CEH – Day 11 Documentation

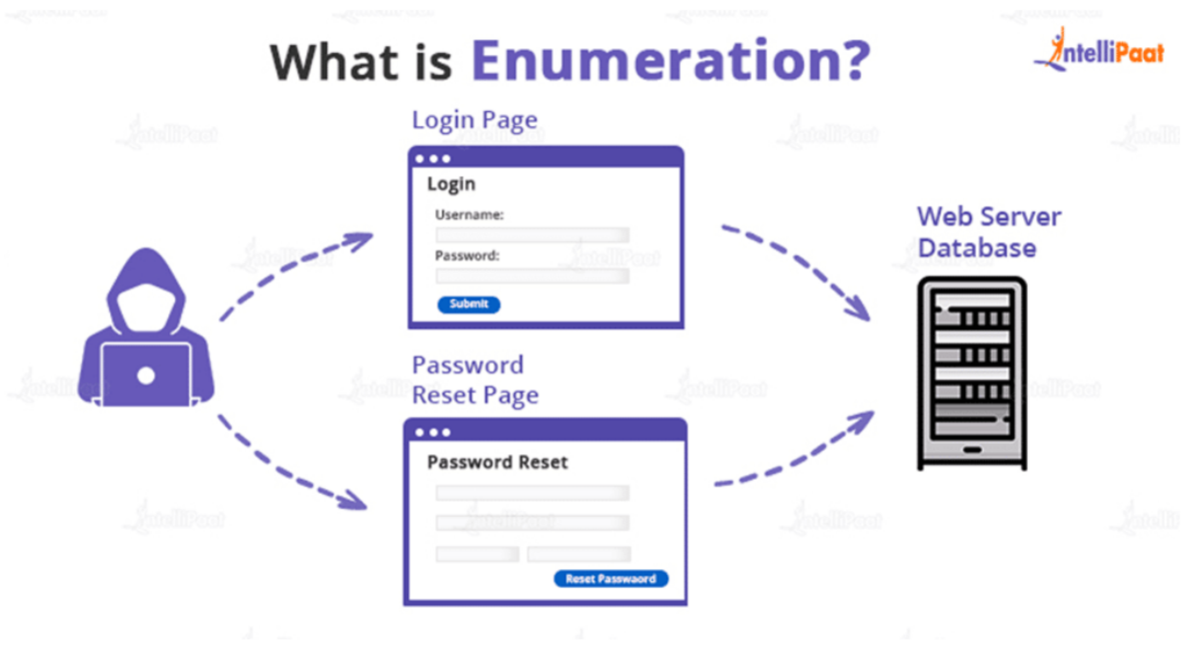
DNS Enumeration & Password Attacks

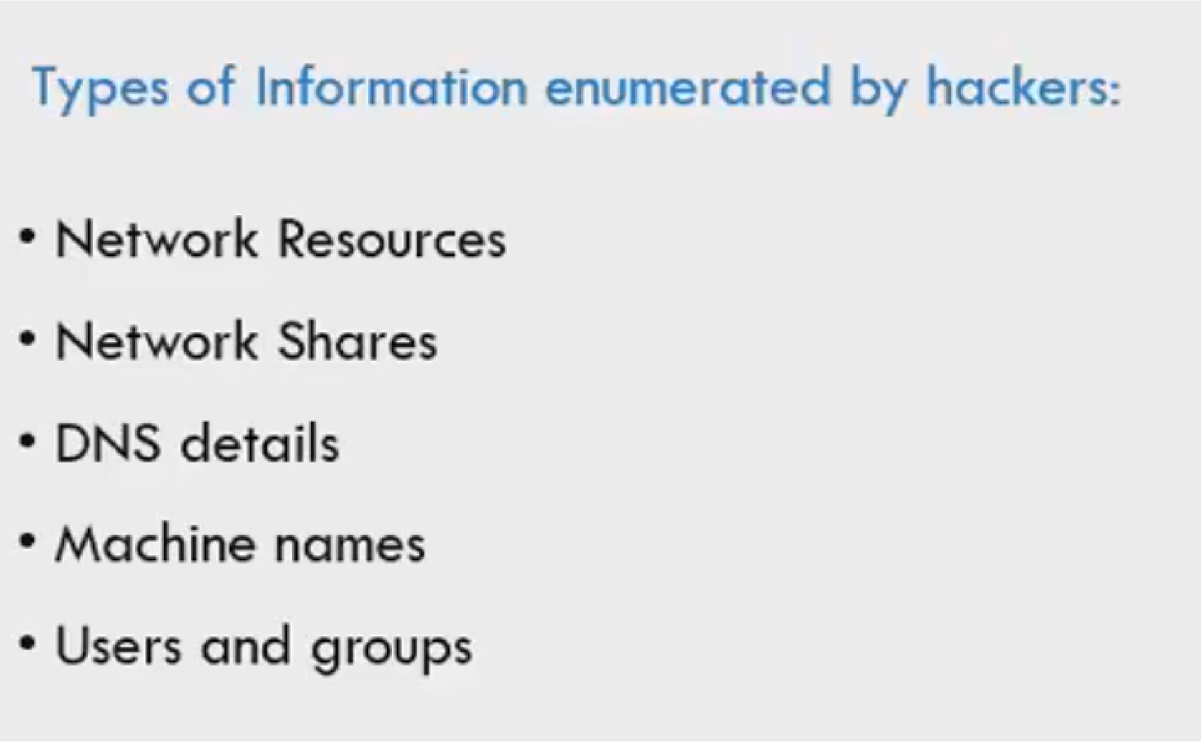
> Part of CEH (Certified Ethical Hacker) Practical Learning
> Topic: DNS Enumeration, FTP Enumeration & Password Attacks

Table of Contents

What is Enumeration?

Enumeration is the process of actively extracting detailed information from a target system by sending structured queries and analyzing responses.





Types of Information enumerated by hackers:

- Network Resources
- Network Shares
- DNS details
- Machine names
- Users and groups

Goal: To gather as much valid information as possible about the target environment.

Information Gathered During Enumeration

Network and Website Information:

- Active hosts
- Subdomains (mail.domain.com, vpn.domain.com)
- Open ports and running services

Network Shares:

- Shared folders
- File permissions
- Misconfigured public shares

Accessing SMB Share (Windows): Win + R
\192.168.1.25

DNS Information:

- DNS records
- Name servers
- Subdomains

System Details:

- Hostnames
- Machine names

Users and Groups:

- Valid usernames

- Administrator accounts
- Privilege information

DNS Basics

DNS (Domain Name System) converts domain names into IP addresses.

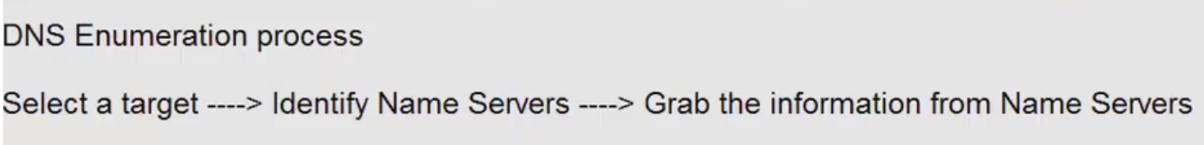
DNS Resolution Flow:

1. Browser sends request to DNS Resolver
2. Resolver contacts Root Server, TLD Server, and Authoritative DNS Server
3. IP address is returned to the browser

DNS Resolver acts as the DNS client.

What is DNS Enumeration?

DNS Enumeration is the process of collecting all DNS-related information about a target domain.



DNS Enumeration process

Select a target ----> Identify Name Servers ----> Grab the information from Name Servers

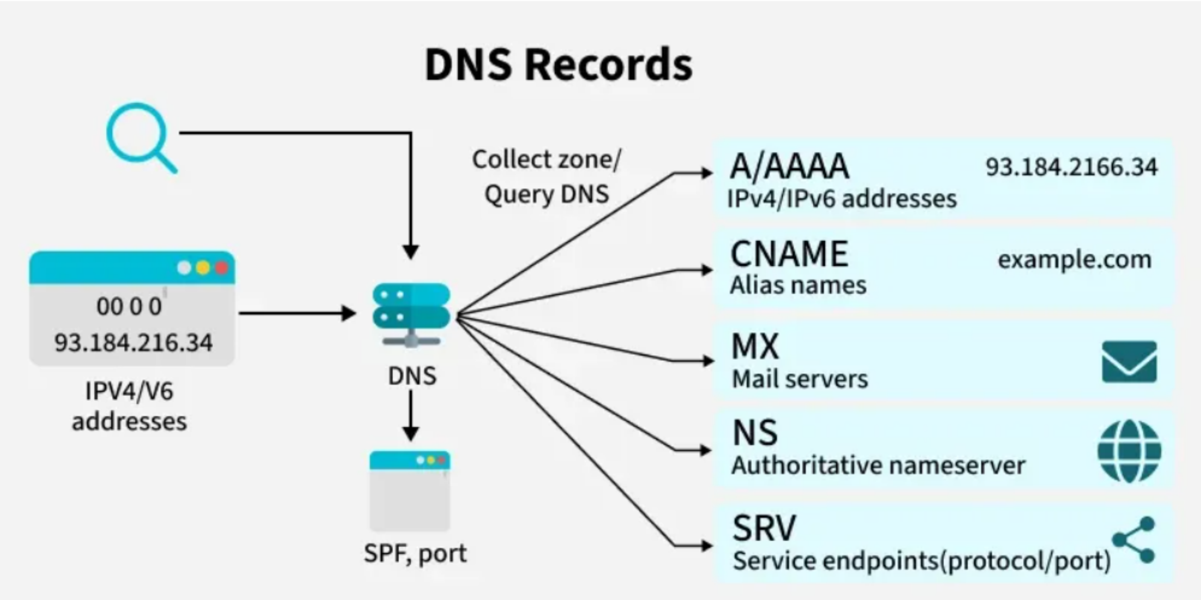
Information Collected:

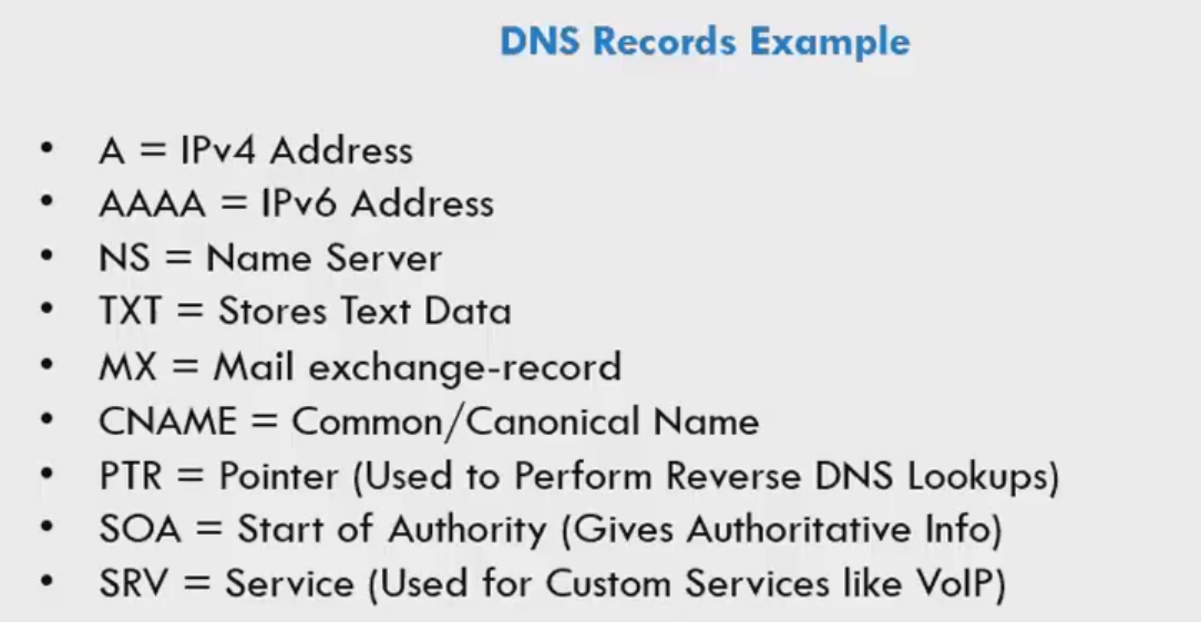
- DNS servers
- Subdomains
- IP addresses
- Mail servers
- TXT records
- Zone transfer data

Helps in understanding the entire domain structure.

