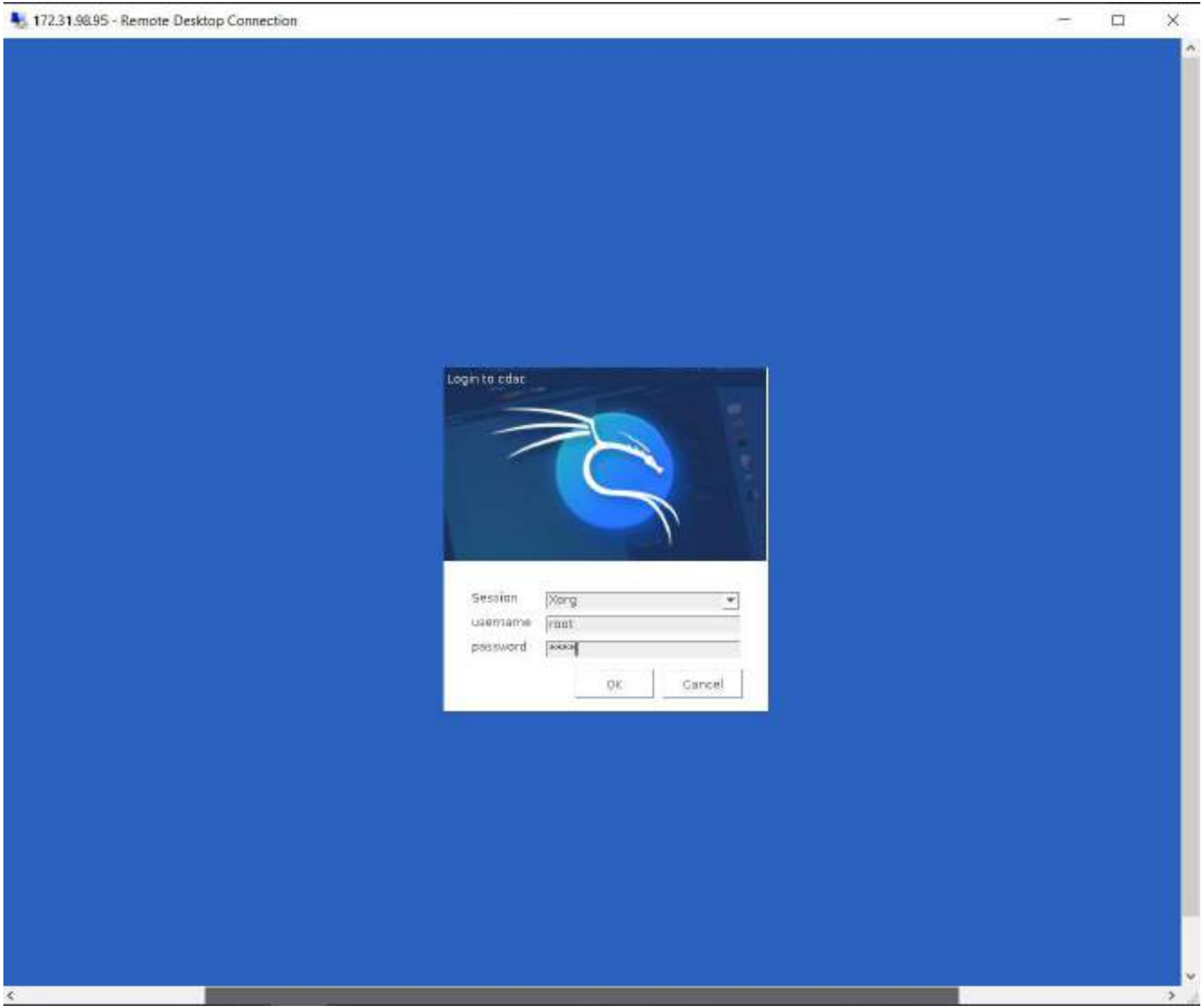
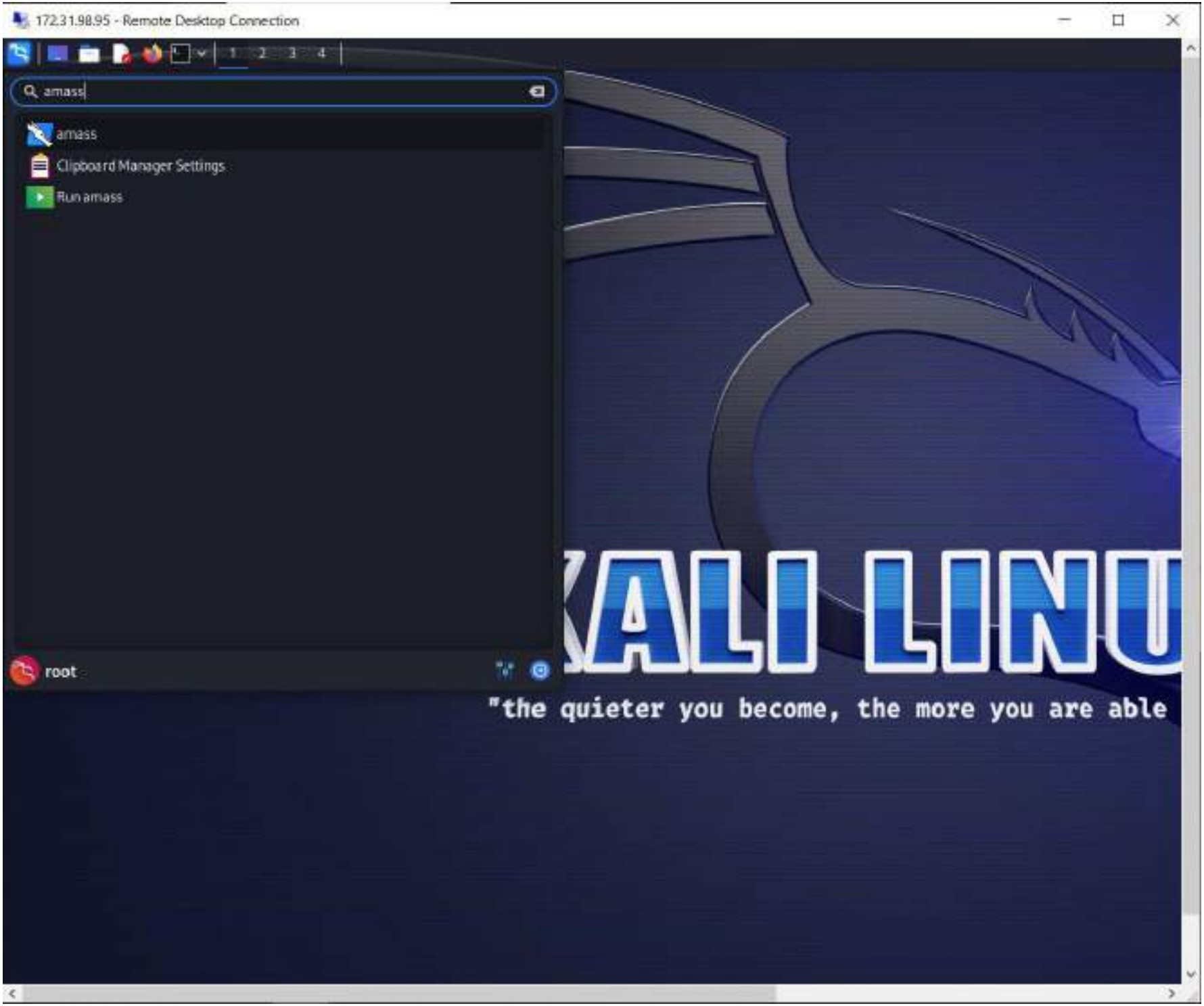
