di mesin utama nyalain python server

```
python -m http.server
```

- di mesin windows server get file nya

```
curl ip_mesin_utama:8000/abandoned.zip -o abandoned.zip
```

- ekstrak aja ke /inetpub/wwwroot, then coba akses dari luar ip nya
- then berhasil akses web nya, path2 nya juga work, /robots.txt ada

3 - Foothold And Privilege Escalation

3.1 - Foothold

- buat web static
- isinya nanti ada sensitive data di .env
- taruh web static nya di \inetpub\wwwroot

Creds and Directory Leak

- /robots.txt set begini

```
User-agent: *
Disallow: /assets
Disallow: /abandoned
```

- /abandoned/.env set begini

```
forgotten_me=leave_me_alone
APP_ENV=production
LDAP_BIND_USER=abandoned_svc
LDAP_BIND_PASS=emptyroom
LDAP_BASE_DN=DC=abandoned,DC=local
LDAP_HOST=127.0.0.1
```

- /assets/css/style.css

```
.forgotten-me {
    messages: leave_me_alone
}
```

3.2 - Privilege Escalation

ACL Abuse (GenericALL to Administrator)

- kalau mau validasi disini

```
dsacls "CN=Administrator,CN=Users,DC=abandoned,DC=local"
```

- lalu cek apakah ada nama user yg dipilih dan full access control

ACL Abuse (GenericALL to Domain Admins)

- kalau mau validasi disini
- karna ku taruh ke group domain admins nya jadi gini deh

```
dsquery group -name "Domain Admins"
dsacls "CN=Domain Admins,OU=group,DC=abandoned,DC=local"
```

Issue

- AV nyala bro, gabisa winpeas, disable dulu lah yaelah
- ke windows security, virus threat protection

- dah off in semua lah

Issue 2

- tiap ngerjain mesinnya lama, acl nya mati, emptyplace_svc gapunya privilege lagi
- mau privesc denied terus kalau udah waktunya , kalau belum waktunya masih bisa privesc
- disebabkan SDProp, yang tiap 1 jam nge clear group2 protected gitu lah yg anomali di clear
- di AdminSDHolder letaknya, jadi kalau mau acl nya abadi, masukin aja ke situ emptyplace nya
- cek dulu disini

```
dsacls "CN=AdminSDHolder,CN=System,DC=abandoned,DC=local"
```

- lalu buat biar ada nantinya

```
dsacls "CN=AdminSDHolder,CN=System,DC=abandoned,DC=local" /G emptyplace_svc:GA
```

4 - Creds

Windows Server

- Administrator:lon3w0lf_f0r3ver

LDAP

```
LDAP_BIND_USER=abandoned_svc
LDAP_BIND_PASS=emptyroom
DOMAIN=abandoned.local
```

5 - Active Directory

5.1 - ACL (Access Control List)

Ke user Administrator

- buka active directory users and computers
- terus ke view -> advanced features
- kalau udah coba ke domain -> users -> klik kanan di administrator
- klik properties, security, add, ketik emptyp checknames, ok, apply ok
- full controls nya allow, buat emptyplace_svc ini

- next coba refresh mesin nya

Ke domain Admins

- buka active directory users and computers
- view -> advanced features
- kalau udah coba ke domain -> (cari domain admins nya)
- disini di groups, klik kanan domain admins
- properties, security add -> emptypla checknames, ok apply ok
- set full controls allow nya buat emptyplace_svc
- next coba refresh mesinnya

Issues

- pas export .ova dsacls nya ga ada si emptyplace genericAll ke administrator
- kemungkinan belum kesimpen di ntds.dit tapi udah ke export .ova duluan
- eh bukan, ternyata gada pengaruhnya soalnya di main machine juga gada sih genericAll nya
- mungkin karna abis nambahin deskripsi jadi keubah configgnya, ulang lagi aja

5.2 - Domain Services (AD DS)

Install and Setup

- next2 terus aja set default nya gimana install ampe selesai
- kalau ada centang kuning di bendera klik aja, terus promote this server to a domain controller
- add new forest
- namain: ABANDONED.local, next
- kasih passwordnya sama kayak administraro aja: lon3w0lf_f0r3ver
- next2 aja, netbios nya default ke ABANDONED, then next2 aja sampai install
- nanti kalau done, users berubah jadi ABANDONED\Administrator

Settings After Setup

- search ke AD users and computers
- klik kanan di domain mu, new -> organizational unit, nah masukin semua security kesana
- users nya biar tinggal admin sama guest
- bikin 2 users, skenario nya yg 1 buat ldap
- yg 1 naruh user.txt and crack passnya di kerberos jadi pass nya yg ada di rockyou

Issue

- ada issue password gabisa di set lemah, solusi
- ke group policy management, search aja, terus dropdown domains
- sampai ada default domain, klik kanan edit
- computer config, policies, windows set, security set, account, password
- complexity di disabled, apply, mungkin restart dulu abis itu, terus coba lagi

Other Issue

- .env gabisa di akses di web nya, di /abandoned/.env malah 404 not found
- ke IIS manager, search aja
- terus ke domain mu, terus ke request filtering
- klik, open feature, delete .env kalau ada, masalahnya disini gada dan tetep strict
- udah pakai web.config juga gabisa, malah 500 tadinya 404
- solusi: ganti aja nama filenya, .env jadi env.txt biar bisa di akses pemain

Users

- user 1

```
abandoned_svc:emptyroom
emptyplace_svc:darkness
```

5.3 - Kerberos

- kerberos target set ke si emptyplace_svc

```
setspn -A MSSQLSvc/abandoned.local emptyplace_svc
```

Issue kerberos

- jam windows kan ga sinkron dia, 01.00, di linux dan aslinya 21.08
- penyebab karna mesinnya ku suspend, jadi ga ku shutdown ama restart vm nya
- fix nya di cmd:

```
time
```

- lalu perbaikin jam windows nya, and attack kerberos lagi

Kerberoasting Tips

- error begini

```
Hashfile 'hash' on line 1 (krb5tg...25686d89ad0c71166341be55f12d43e5):
Separator unmatched
No hashes loaded.
```

- solusi, nanti copy kerberos nya dari terminal dan gausah tempel2 ngawur
- copy dari terminal semuanya mulai dari ini lalu paste nanti ada:

```
hashcat --identify 'krb5tgs$23$*emptyplace_sv.....'
13100 | Kerberos 5, etype 23, TGS-REP
```

- untuk ngecrack tinggal gini aja

```
echo '$krb5tgs$23$*emptypl.....' > hash
hashcat -m 13100 hash /usr/share/wordlists/rockyou.txt
```

5.4 - Win RM (Remote Management)

- karna users emptyplace_svc udah dapat creds nya dari TGT kerberos
- jadi kita bikin biar pemain bisa win-rm pake creds tersebut
- sekarang search ke Active directory users and computers
- ke Builtin -> remote management users klik 2x
- klik add -> masukin emptyplace, klik checknames -> ok
- apply and ok, then restart machine nya

Evil-winrm

- nah entah kenapa evil winrm nya gapake domain

```
evil-winrm -i [ip] -u emptyplace_svc -p darkness
```

- eh gini bisa sih

```
evil-winrm -i [ip] -u 'ABANDONED\emptyplace_svc' -p darkness
evil-winrm -i [ip] -u emptyplace_svc@abandoned.local -p darkness
```

Flags

- user.txt: FLAG{7c479458fa8e35d63da1d0efe0d2d5d9}
- root.txt: FLAG{52e1febc6c6b321f18b5467424d85dea}