DNS Record Types

A record – IPv4 address mapping
AAAA record – IPv6 address mapping
NS record – Name server
MX record – Mail server
TXT record – Verification or SPF
CNAME record – Alias
SOA record – Zone authority information
PTR record – Reverse DNS mapping





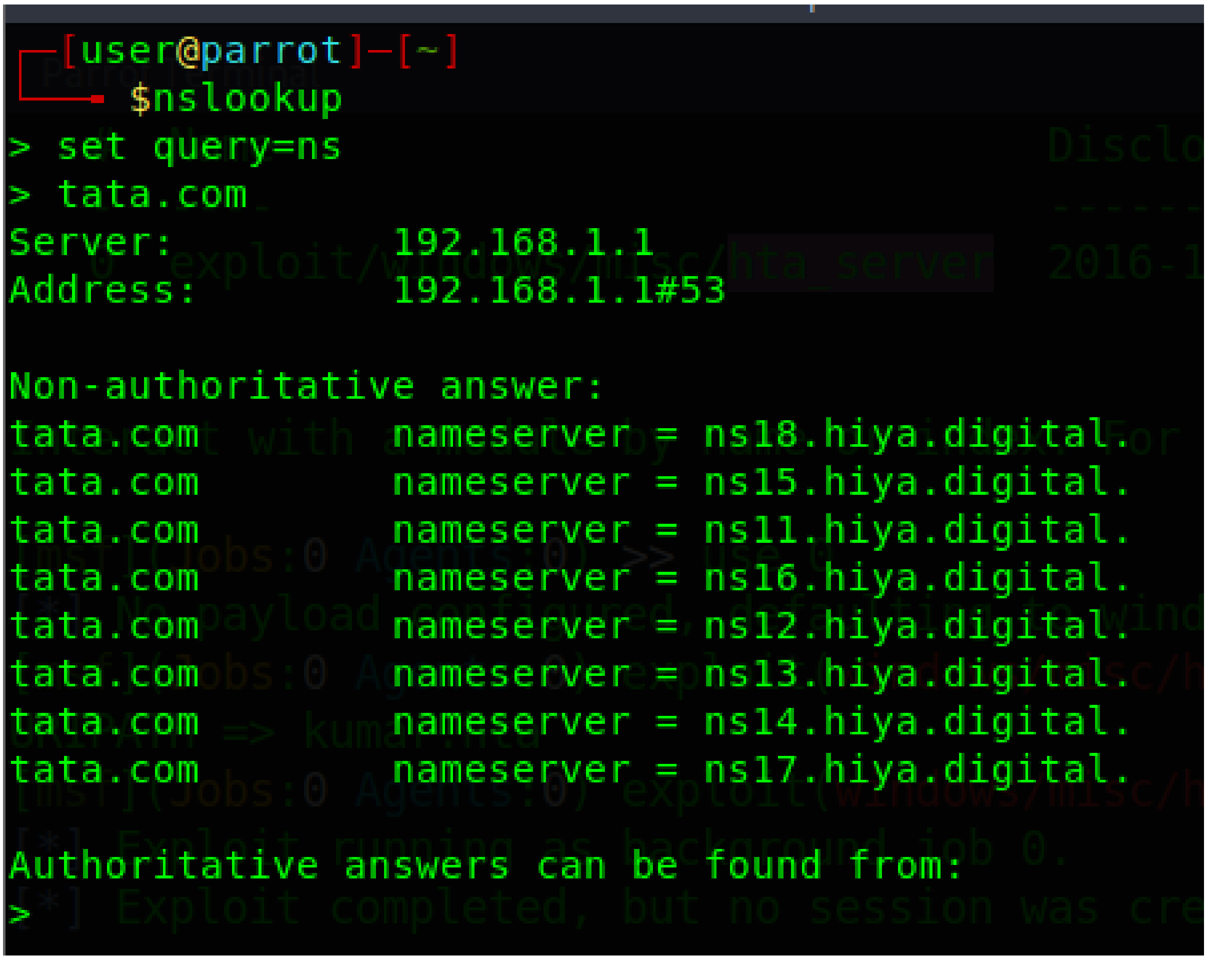
DNS Records Example

- A = IPv4 Address
- AAAA = IPv6 Address
- NS = Name Server
- TXT = Stores Text Data
- MX = Mail exchange-record
- CNAME = Common/Canonical Name
- PTR = Pointer (Used to Perform Reverse DNS Lookups)
- SOA = Start of Authority (Gives Authoritative Info)
- SRV = Service (Used for Custom Services like VoIP)

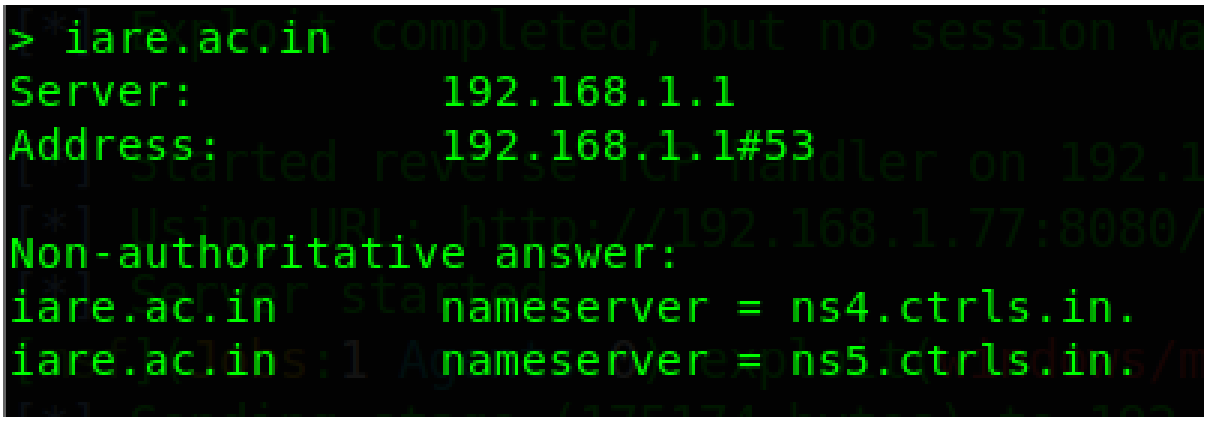
DNS Enumeration Tools

dig (Domain Information Groper): Used for detailed DNS queries and provides answer, authority, and additional sections.

nslookup: Used for quick DNS lookups and basic DNS enumeration.



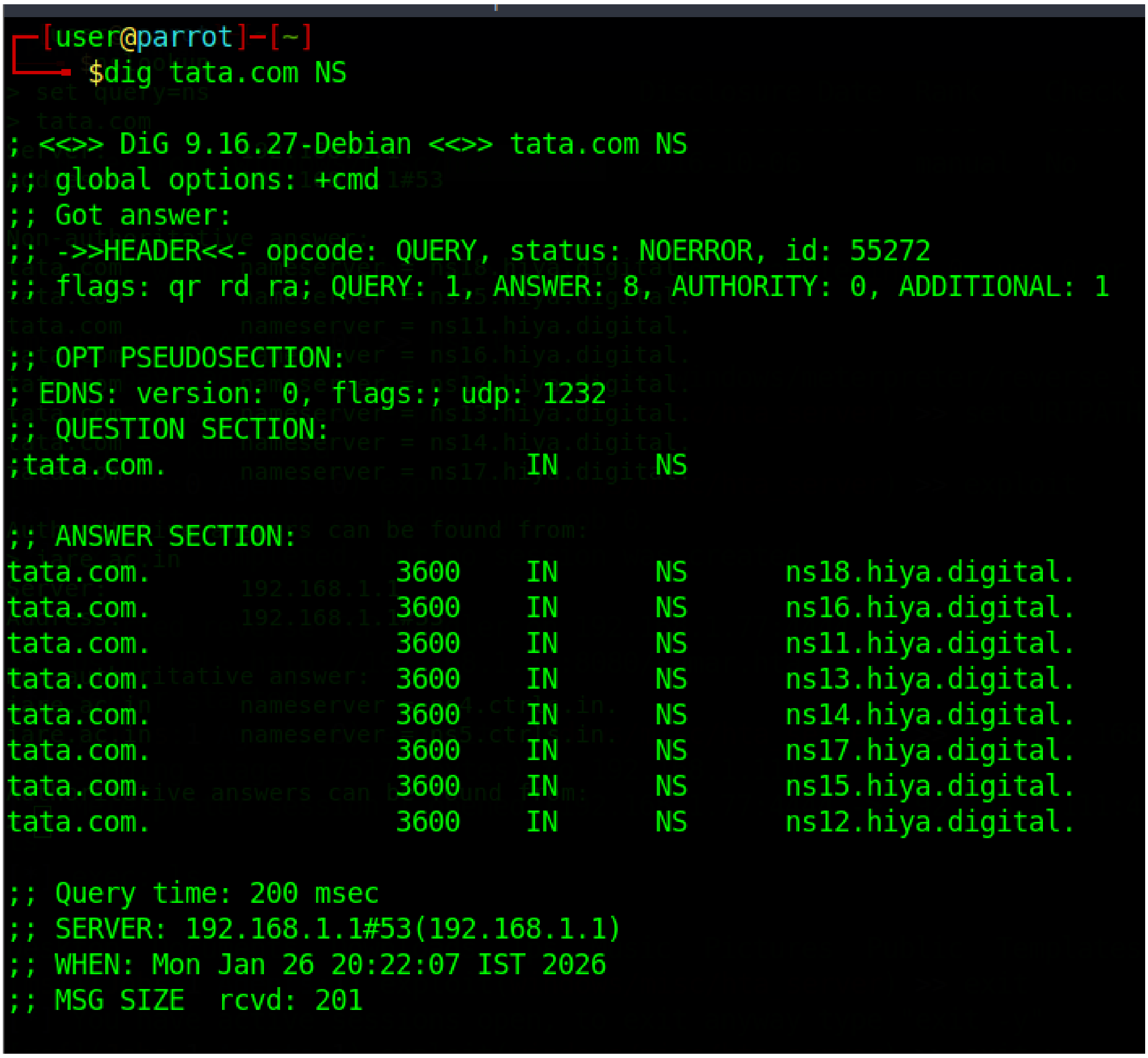
```
┌─[user@parrot]─[~]
└──╼ $nslookup
> set query=ns
> tata.com
Server:         192.168.1.1
Address:        192.168.1.1#53

Non-authoritative answer:
tata.com        nameserver = ns18.hiya.digital.
tata.com        nameserver = ns15.hiya.digital.
tata.com        nameserver = ns11.hiya.digital.
tata.com        nameserver = ns16.hiya.digital.
tata.com        nameserver = ns12.hiya.digital.
tata.com        nameserver = ns13.hiya.digital.
tata.com        nameserver = ns14.hiya.digital.
tata.com        nameserver = ns17.hiya.digital.

Authoritative answers can be found from:
>
```



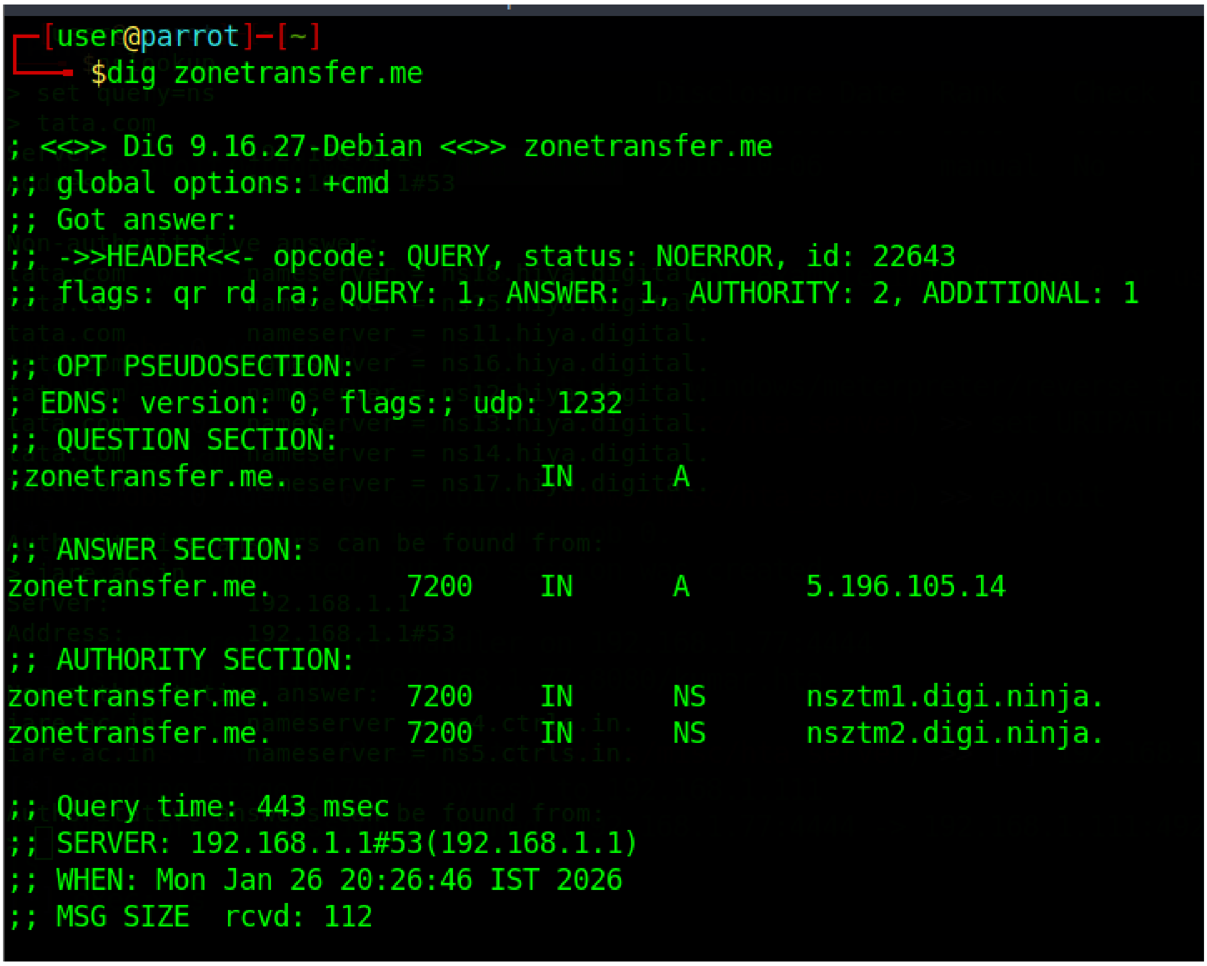
```
> iare.ac.in
Server:         192.168.1.1
Address:        192.168.1.1#53

Non-authoritative answer:
iare.ac.in      nameserver = ns4.ctrls.in.
iare.ac.in      nameserver = ns5.ctrls.in.
```