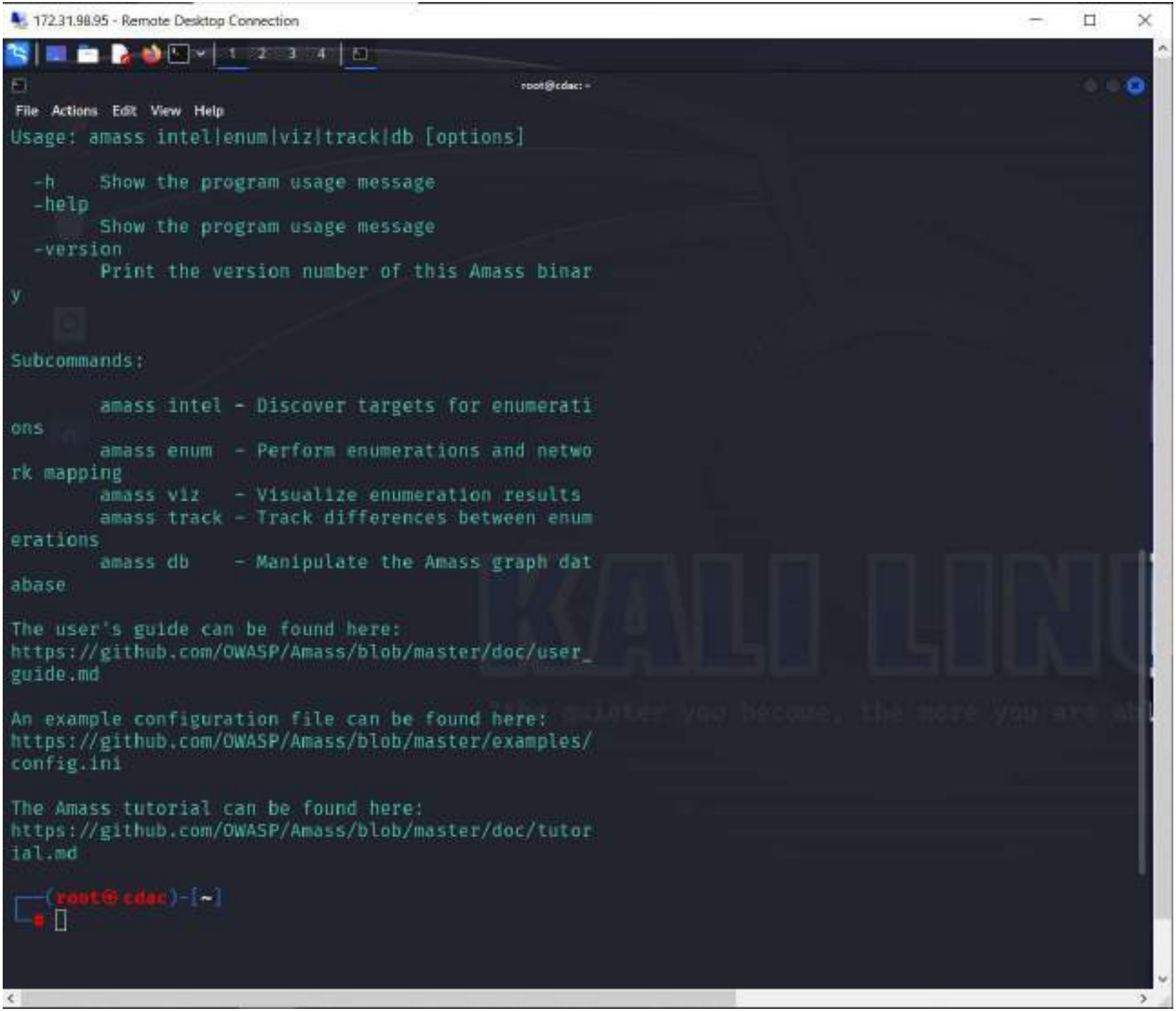
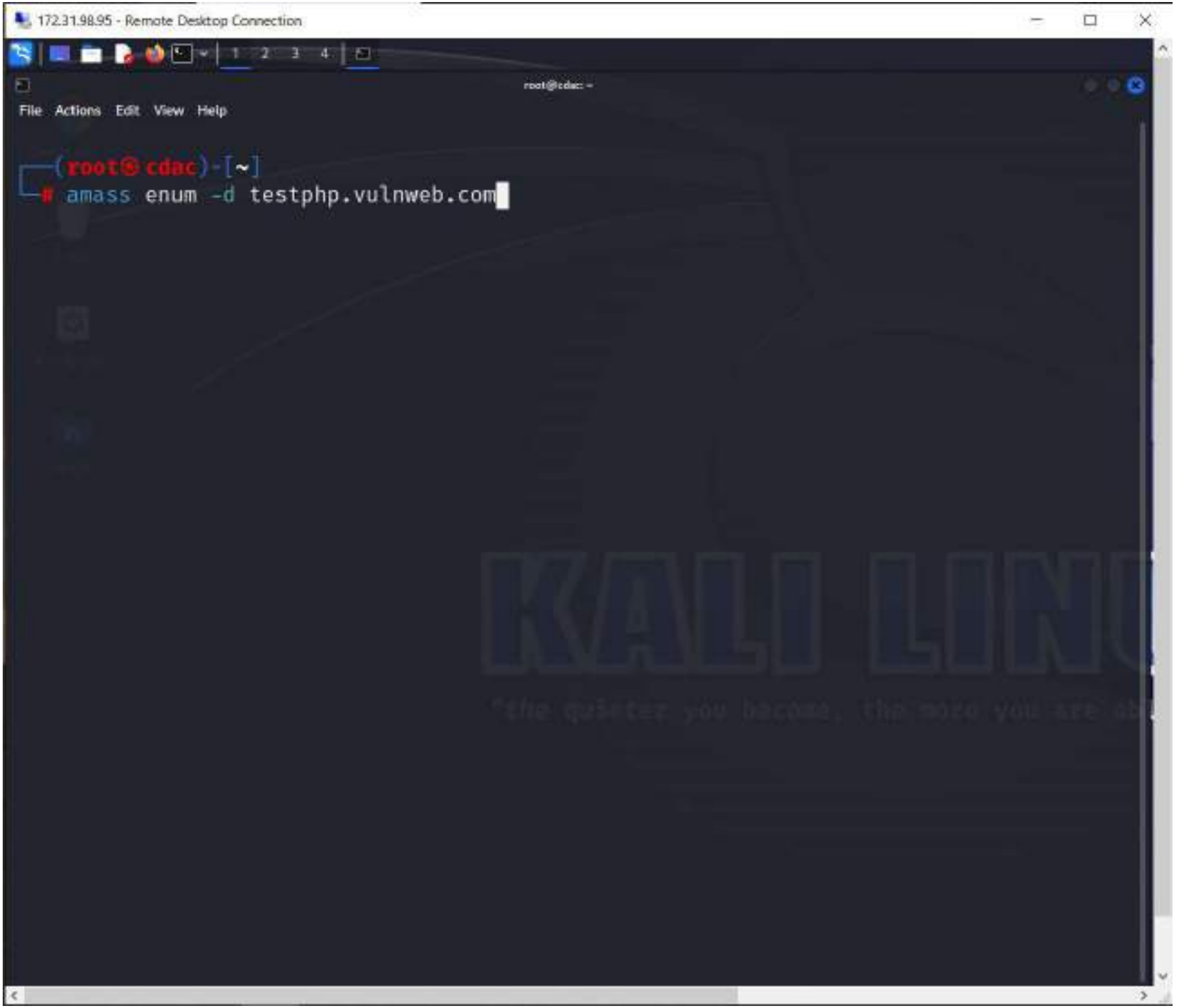