DNS Enumeration Process

1. Select target domain
2. Identify name servers
3. Query DNS records
4. Discover subdomains
5. Test zone transfer vulnerability



```
┌─[user@parrot]─[~]
└──╼ $dig tata.com NS

; <<>> DiG 9.16.27-Debian <<>> tata.com NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 55272
;; flags: qr rd ra; QUERY: 1, ANSWER: 8, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;tata.com.                      IN      NS

;; ANSWER SECTION:
tata.com.               3600    IN      NS      ns18.hiya.digital.
tata.com.               3600    IN      NS      ns16.hiya.digital.
tata.com.               3600    IN      NS      ns11.hiya.digital.
tata.com.               3600    IN      NS      ns13.hiya.digital.
tata.com.               3600    IN      NS      ns14.hiya.digital.
tata.com.               3600    IN      NS      ns17.hiya.digital.
tata.com.               3600    IN      NS      ns15.hiya.digital.
tata.com.               3600    IN      NS      ns12.hiya.digital.

;; Query time: 200 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: Mon Jan 26 20:22:07 IST 2026
;; MSG SIZE  rcvd: 201
```

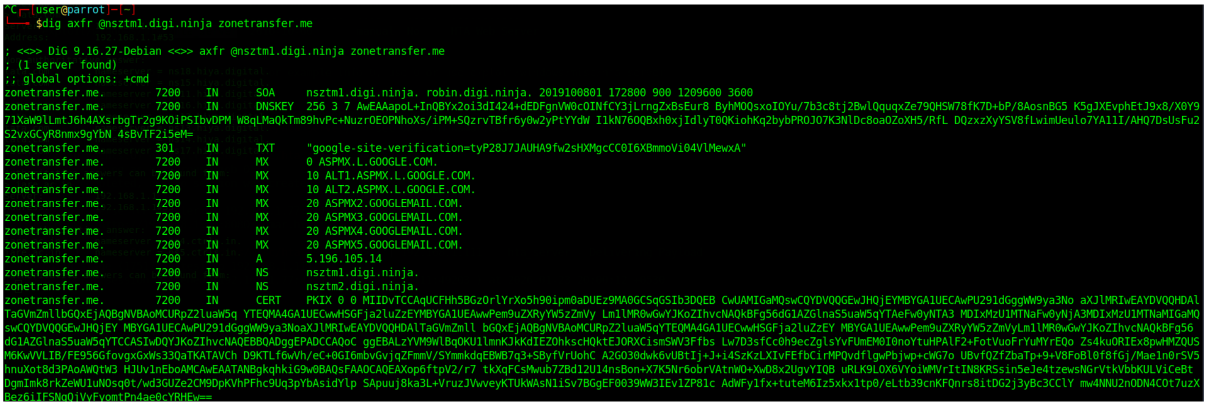


```
┌─[user@parrot]─[~]
└──╼ $dig zonetransfer.me

; <<>> DiG 9.16.27-Debian <<>> zonetransfer.me
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 22643
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;zonetransfer.me.               IN      A

;; ANSWER SECTION:
zonetransfer.me.        7200    IN      A       5.196.105.14

;; AUTHORITY SECTION:
zonetransfer.me.        7200    IN      NS      nsztm1.digi.ninja.
zonetransfer.me.        7200    IN      NS      nsztm2.digi.ninja.

;; Query time: 443 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: Mon Jan 26 20:26:46 IST 2026
;; MSG SIZE  rcvd: 112
```

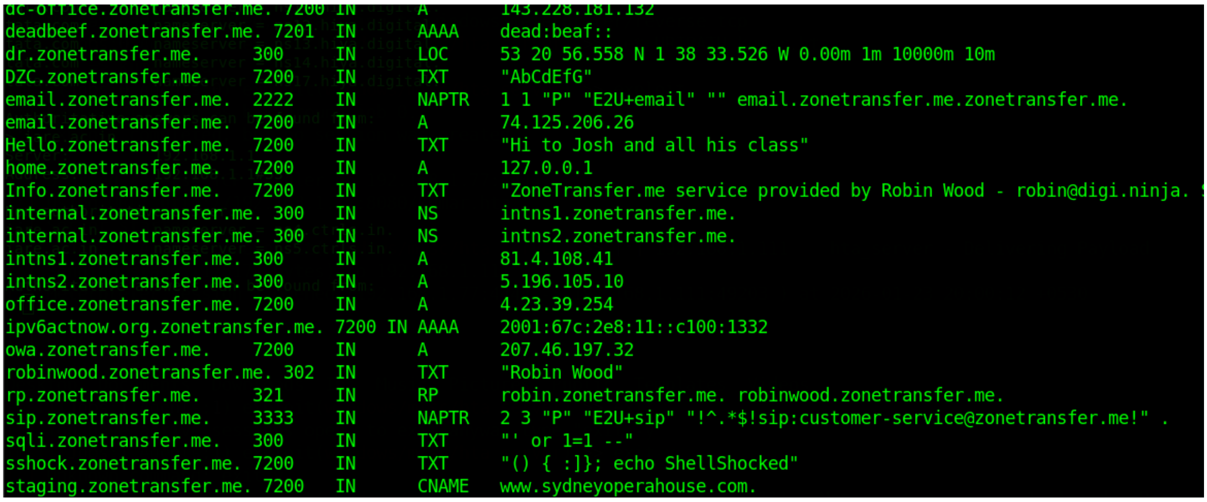
DNS Zone Transfer (AXFR)

Zone Transfer copies DNS records from one DNS server to another.

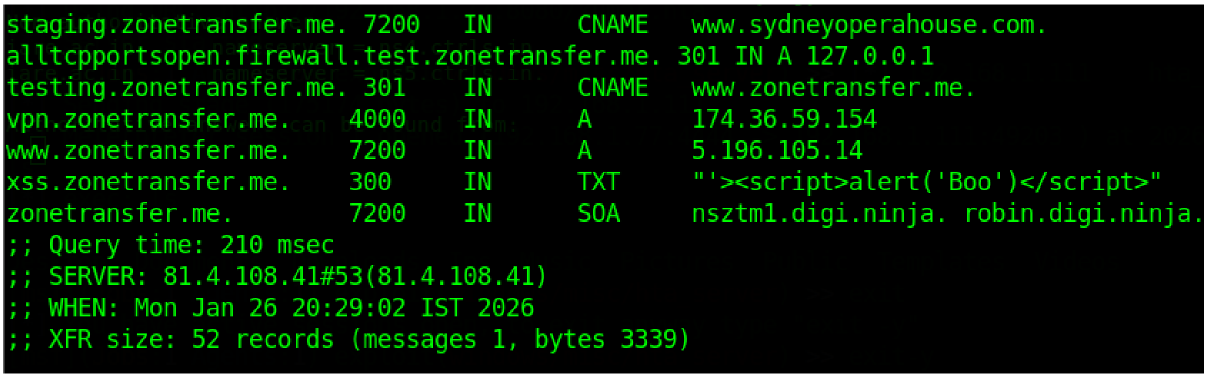
AXFR refers to a full zone transfer.



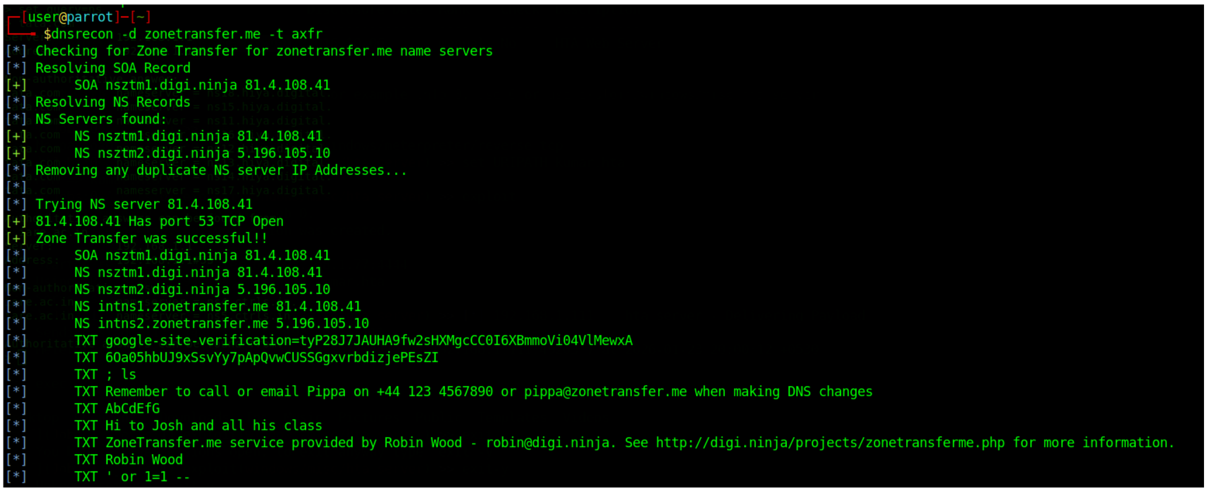
```
^C┌─[user@parrot]─[~]
└──╼ $dig axfr @nsztm1.digi.ninja zonetransfer.me

; <<>> DiG 9.16.27-Debian <<>> axfr @nsztm1.digi.ninja zonetransfer.me
; (1 server found)
;; global options: +cmd
zonetransfer.me.        7200    IN      SOA     nsztm1.digi.ninja. robin.digi.ninja. 2019100801 172800 900 1209600 3600
zonetransfer.me.        7200    IN      DNSKEY  256 3 7 AwEAAapoL+InQBYx2oi3dI424+dEDFgnVW0cOINfCY3jLrngZxBsEur8 ByhMOQsxoIOYu/7b3c8tj2BwlQquqxZe79QHSW78fK7D+bP/8AosnBG5 K5gJXEvphEtJ9x8/X0Y9
71XaW9lLmtJ6h4AXsrbgTr2g9KOiPSIbvDPM W8qLMaQkTm89hvPc+NuzrOEOPNhoXs/iPM+SQzrvTBfr6y0w2yPtYYdW I1kN76OQBxh0xjIdlyT0QKiohKq2bybPROJO7K3NlDc8oaOZoXH5/RfL DQzxzXyYSV8fLwimUeulo7YA11I/AHQ7DsUsFu2
S2vxGCyR8nmx9gYbN 4sBvTF2i5eM=
zonetransfer.me.        301     IN      TXT     "google-site-verification=tyP28J7JAUHA9fw2sHXMgcCC0I6XBmmoVi04VlMewxA"
zonetransfer.me.        7200    IN      MX      0 ASPMX.L.GOOGLE.COM.
zonetransfer.me.        7200    IN      MX      10 ALT1.ASPMX.L.GOOGLE.COM.
zonetransfer.me.        7200    IN      MX      10 ALT2.ASPMX.L.GOOGLE.COM.
zonetransfer.me.        7200    IN      MX      20 ASPMX2.GOOGLEMAIL.COM.
zonetransfer.me.        7200    IN      MX      20 ASPMX3.GOOGLEMAIL.COM.
zonetransfer.me.        7200    IN      MX      20 ASPMX4.GOOGLEMAIL.COM.
zonetransfer.me.        7200    IN      MX      20 ASPMX5.GOOGLEMAIL.COM.
zonetransfer.me.        7200    IN      A       5.196.105.14
zonetransfer.me.        7200    IN      NS      nsztm1.digi.ninja.
zonetransfer.me.        7200    IN      NS      nsztm2.digi.ninja.
zonetransfer.me.        7200    IN      CERT    PKIX 0 0 MIIDvTCCAqUCFHh5BGzOrlYrXo5h90ipm0aDUEz9MA0GCSqGSIb3DQEB CwUAMIGaMQswCQYDVQQGEwJHQjEYMBYGA1UECAwPU291dGggWW9ya3No aXJlMRIwEAYDVQQHDAl
TaGVmZmllbGQxEjAQBgNVBAoMCURpZ2luaW5q YTEQMA4GA1UECwwHSGFja2luZzEYMBYGA1UEAwwPem9uZXRyYW5zZmVy Lm1lMR0wGwYJKoZIhvcNAQkBFg56dG1AZGlnaS5uaW5qYTAeFw0yNTA3 MDIxMzU1MTNaFw0yNjA3MDIxMzU1MTNaMIGaMQ
swCQYDVQQGEwJHQjEY MBYGA1UECAwPU291dGggWW9ya3NoaXJlMRIwEAYDVQQHDAlTaGVmZmll bGQxEjAQBgNVBAoMCURpZ2luaW5qYTEQMA4GA1UECwwHSGFja2luZzEY MBYGA1UEAwwPem9uZXRyYW5zZmVyLm1lMR0wGwYJKoZIhvcNAQkBFg56
dG1AZGlnaS5uaW5qYTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoC ggEBALzYVM9WlBqOKU1lmnKJkKdIEZOhkscHQktEJORXCismSWV3Ffbs Lw7D3sfCc0h9ecZglsYvFUmEM0I0noYtuHPAlF2+FotVuoFrYuMYrEQo Zs4kuORIEx8pwHMZQUS
M6KwVVLIB/FE956GfovgxGxWs33QaTKATAVCh D9KTLf6wVh/eC+0GI6mbvGvjqZFmmV/SYmmkdqEBWB7q3+SByfVrUohC A2GO30dwk6vUBtIj+J+i4SzKzLXIvFEfbCirMPQvdflgwPbjwp+cWG7o UBvfQZfZbaTp+9+V8FoBl0f8fGj/Mae1n0rSV5
hnuXot8d3PAoAWQtW3 HJUv1nEboAMCAwEAATANBgkqhkiG9w0BAQsFAAOCAQEAXop6ftpV2/r7 tkXqFCsMwub7ZBd12U14nsBon+X7K5Nr6obrVAtnWO+XwD8x2UgvYIQB uRLK9LOX6VYoiWMVrItIN8KRSsin5eJe4tzewsNGrVtkVbbKULViCeBt
DgmImk8rkZeWU1uNOsq0t/wd3GUZe2CM9DpKVhPFhc9Uq3pYbAsidYlp SApuuj8ka3L+VruzJVwveyKTUkWAsN1iSv7BGgEF0039WW3IEv1ZP81c AdWFy1fx+tuteM6Iz5xkx1tp0/eLtb39cnKFQnrs8itDG2j3yBc3CClY mw4NNU2nODN4COt7uzX
Bez6iIFSNgQjVyFyomtPn4ae0cYRHEw==
```



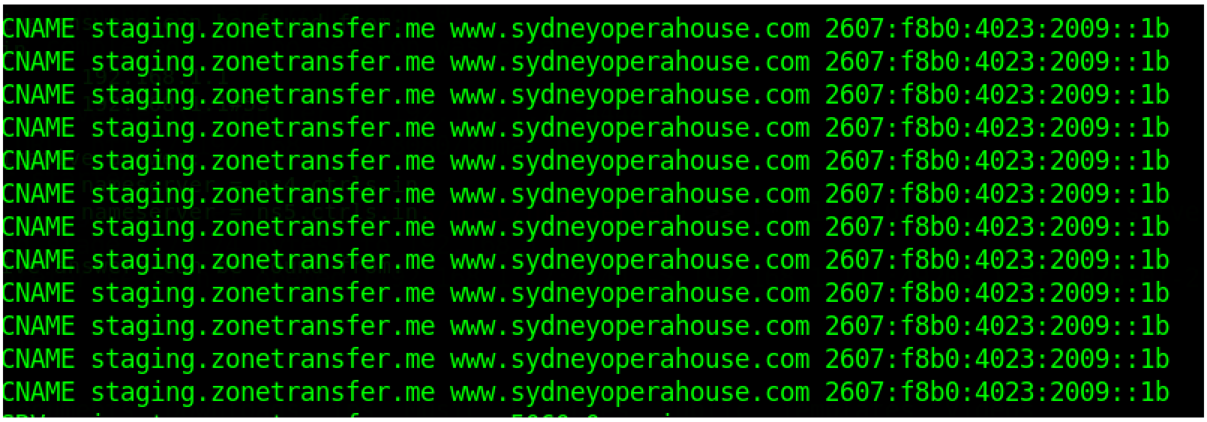
```
dc-office.zonetransfer.me. 7200 IN     A      143.228.181.132
deadbeef.zonetransfer.me. 7201  IN     AAAA   dead:beaf::
dr.zonetransfer.me.       300   IN     LOC    53 20 56.558 N 1 38 33.526 W 0.00m 1m 10000m 10m
DZC.zonetransfer.me.      7200  IN     TXT    "AbCdEfG"
email.zonetransfer.me.    2222  IN     NAPTR  1 1 "P" "E2U+email" "" email.zonetransfer.me.zonetransfer.me.
email.zonetransfer.me.    7200  IN     A      74.125.206.26
Hello.zonetransfer.me.    7200  IN     TXT    "Hi to Josh and all his class"
home.zonetransfer.me.     7200  IN     A      127.0.0.1
Info.zonetransfer.me.     7200  IN     TXT    "ZoneTransfer.me service provided by Robin Wood - robin@digi.ninja.
internal.zonetransfer.me. 300   IN     NS     intns1.zonetransfer.me.
internal.zonetransfer.me. 300   IN     NS     intns2.zonetransfer.me.
intns1.zonetransfer.me. 300     IN     A      81.4.108.41
intns2.zonetransfer.me. 300     IN     A      5.196.105.10
office.zonetransfer.me. 7200    IN     A      4.23.39.254
ipv6actnow.org.zonetransfer.me. 7200 IN AAAA  2001:67c:2e8:11::c100:1332
owa.zonetransfer.me.      7200  IN     A      207.46.197.32
robinwood.zonetransfer.me. 302  IN     TXT    "Robin Wood"
rp.zonetransfer.me.       321   IN     RP     robin.zonetransfer.me. robinwood.zonetransfer.me.
sip.zonetransfer.me.      3333  IN     NAPTR  2 3 "P" "E2U+sip" "!^.*$!sip:customer-service@zonetransfer.me!" .
sqli.zonetransfer.me.     300   IN     TXT    "' or 1=1 --"
sshock.zonetransfer.me. 7200    IN     TXT    "() { :]}; echo ShellShocked"
staging.zonetransfer.me. 7200   IN     CNAME  www.sydneyoperahouse.com.
```



```
staging.zonetransfer.me. 7200   IN      CNAME   www.sydneyoperahouse.com.
alltcpportsopen.firewall.test.zonetransfer.me. 301 IN A 127.0.0.1
testing.zonetransfer.me. 301    IN      CNAME   www.zonetransfer.me.
vpn.zonetransfer.me.     4000   IN      A       174.36.59.154
www.zonetransfer.me.     7200   IN      A       5.196.105.14
xss.zonetransfer.me.     300    IN      TXT     "'><script>alert('Boo')</script>"
zonetransfer.me.         7200   IN      SOA     nsztm1.digi.ninja. robin.digi.ninja.
;; Query time: 210 msec
;; SERVER: 81.4.108.41#53(81.4.108.41)
;; WHEN: Mon Jan 26 20:29:02 IST 2026
;; XFR size: 52 records (messages 1, bytes 3339)
```



```
┌─[user@parrot]─[~]
└──╼ $dnsrecon -d zonetransfer.me -t axfr
[*] Checking for Zone Transfer for zonetransfer.me name servers
[*] Resolving SOA Record
[+]      SOA nsztm1.digi.ninja 81.4.108.41
[*] Resolving NS Records
[*] NS Servers found:
[+]      NS nsztm1.digi.ninja 81.4.108.41
[+]      NS nsztm2.digi.ninja 5.196.105.10
[*] Removing any duplicate NS server IP Addresses...
[*]
[*] Trying NS server 81.4.108.41
[+] 81.4.108.41 Has port 53 TCP Open
[+] Zone Transfer was successful!!
[*]      SOA nsztm1.digi.ninja 81.4.108.41
[*]      NS nsztm1.digi.ninja 81.4.108.41
[*]      NS nsztm2.digi.ninja 5.196.105.10
[*]      NS intns1.zonetransfer.me 81.4.108.41
[*]      NS intns2.zonetransfer.me 5.196.105.10
[*]      TXT google-site-verification=tyP28J7JAUHA9fw2sHXMgcCC0I6XBmmoVi04VlMewxA
[*]      TXT 6Oa05hbUJ9xSsvYy7pApQvwCUSSGgxvrbdizjePEsZI
[*]      TXT ; ls
[*]      TXT Remember to call or email Pippa on +44 123 4567890 or pippa@zonetransfer.me when making DNS changes
[*]      TXT AbCdEfG
[*]      TXT Hi to Josh and all his class
[*]      TXT ZoneTransfer.me service provided by Robin Wood - robin@digi.ninja. See http://digi.ninja/projects/zonetransferme.php for more information.
[*]      TXT Robin Wood
[*]      TXT ' or 1=1 --
```



```
CNAME staging.zonetransfer.me www.sydneyoperahouse.com 2607:f8b0:4023:2009::1b
CNAME staging.zonetransfer.me www.sydneyoperahouse.com 2607:f8b0:4023:2009::1b
CNAME staging.zonetransfer.me www.sydneyoperahouse.com 2607:f8b0:4023:2009::1b
CNAME staging.zonetransfer.me www.sydneyoperahouse.com 2607:f8b0:4023:2009::1b
CNAME staging.zonetransfer.me www.sydneyoperahouse.com 2607:f8b0:4023:2009::1b
CNAME staging.zonetransfer.me www.sydneyoperahouse.com 2607:f8b0:4023:2009::1b
CNAME staging.zonetransfer.me www.sydneyoperahouse.com 2607:f8b0:4023:2009::1b
CNAME staging.zonetransfer.me www.sydneyoperahouse.com 2607:f8b0:4023:2009::1b
CNAME staging.zonetransfer.me www.sydneyoperahouse.com 2607:f8b0:4023:2009::1b
CNAME staging.zonetransfer.me www.sydneyoperahouse.com 2607:f8b0:4023:2009::1b
CNAME staging.zonetransfer.me www.sydneyoperahouse.com 2607:f8b0:4023:2009::1b
CNAME staging.zonetransfer.me www.sydneyoperahouse.com 2607:f8b0:4023:2009::1b
```

Risk:

- Disclosure of all subdomains
- Internal hostnames
- Network structure

- Mail servers

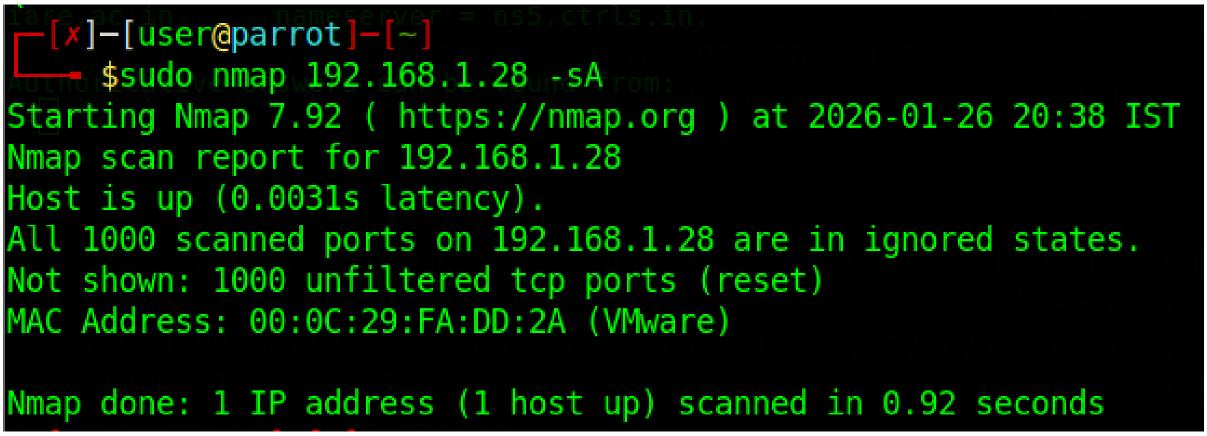
Prevention:

- Allow zone transfers only to trusted IPs
- Disable public AXFR
- Use TSIG authentication

Advanced DIG Commands

Dig can query specific DNS servers, return short output, and trace DNS resolution paths from root to authoritative servers.

Nmap & DNS Enumeration



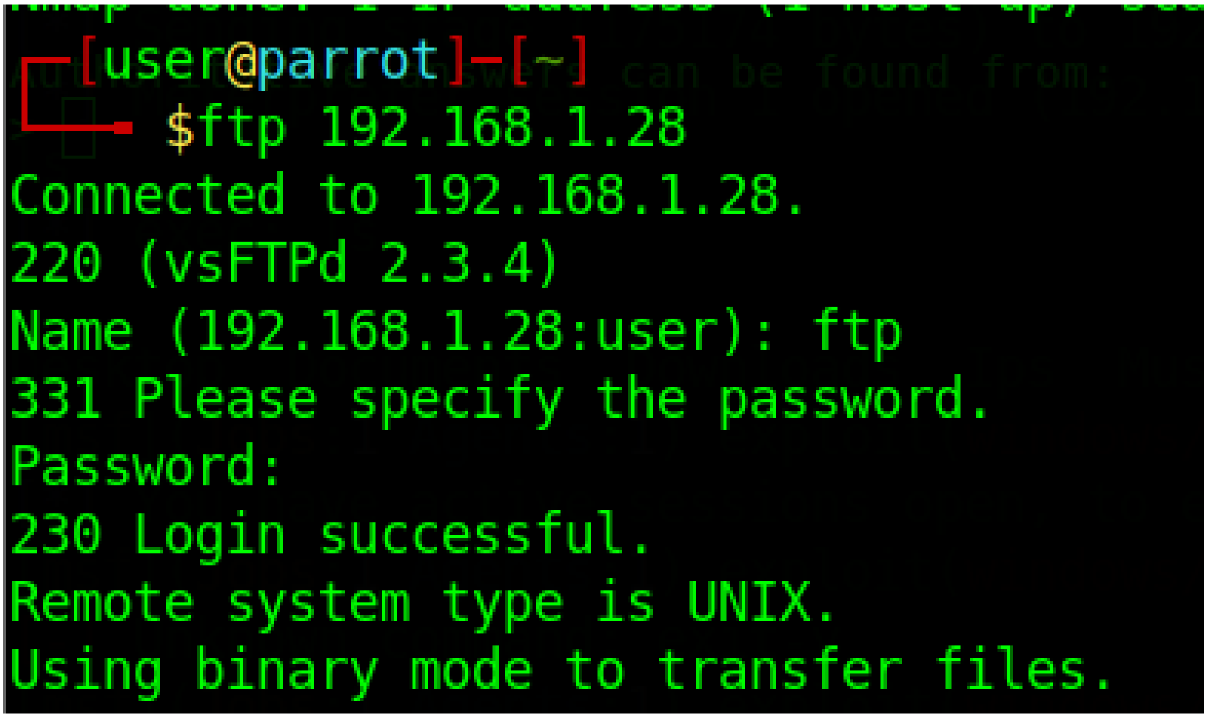
```
┌─[✗]─[user@parrot]─[~]
└──╼ $sudo nmap 192.168.1.28 -sA
Starting Nmap 7.92 ( https://nmap.org ) at 2026-01-26 20:38 IST
Nmap scan report for 192.168.1.28
Host is up (0.0031s latency).
All 1000 scanned ports on 192.168.1.28 are in ignored states.
Not shown: 1000 unfiltered tcp ports (reset)
MAC Address: 00:0C:29:FA:DD:2A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.92 seconds
```

DNS operates on Port 53.