172.31.98.95 - Remote Desktop Connection
Login to cdac
Session
Xorg
username
root
password
OK
Cancel

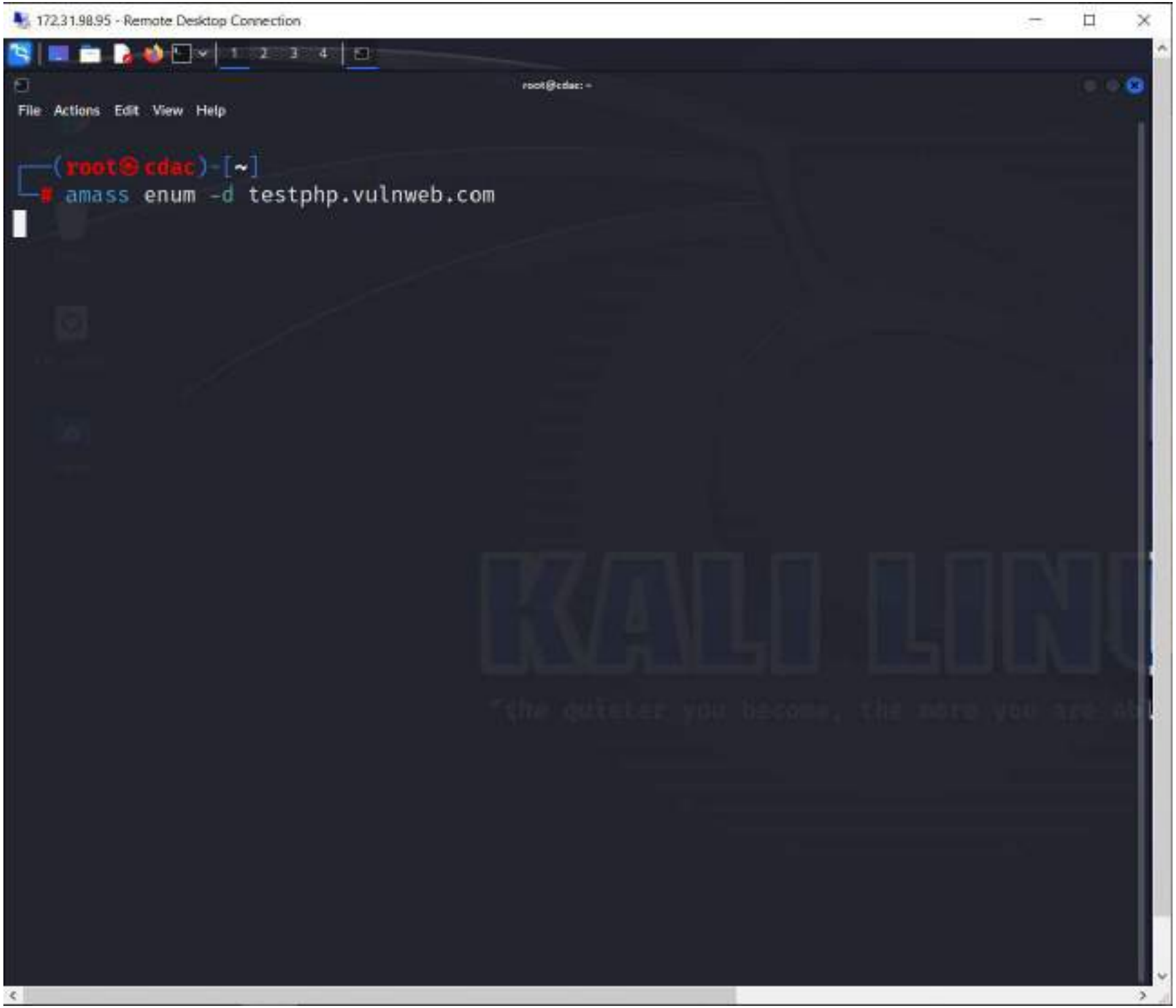

172.31.98.95 - Remote Desktop Connection
1 2 3 4
Google Chr...
Trash
File System
Home
KALI LINU
"the quieter you become, the more you are able