UDP 53 – Normal DNS queries
TCP 53 – Zone transfer and large DNS responses

Nmap can be used for host discovery, firewall detection, and DNS port scanning.

FTP Enumeration Basics



```
┌─[user@parrot]─[~]
└──╼ $ftp 192.168.1.28
Connected to 192.168.1.28.
220 (vsFTPd 2.3.4)
Name (192.168.1.28:user): ftp
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
```

FTP (File Transfer Protocol) allows file transfer between client and server.

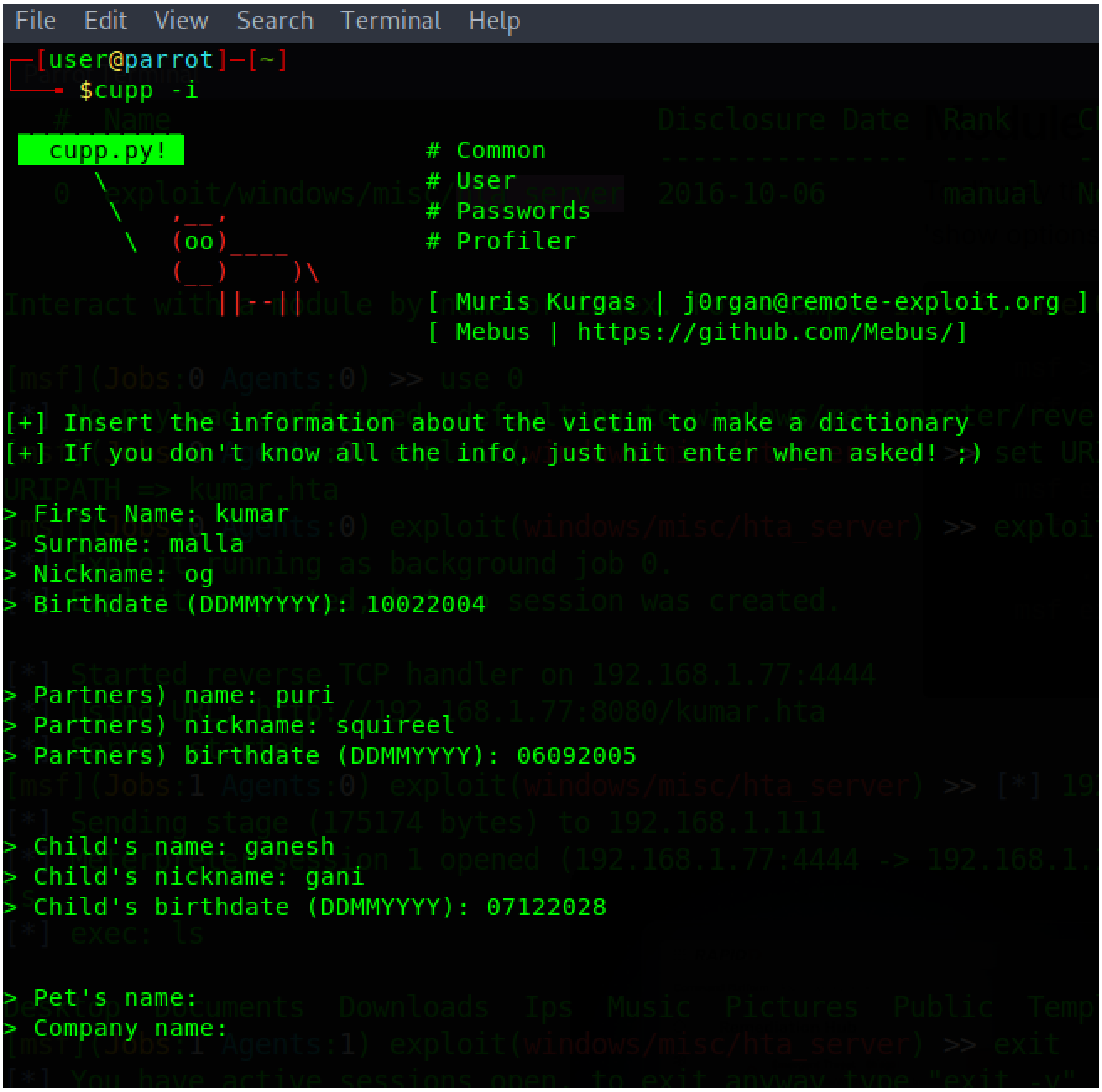
FTP Ports:

- TCP 21 – Control channel
- TCP 20 – Data channel

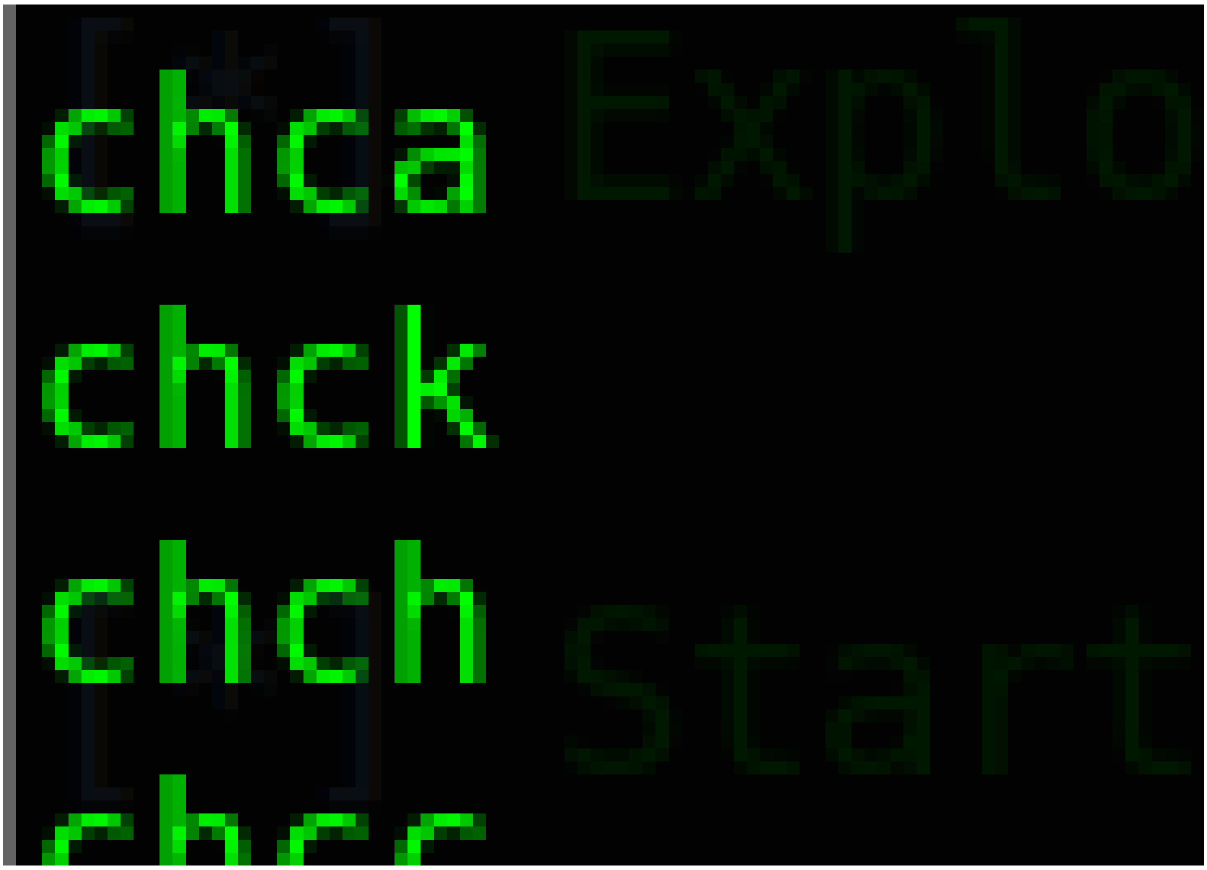
FTP is insecure because credentials are sent in plain text.

Password Attacks

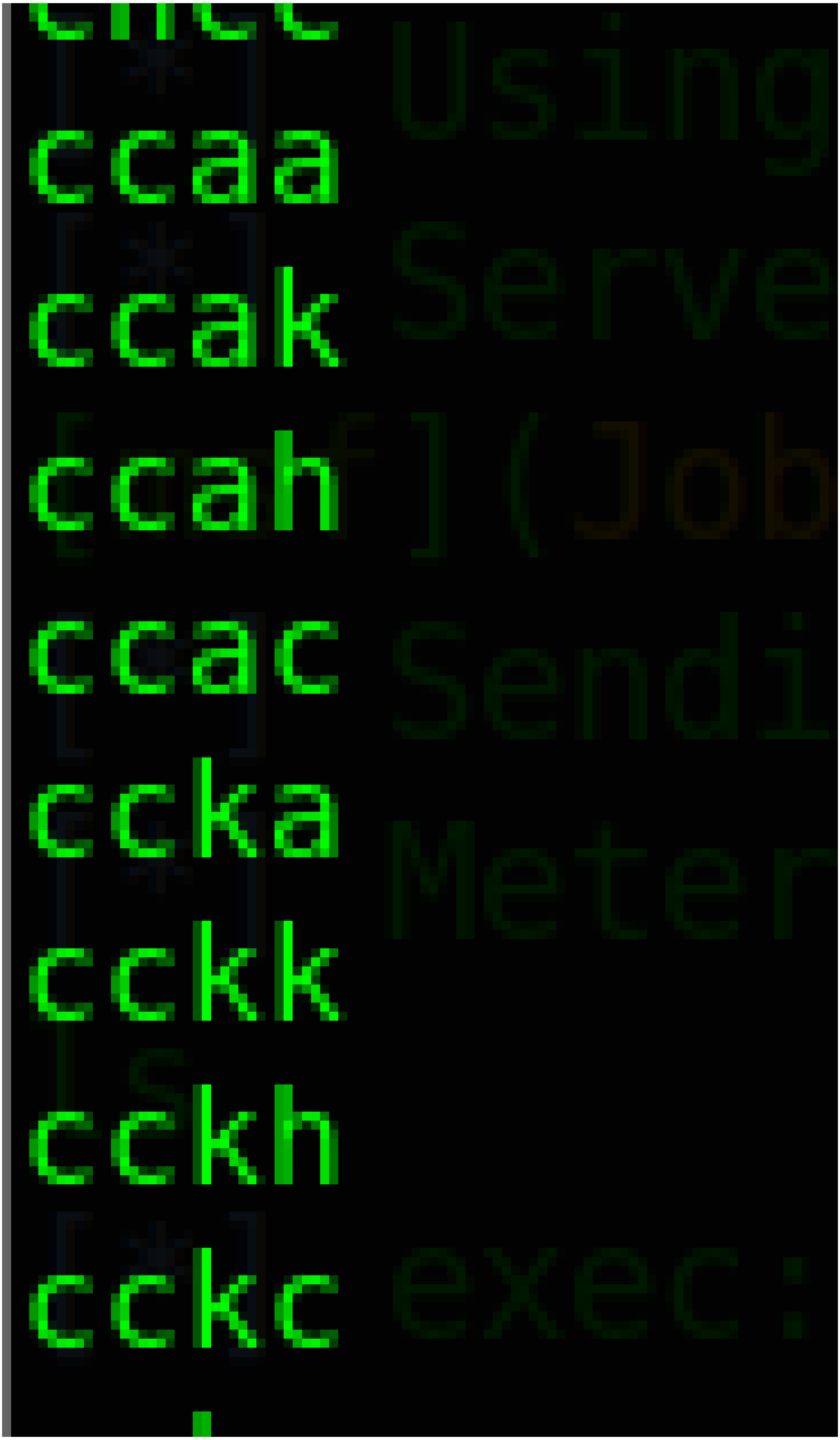
Dictionary Attack: Uses predefined wordlists such as admin, root, and password.



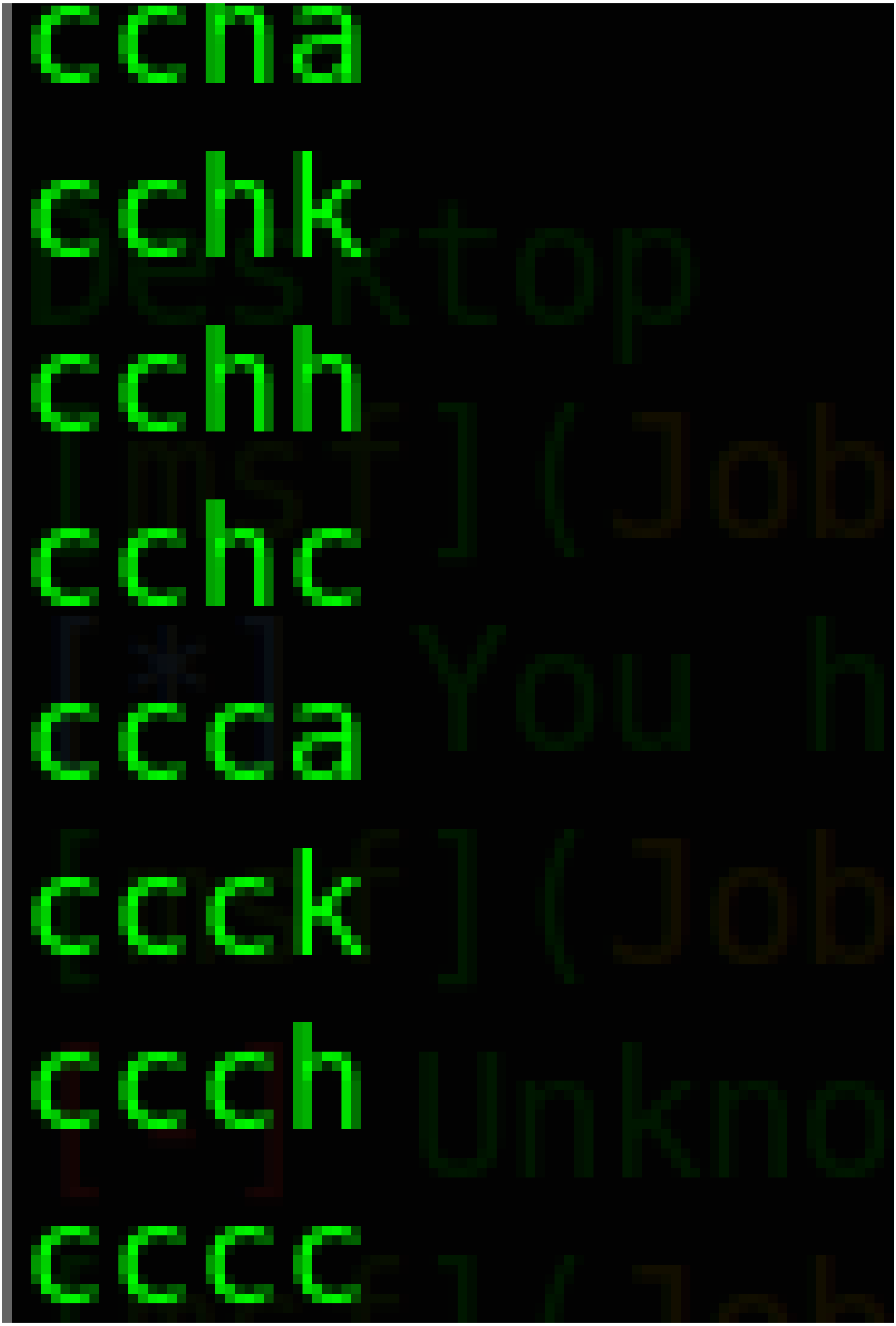
```
┌─[user@parrot]─[~]
└──╼ $cupp -i
 ___________
   cupp.py!                 # Common
      \                     # User
       \   ,__,             # Passwords
        \  (oo)____         # Profiler
           (__)    )\
              ||--||        [ Muris Kurgas | j0rgan@remote-exploit.org ]
                            [ Mebus | https://github.com/Mebus/]


[+] Insert the information about the victim to make a dictionary
[+] If you don't know all the info, just hit enter when asked! ;)

> First Name: kumar
> Surname: malla
> Nickname: og
> Birthdate (DDMMYYYY): 10022004


> Partners) name: puri
> Partners) nickname: squireel
> Partners) birthdate (DDMMYYYY): 06092005


> Child's name: ganesh
> Child's nickname: gani
> Child's birthdate (DDMMYYYY): 07122028


> Pet's name:
> Company name:
```



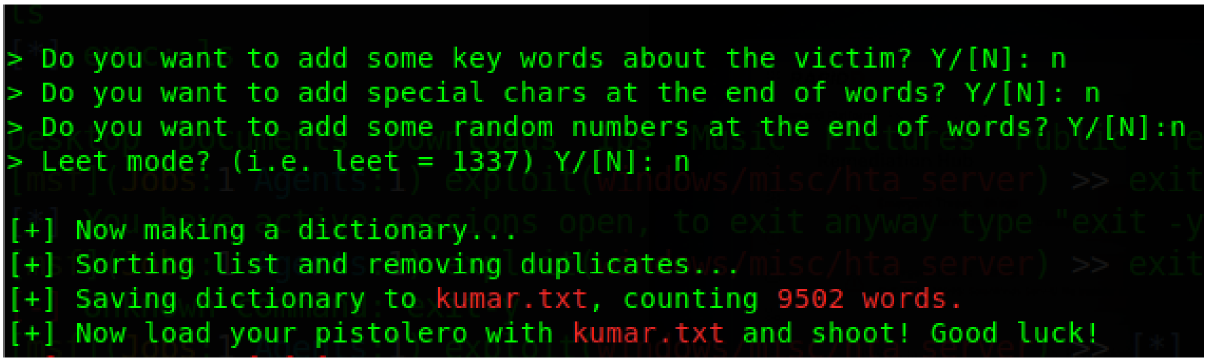
```
chca
chck
chch
chcr
```



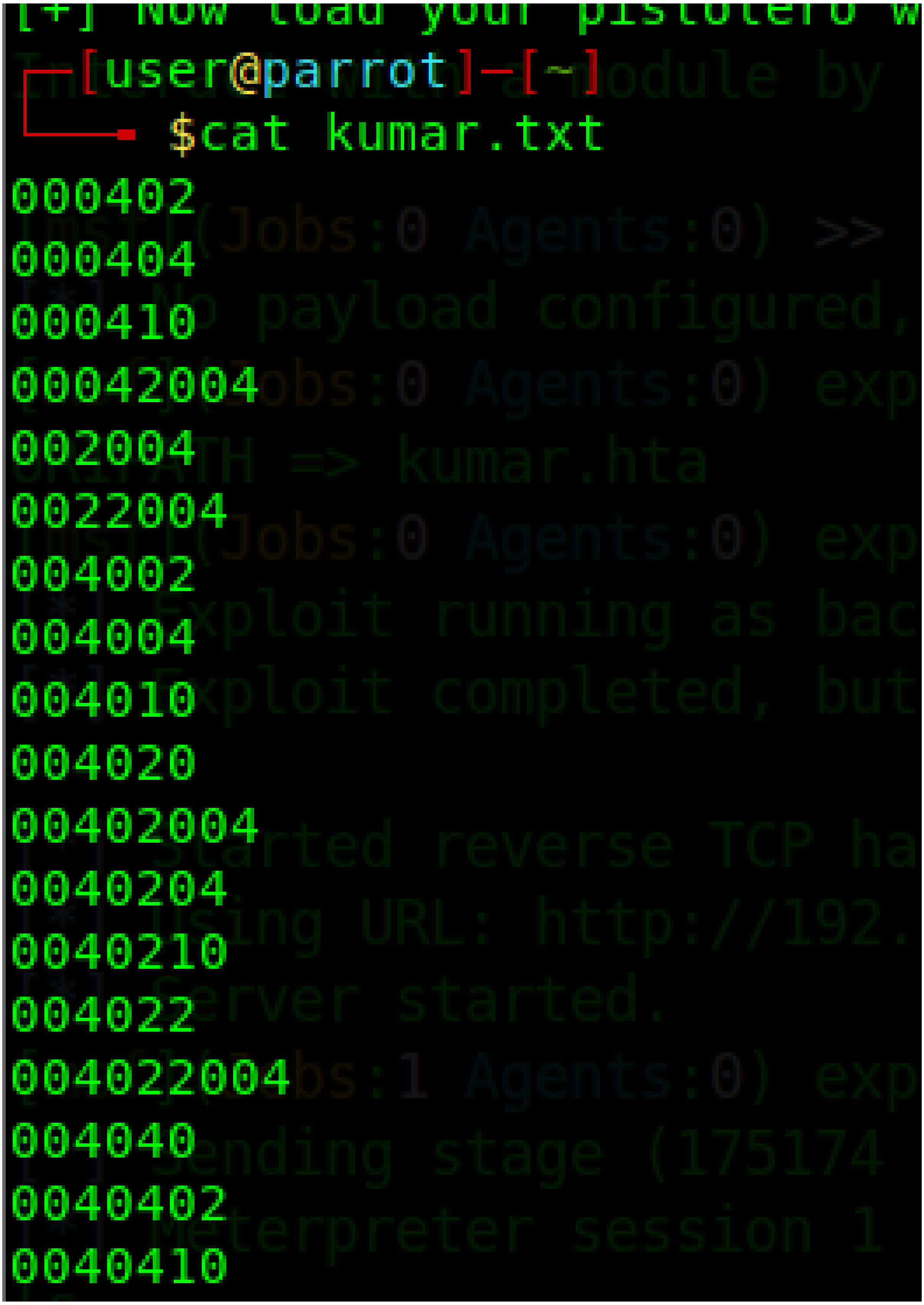
```
ccaa Using
ccak Serve
ccah ](Job
ccac Sendi
ccka Meter
cckk
cckh
cckc exec:
```



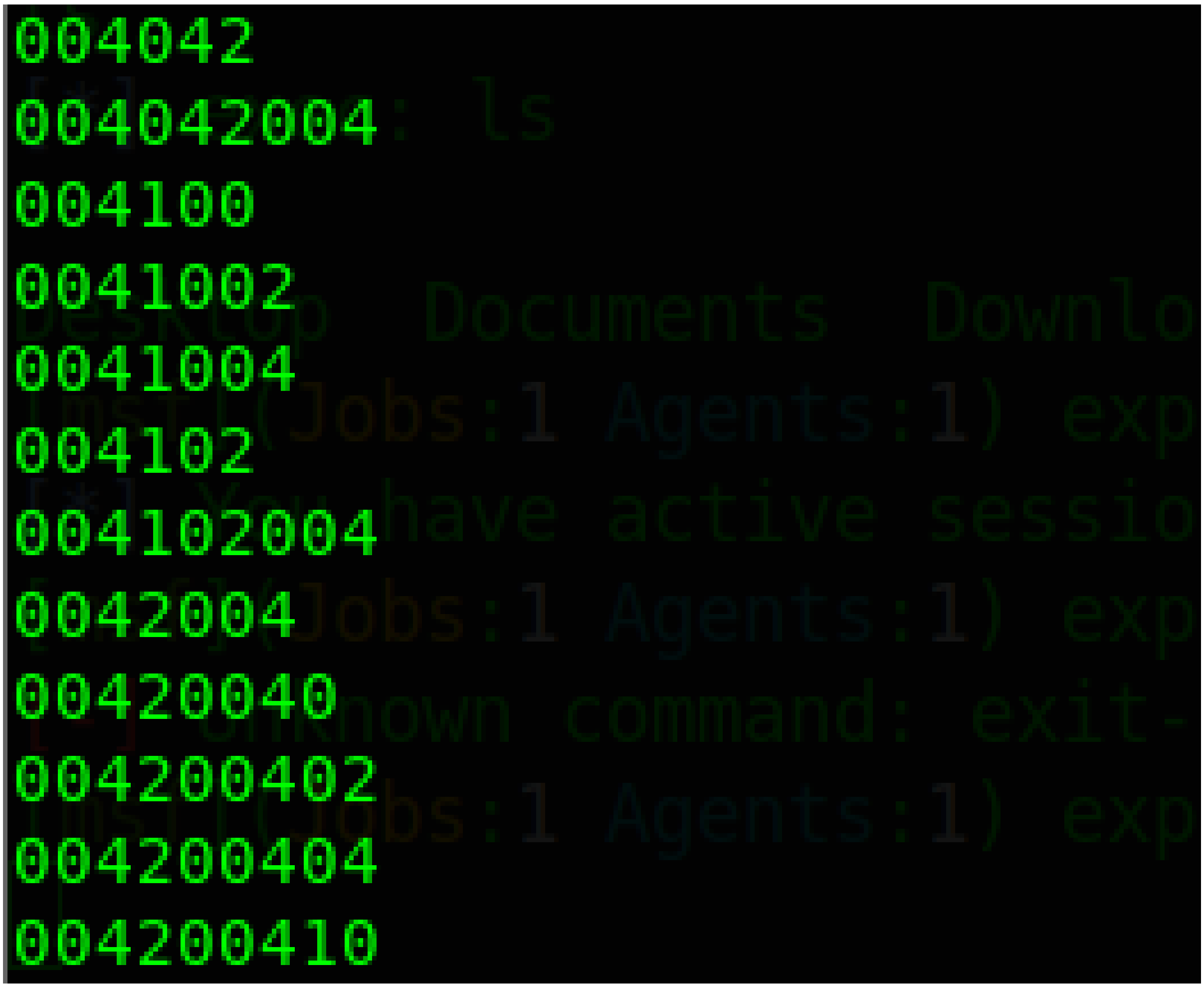
```
ccha
cchk
cchh
cchc
ccca
ccck
ccch
cccc
```