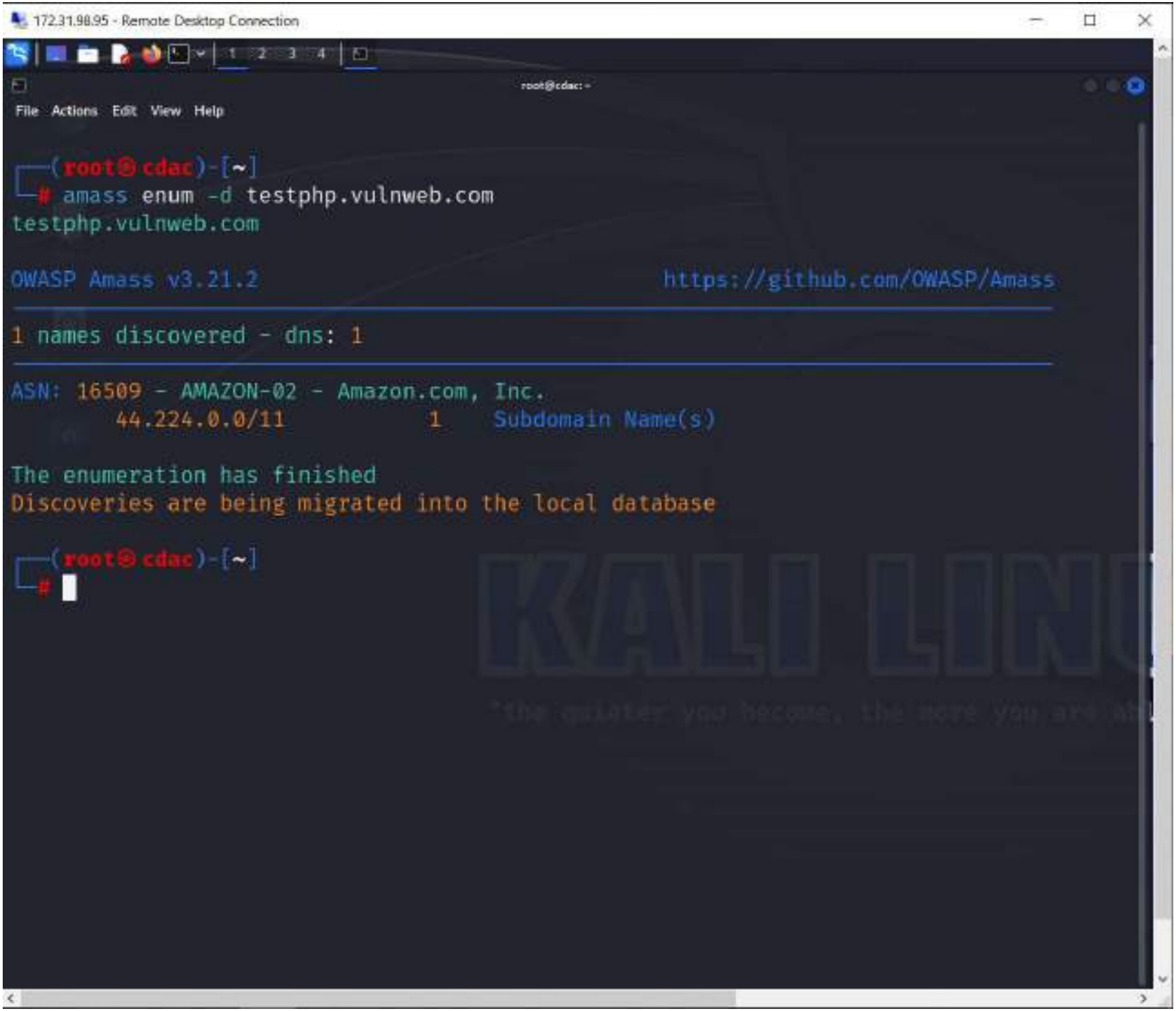

172.31.98.95 - Remote Desktop Connection
1 2 3 4
Favorites
Recently Used
All Applications
Settings
Usual Applications
01 - Information Gathering
02 - Vulnerability Analysis
03 - Web Application Analysis
04 - Database Assessment
05 - Password Attacks
06 - Wireless Attacks
07 - Reverse Engineering
08 - Exploitation Tools
09 - Sniffing & Spoofing
10 - Post Exploitation
11 - Forensics
12 - Reporting Tools
13 - Social Engineering Tools
42 - Kali & OffSec Links
root
CROSS SITE SCRIPTING(XSS) ATTACK
Terminal Emulator
Root Terminal Emulator
File Manager
Text Editor
Kali Linux
Kali Docs
Kali Bugs
OffSec Training
Exploit Database
VulnHub
"the quieter you become, the more you are able

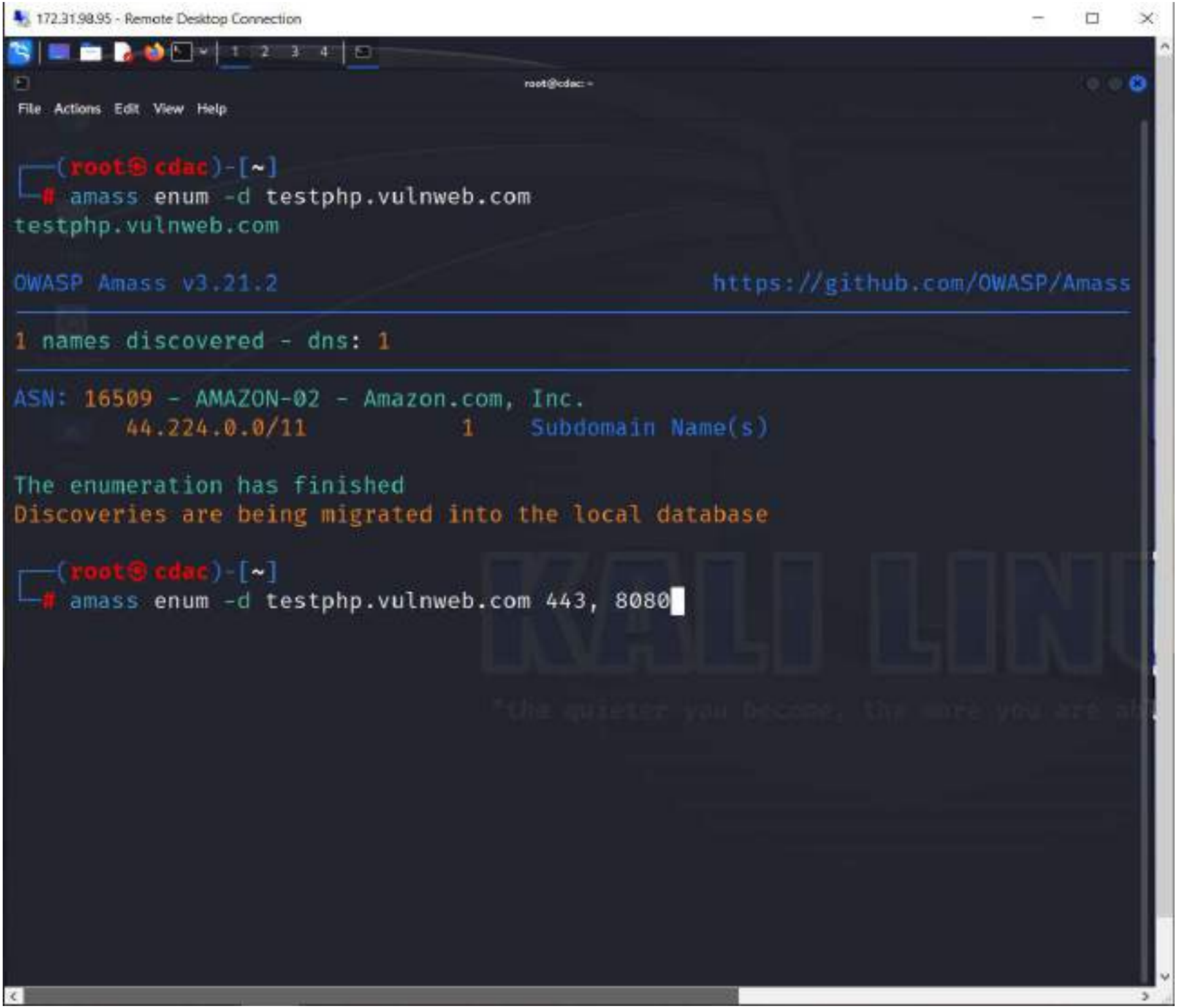

172.31.98.95 - Remote Desktop Connection
1 2 3 4
amass
amass
Clipboard Manager Settings
Run amass
root
KALI LINU
"the quieter you become, the more you are able