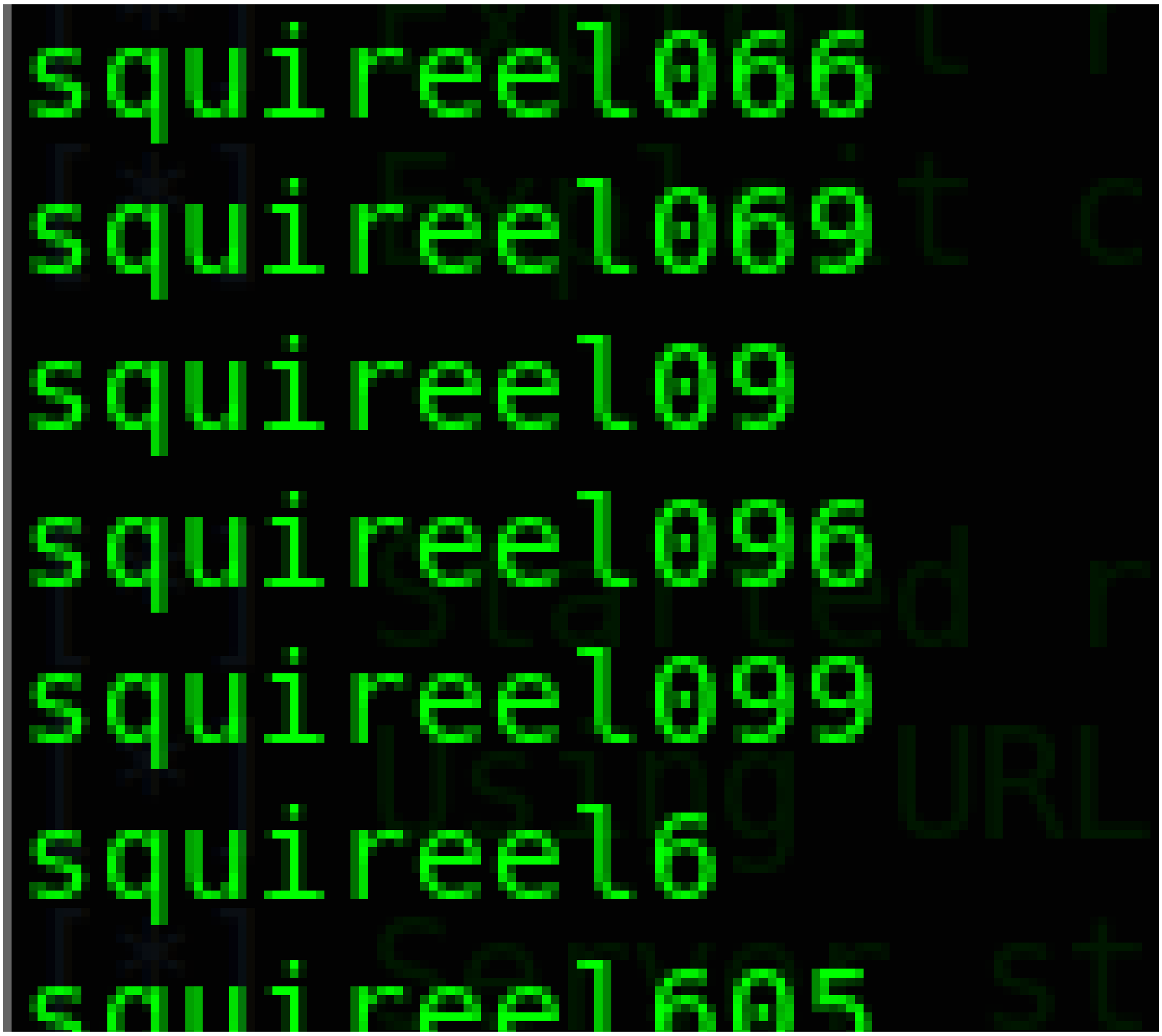
```
> Do you want to add some key words about the victim? Y/[N]: n
> Do you want to add special chars at the end of words? Y/[N]: n
> Do you want to add some random numbers at the end of words? Y/[N]:n
> Leet mode? (i.e. leet = 1337) Y/[N]: n

[+] Now making a dictionary...
[+] Sorting list and removing duplicates...
[+] Saving dictionary to kumar.txt, counting 9502 words.
[+] Now load your pistolero with kumar.txt and shoot! Good luck!
```



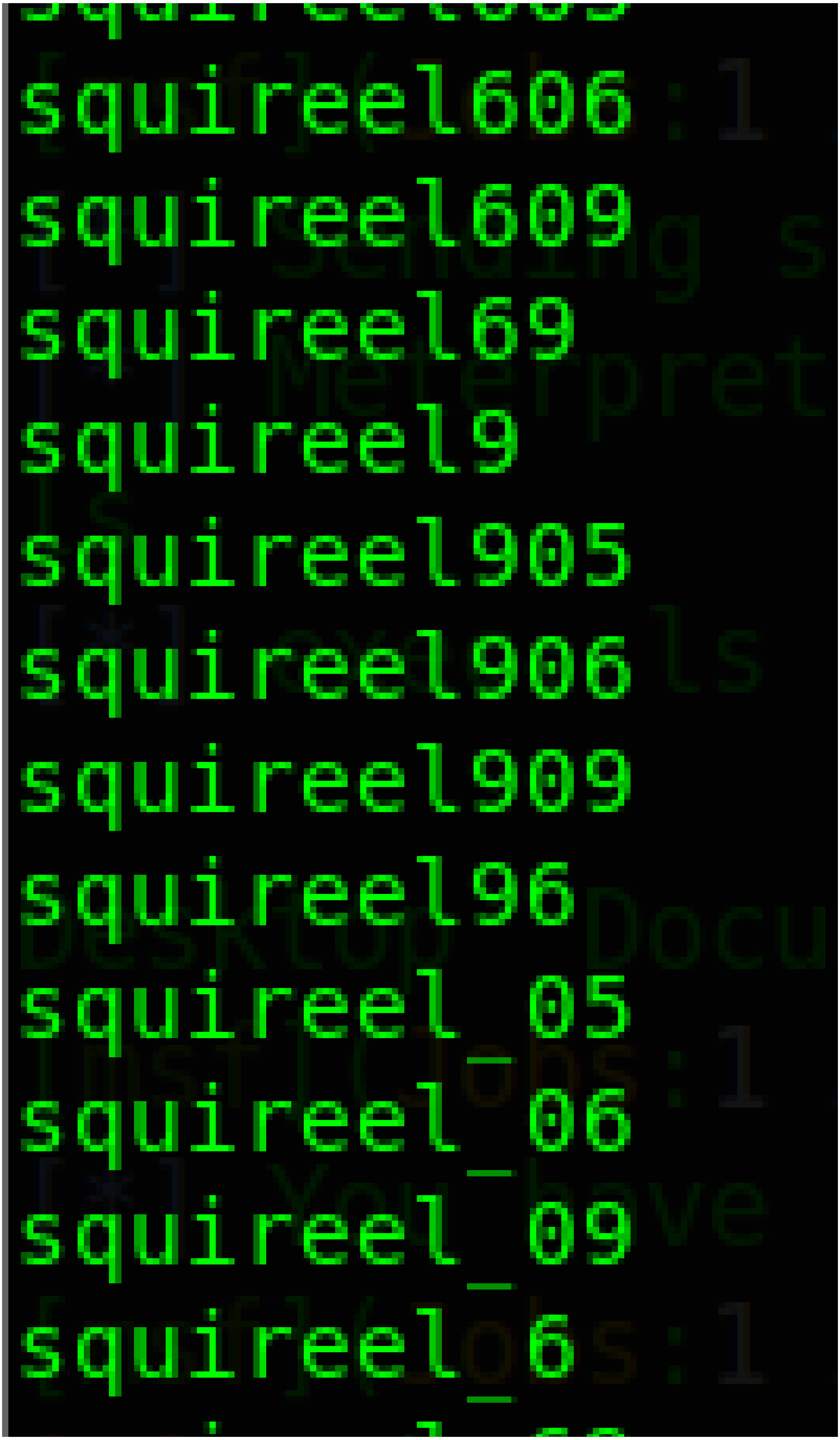
```
[+] Now load your pistolero w
┌─[user@parrot]─[~]
└──╼ $cat kumar.txt
000402
000404
000410
00042004
002004
0022004
004002
004004
004010
004020
00402004
0040204
0040210
004022
004022004
004040
0040402
0040410
```



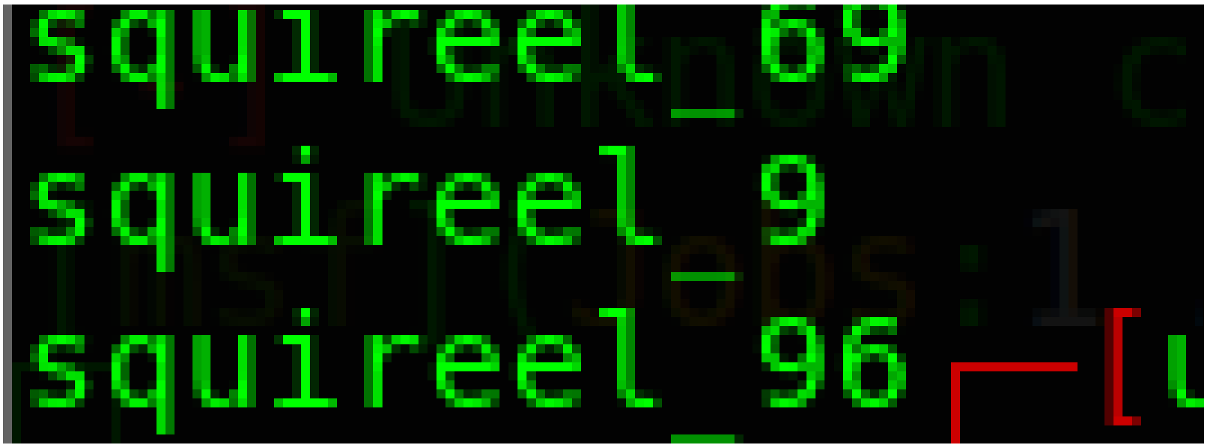
```
004042
004042004
004100
0041002
0041004
004102
004102004
0042004
00420040
004200402
004200404
004200410
```



```
squireel066
squireel069
squireel09
squireel096
squireel099
squireel6
squireel605
```



```
squireel606
squireel609
squireel69
squireel9
squireel905
squireel906
squireel909
squireel96
squireel_05
squireel_06
squireel_09
squireel_6
```



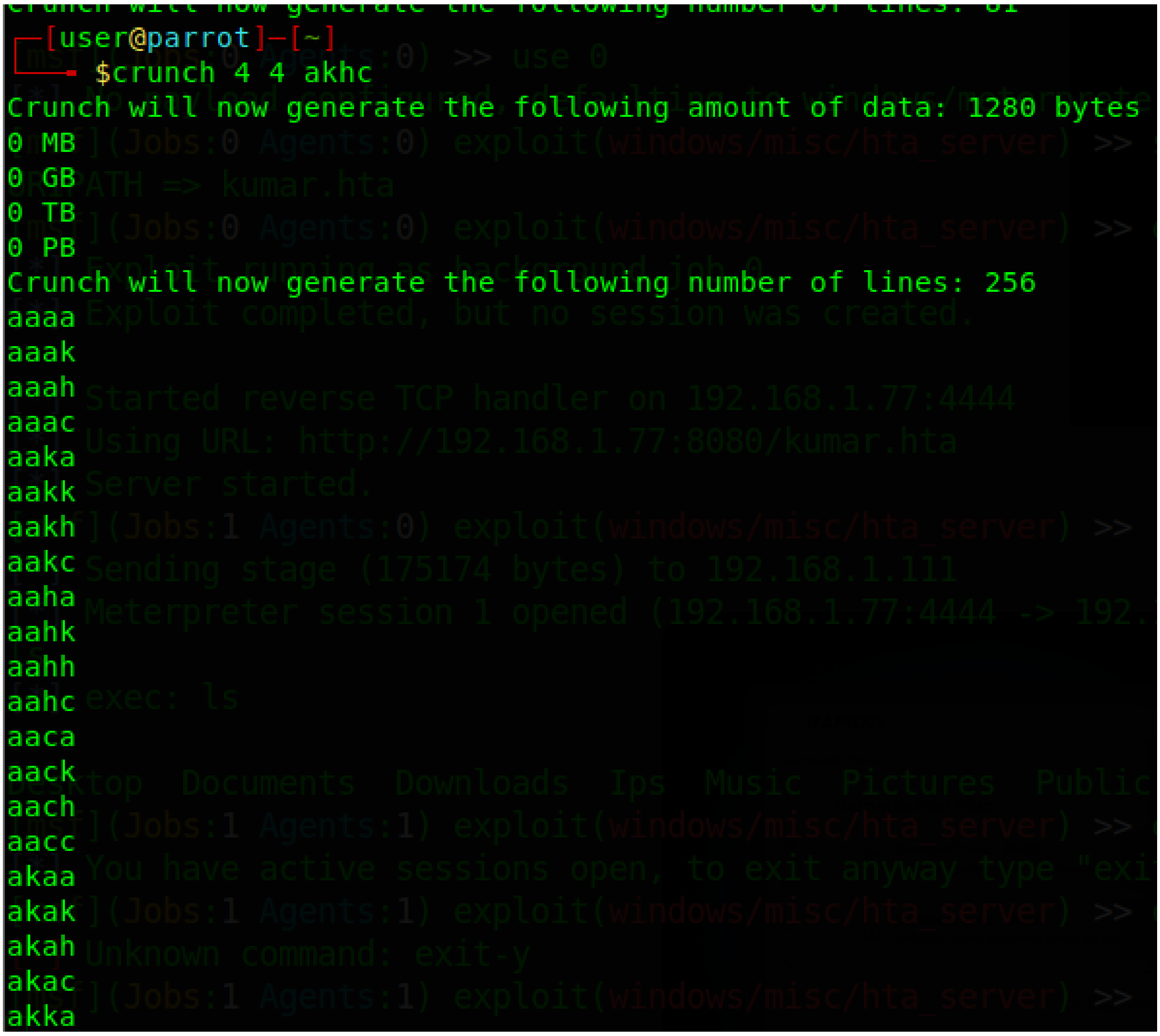
```
squireel_69
squireel_9
squireel_96 ┌─[u
```

Brute Force Attack: Attempts all possible combinations and is very slow for strong passwords.

Hybrid Attack: Combines dictionary words with numbers or symbols such as admin123 or root@2026.

Password List Generation (Crunch)

Crunch is used to generate custom password lists based on defined character sets and length.



```
Crunch will now generate the following number of lines: 81
┌─[user@parrot]─[~]
└──╼ $crunch 4 4 akhc
Crunch will now generate the following amount of data: 1280 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 256
aaaa
aaak
aaah
aaac
aaka
aakk
aakh
aakc
aaha
aahk
aahh
aahc
aaca
aack
aach
aacc
akaa
akak
akah
akac
akka
```

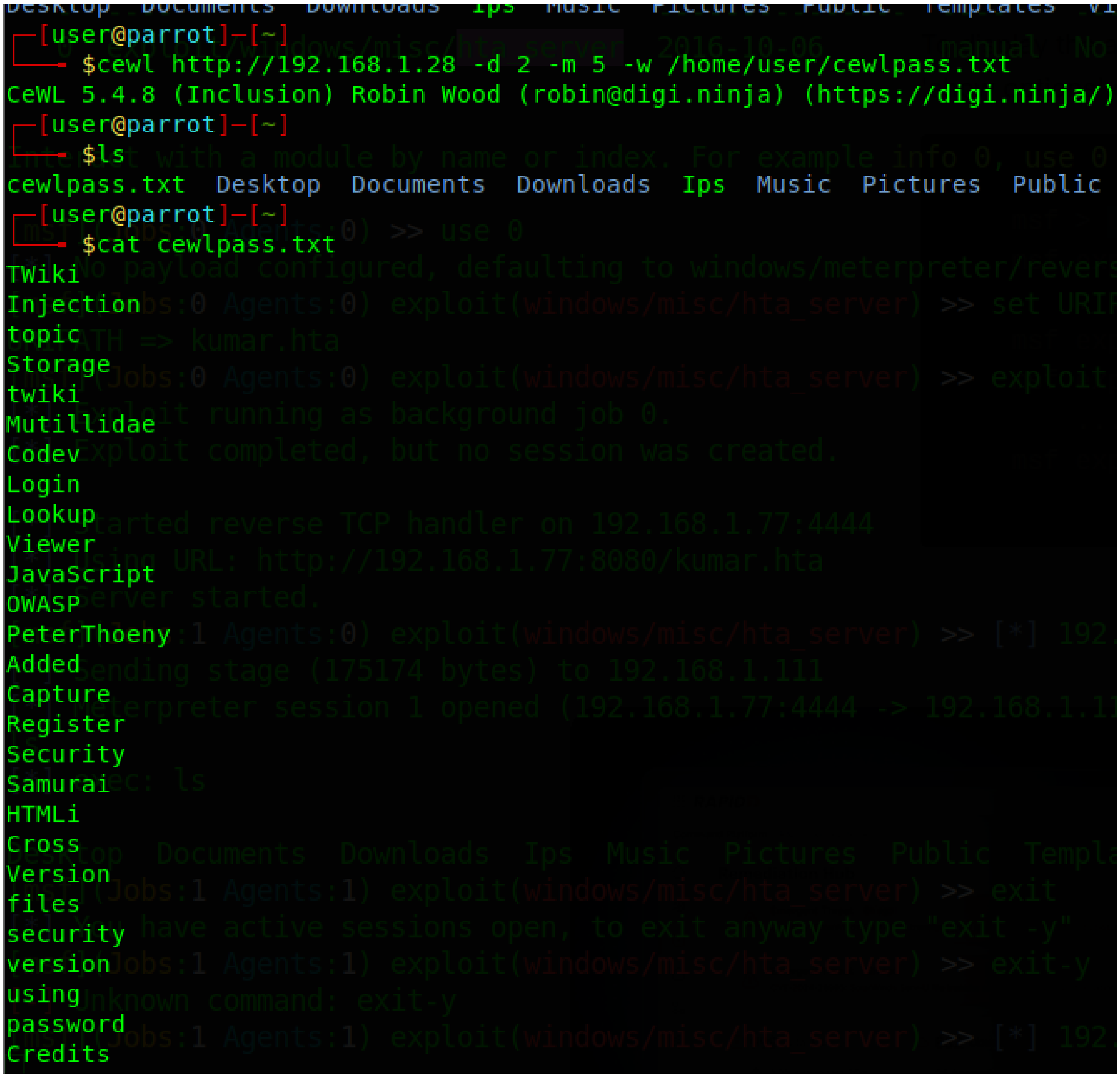
Password Cracking Tools

Hydra: Online password attack tool used against FTP, SSH, HTTP, and other services.

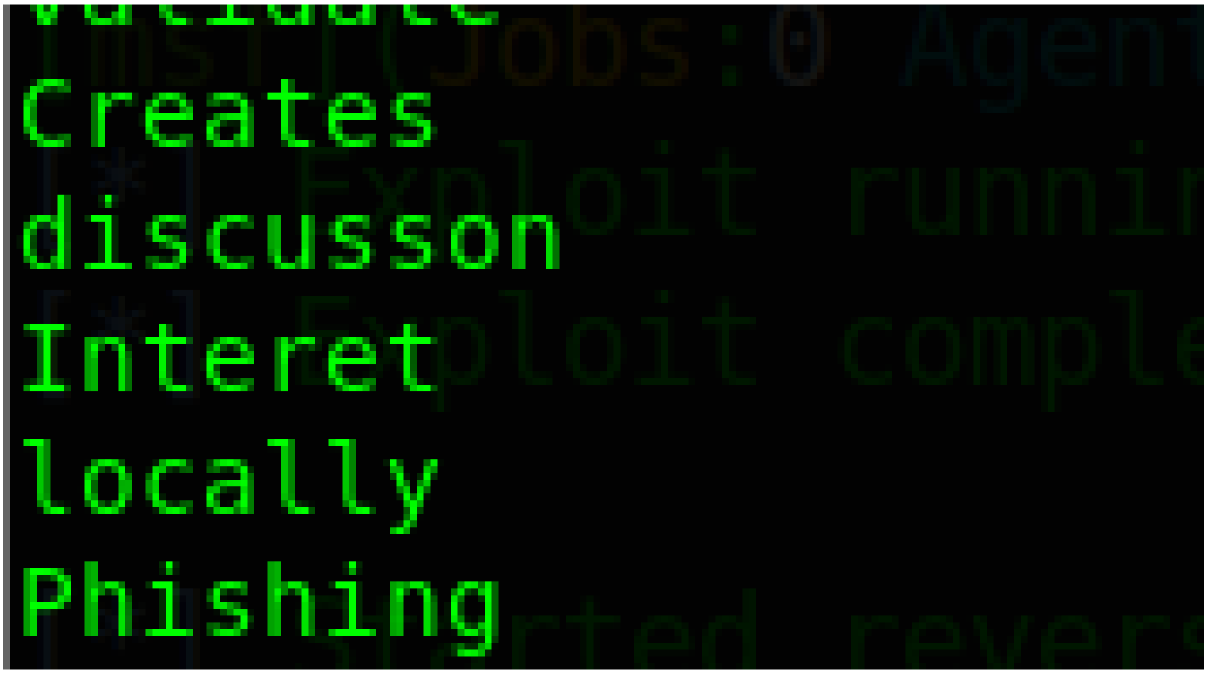
John the Ripper: Offline password cracking tool used to crack hashed passwords.

Custom Wordlist Generation (CeWL)

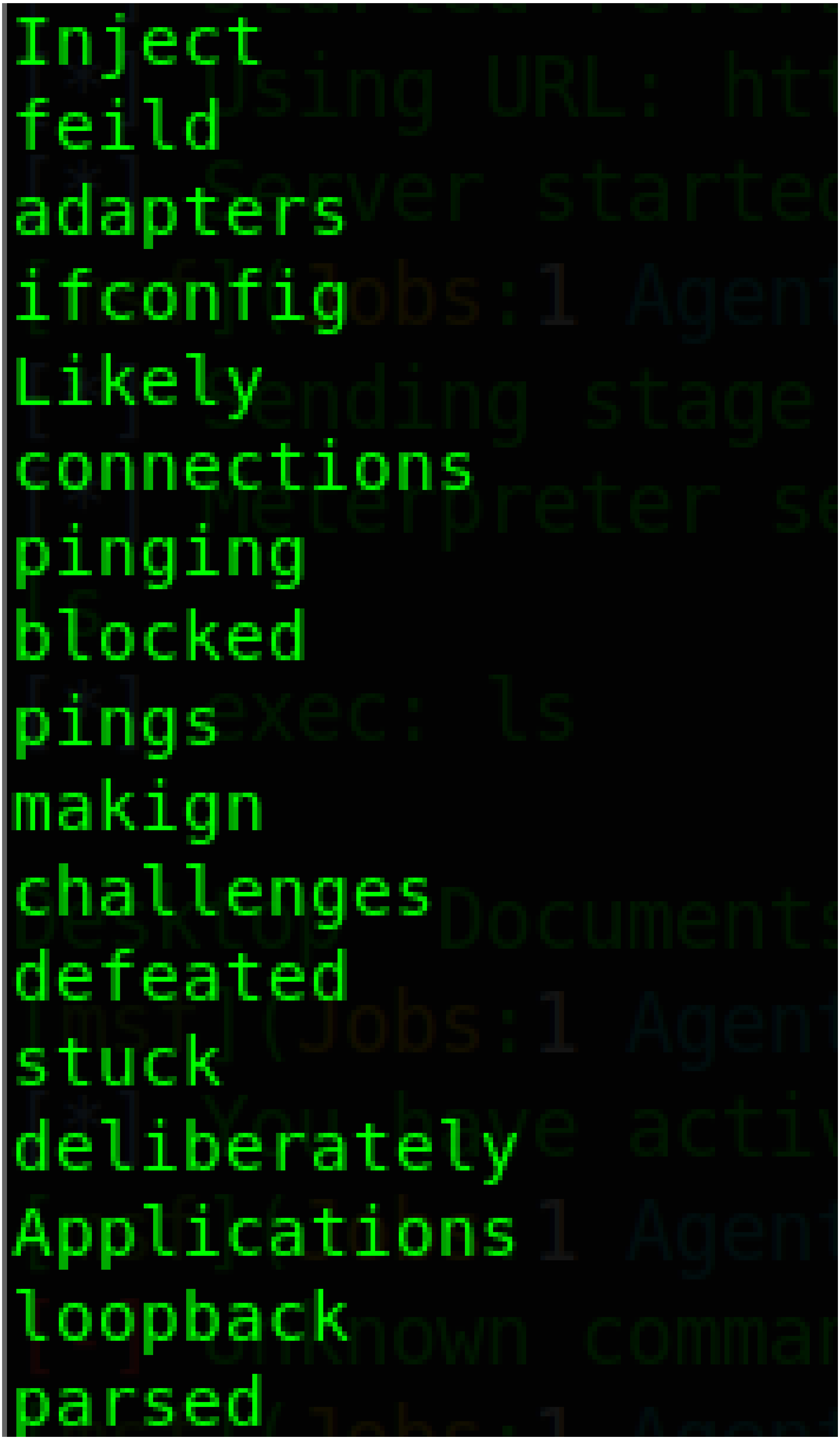
CeWL crawls websites and generates custom wordlists based on depth and minimum word length.



```
┌─[user@parrot]─[~]
└──╼ $cewl http://192.168.1.28 -d 2 -m 5 -w /home/user/cewlpass.txt
CeWL 5.4.8 (Inclusion) Robin Wood (robin@digi.ninja) (https://digi.ninja/)
┌─[user@parrot]─[~]
└──╼ $ls
cewlpass.txt  Desktop  Documents  Downloads  Ips  Music  Pictures  Public
┌─[user@parrot]─[~]
└──╼ $cat cewlpass.txt
TWiki
Injection
topic
Storage
twiki
Mutillidae
Codev
Login
Lookup
Viewer
JavaScript
OWASP
PeterThoeny
Added
Capture
Register
Security
Samurai
HTMLi
Cross
Version
files
security
version
using
password
Credits
```



```
Creates
discusson
Interet
locally
Phishing
```



```
Inject
feild
adapters
ifconfig
Likely
connections
pinging
blocked
pings
makign
challenges
defeated
stuck
deliberately
Applications
loopback
parsed
```

Conclusion

DNS Enumeration is a critical phase in penetration testing that reveals domain structure, misconfigurations, and sensitive information. Combined with FTP enumeration and password attacks, it provides deep insight into target systems. Proper security configuration and strong access controls are essential to prevent exploitation.