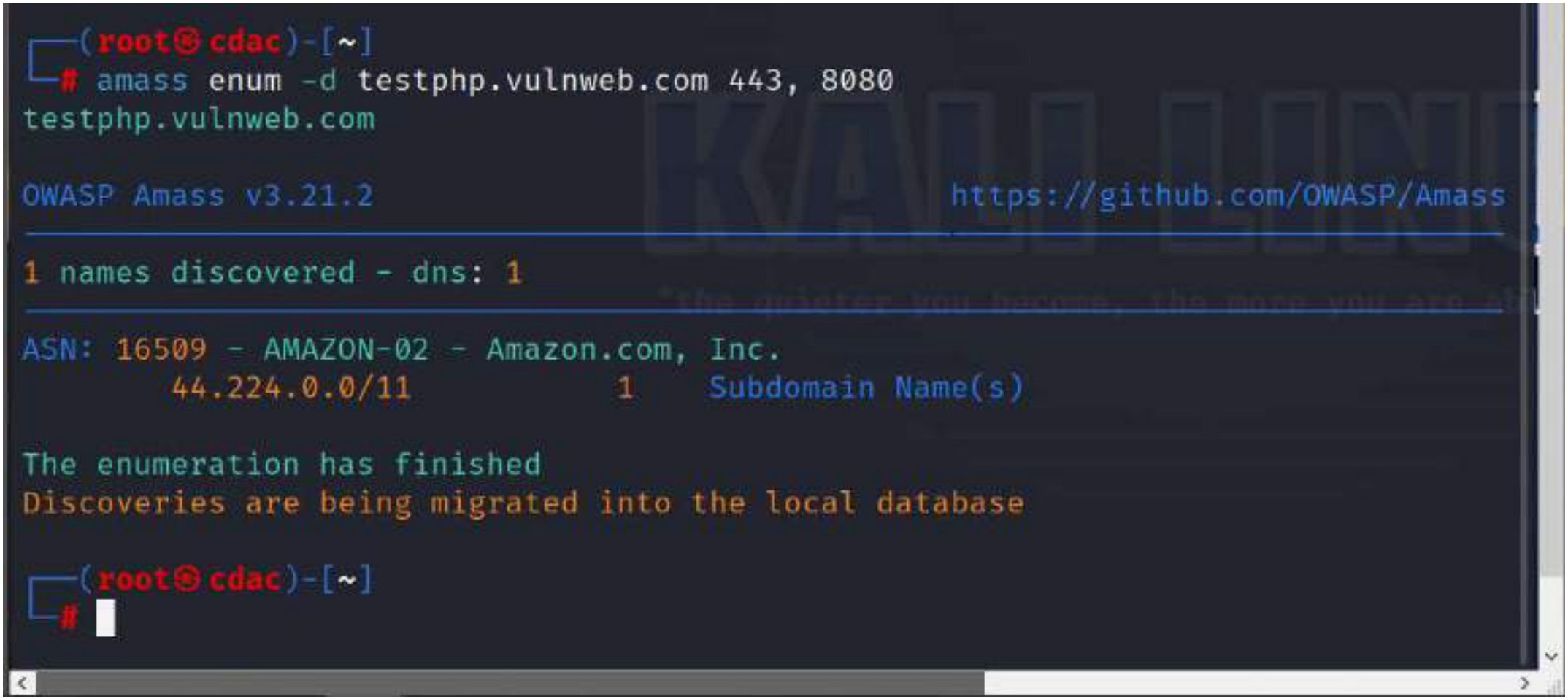

172.31.98.95 - Remote Desktop Connection
1 2 3 4
root@cdac: ~
File Actions Edit View Help
Usage: amass intel|enum|viz|track|db [options]
-h Show the program usage message
-help
Show the program usage message
-version
Print the version number of this Amass binar
y
Subcommands:
amass intel - Discover targets for enumerati
ons
amass enum - Perform enumerations and netwo
rk mapping
amass viz - Visualize enumeration results
amass track - Track differences between enum
erations
amass db - Manipulate the Amass graph dat
abase
The user's guide can be found here:
https://github.com/OWASP/Amass/blob/master/doc/user_
guide.md
An example configuration file can be found here:
https://github.com/OWASP/Amass/blob/master/examples/
config.ini
The Amass tutorial can be found here:
https://github.com/OWASP/Amass/blob/master/doc/tutor
ial.md
root@cdac
~

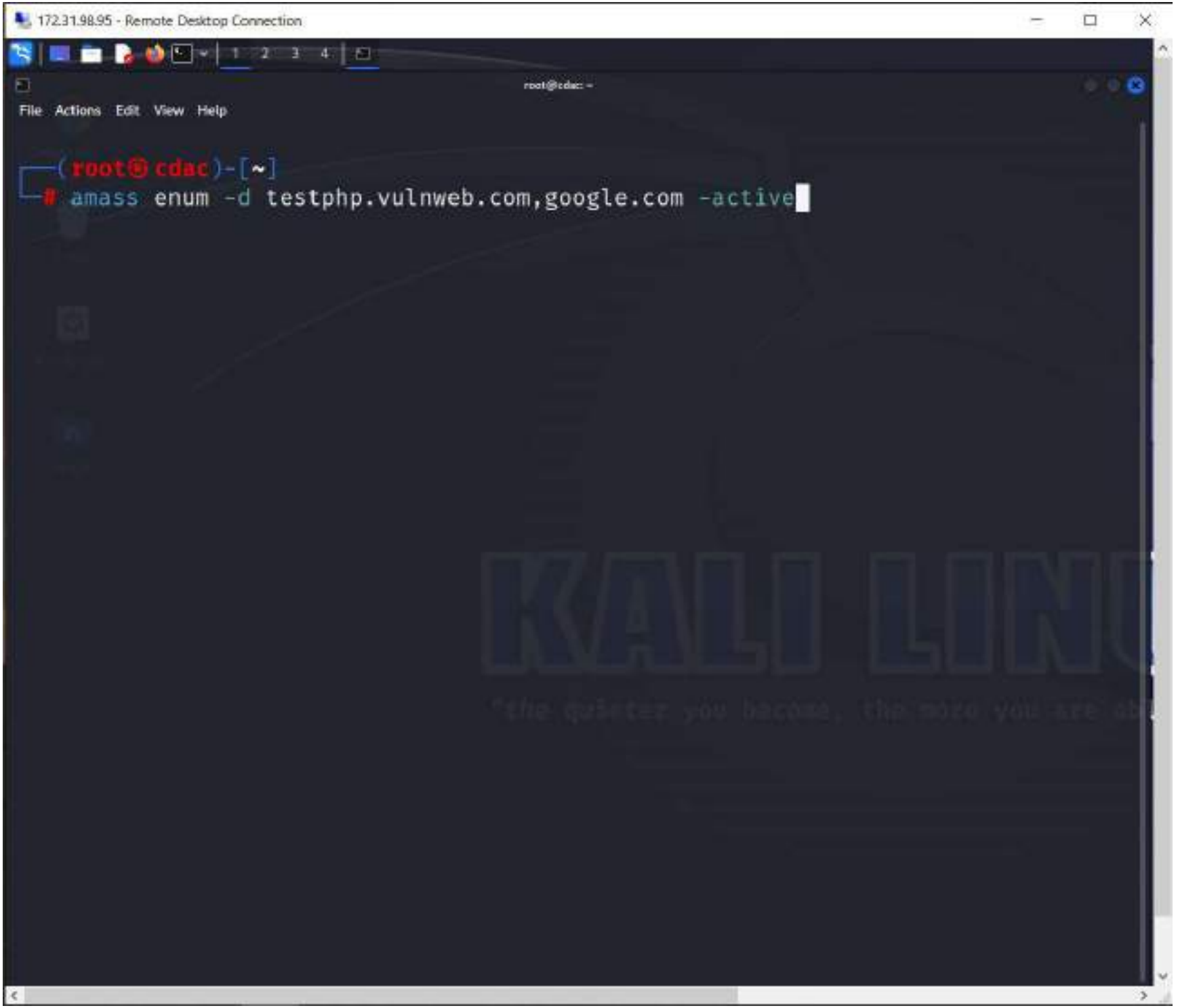

172.31.98.95 - Remote Desktop Connection
1 2 3 4
root@cdac: ~
File Actions Edit View Help
(root㉿cdac)-[~]
amass enum -d testphp.vulnweb.com

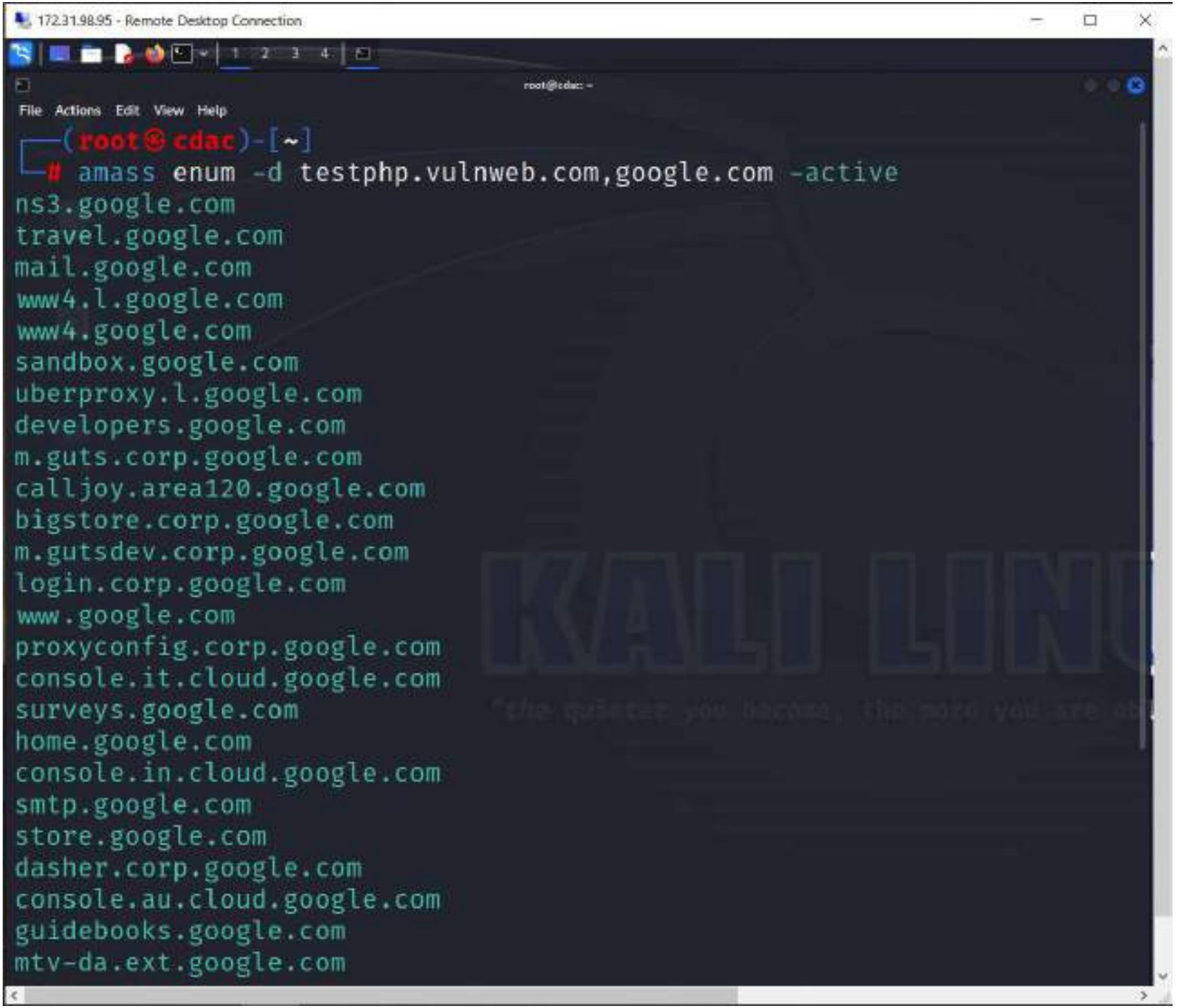

172.31.98.95 - Remote Desktop Connection
1 2 3 4
root@cdac: ~
File Actions Edit View Help
(root㉿cdac)-[~]
amass enum -d testphp.vulnweb.com

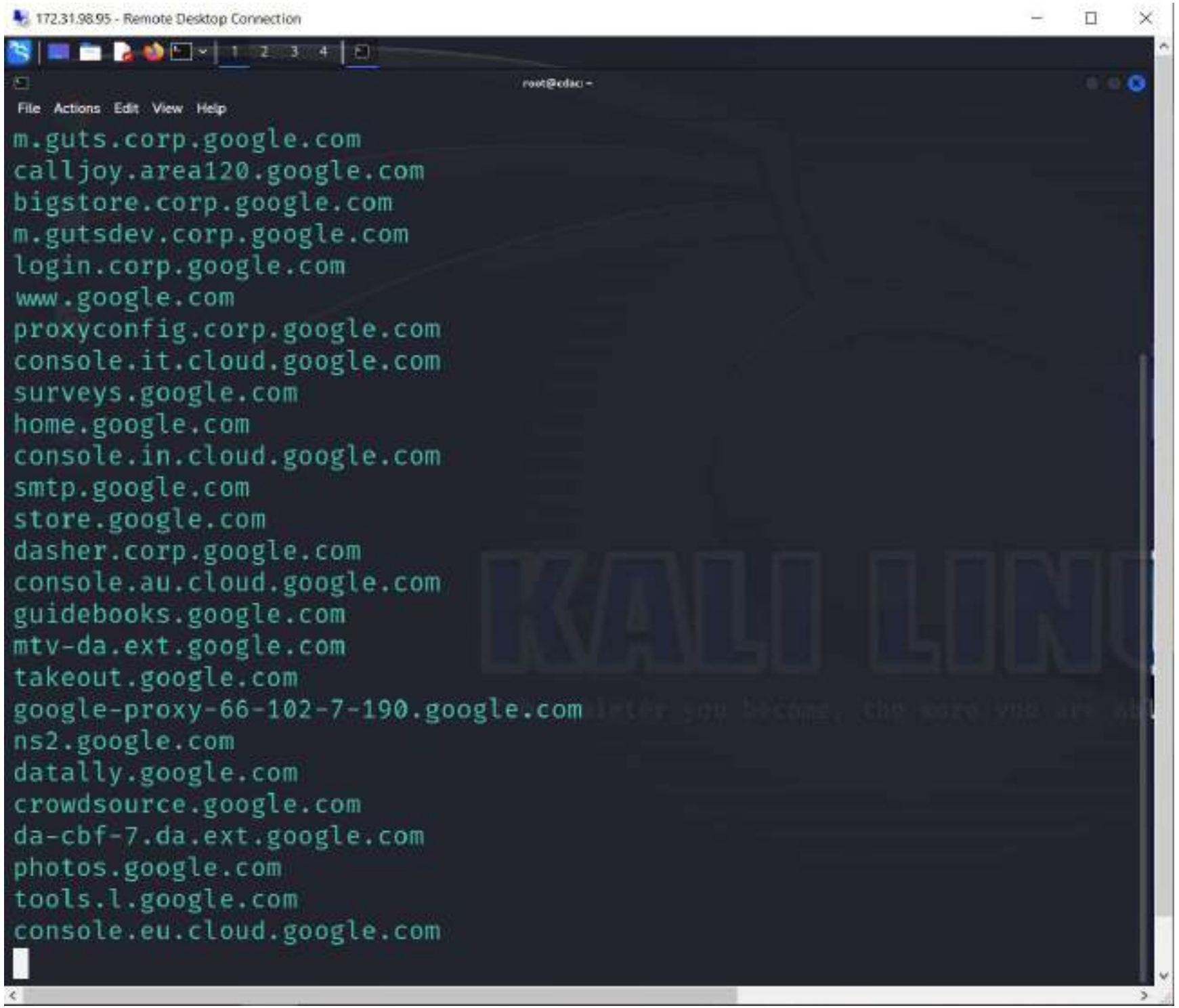

172.31.98.95 - Remote Desktop Connection
File Actions Edit View Help
(root㉿cdac)-[~]
amass enum -d testphp.vulnweb.com
testphp.vulnweb.com
OWASP Amass v3.21.2 https://github.com/OWASP/Amass
1 names discovered - dns: 1
ASN: 16509 - AMAZON-02 - Amazon.com, Inc.
44.224.0.0/11 1 Subdomain Name(s)
The enumeration has finished
Discoveries are being migrated into the local database
(root㉿cdac)-[~]
#

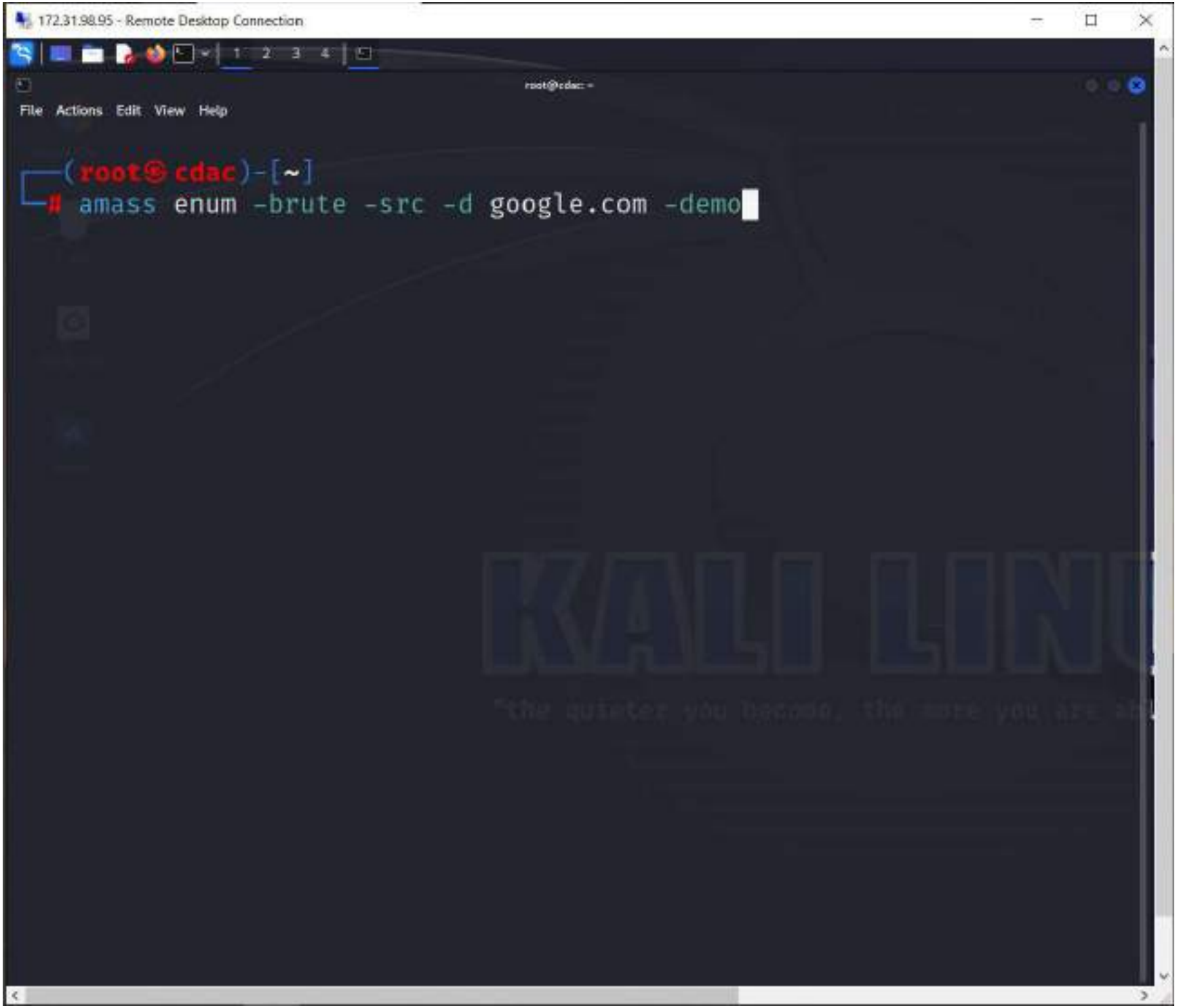

172.31.98.95 - Remote Desktop Connection
1 2 3 4
root@cdac: ~
File Actions Edit View Help
┌──(root㉿cdac)-[~]
└─# amass enum -d testphp.vulnweb.com
testphp.vulnweb.com
OWASP Amass v3.21.2 https://github.com/OWASP/Amass
1 names discovered - dns: 1
ASN: 16509 - AMAZON-02 - Amazon.com, Inc.
44.224.0.0/11 1 Subdomain Name(s)
The enumeration has finished
Discoveries are being migrated into the local database
┌──(root㉿cdac)-[~]
└─# amass enum -d testphp.vulnweb.com 443, 8080

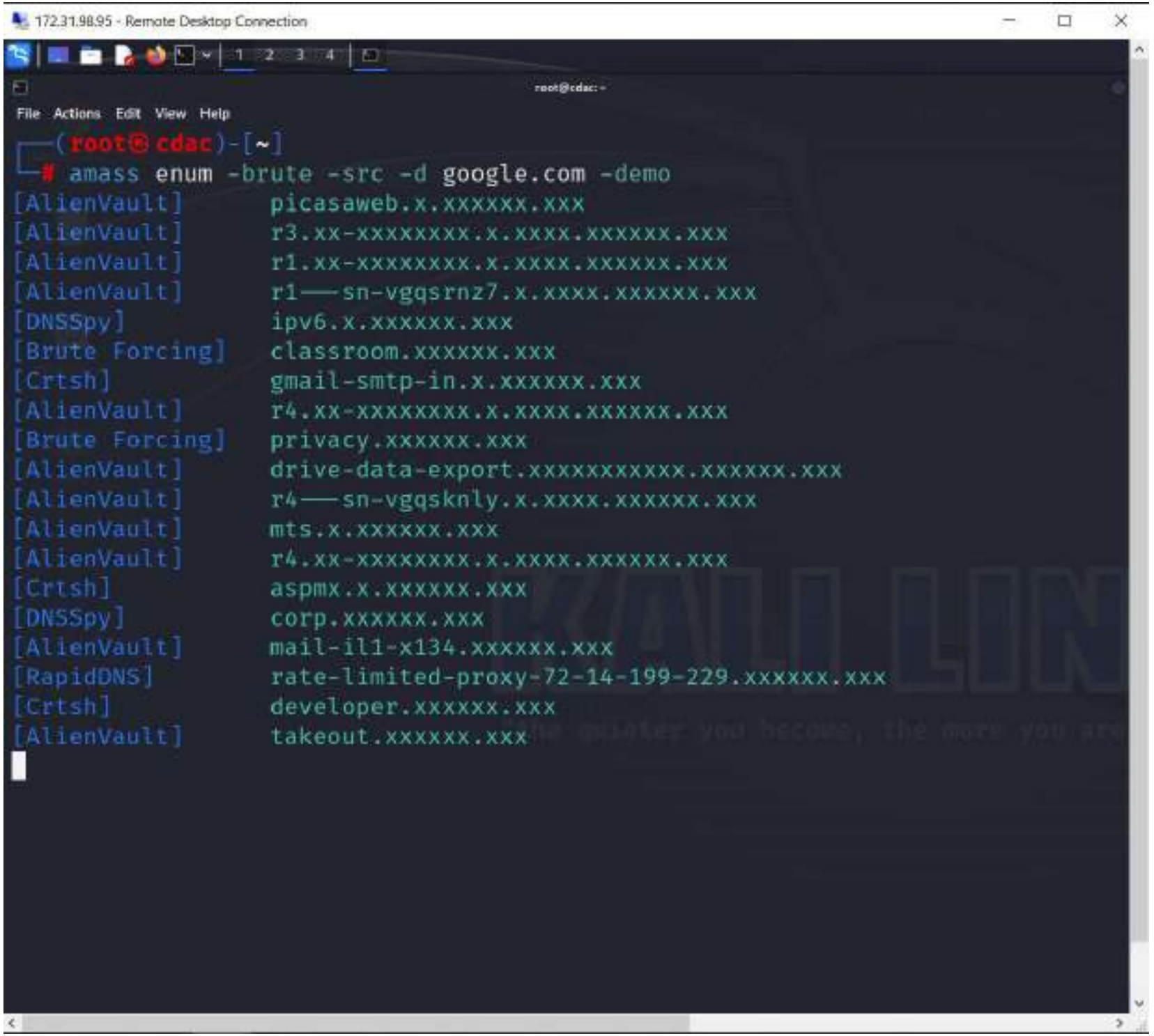

┌──(root㉿cdac)-[~]
└─# amass enum -d testphp.vulnweb.com 443, 8080
testphp.vulnweb.com
OWASP Amass v3.21.2 https://github.com/OWASP/Amass
1 names discovered - dns: 1
ASN: 16509 - AMAZON-02 - Amazon.com, Inc.
44.224.0.0/11 1 Subdomain Name(s)
The enumeration has finished
Discoveries are being migrated into the local database
┌──(root㉿cdac)-[~]
└─#

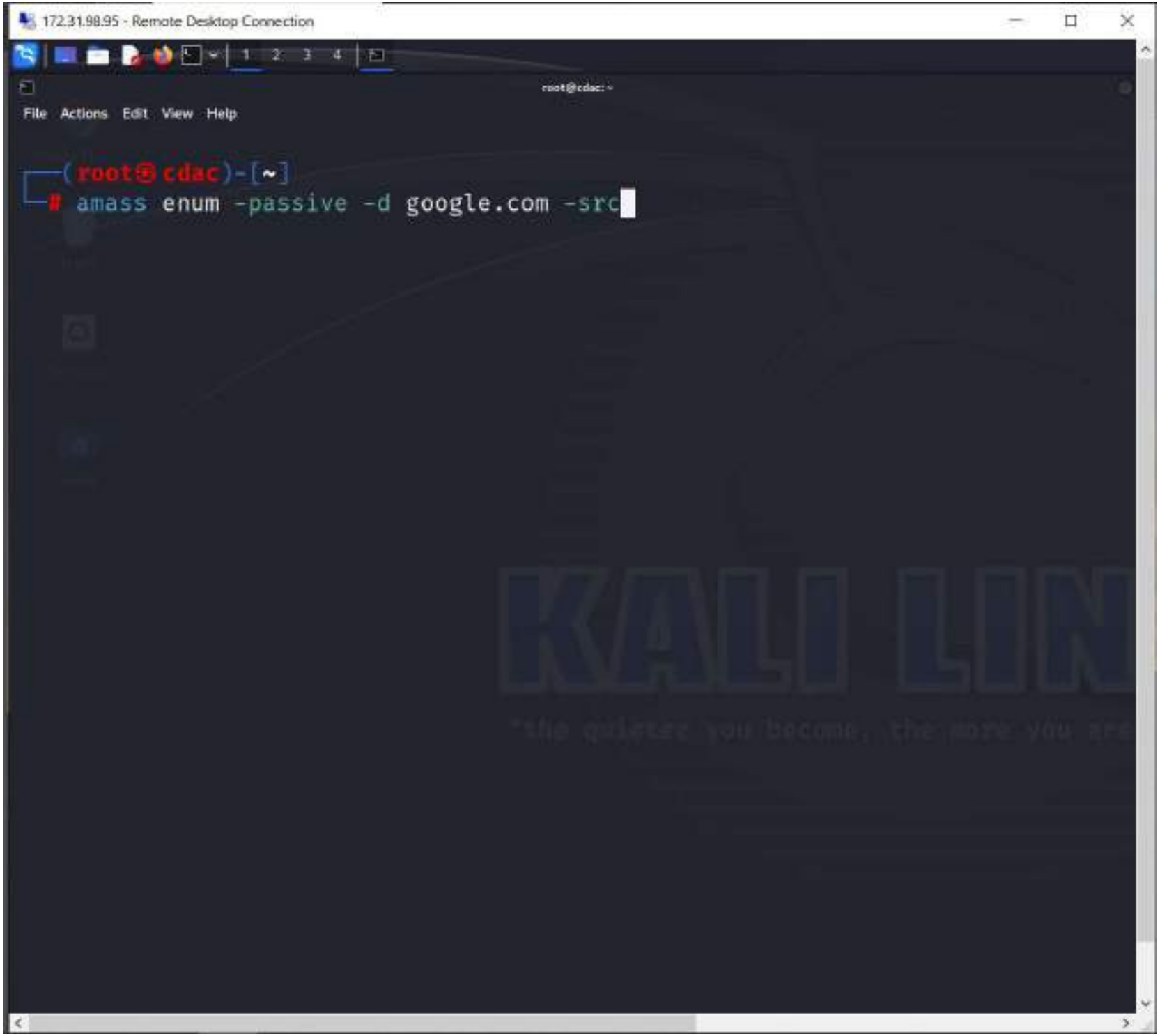

172.31.98.95 - Remote Desktop Connection
1 2 3 4
root@cdac: ~
File Actions Edit View Help
┌──(root㉿cdac)-[~]
└─# amass enum -d testphp.vulnweb.com,google.com -active

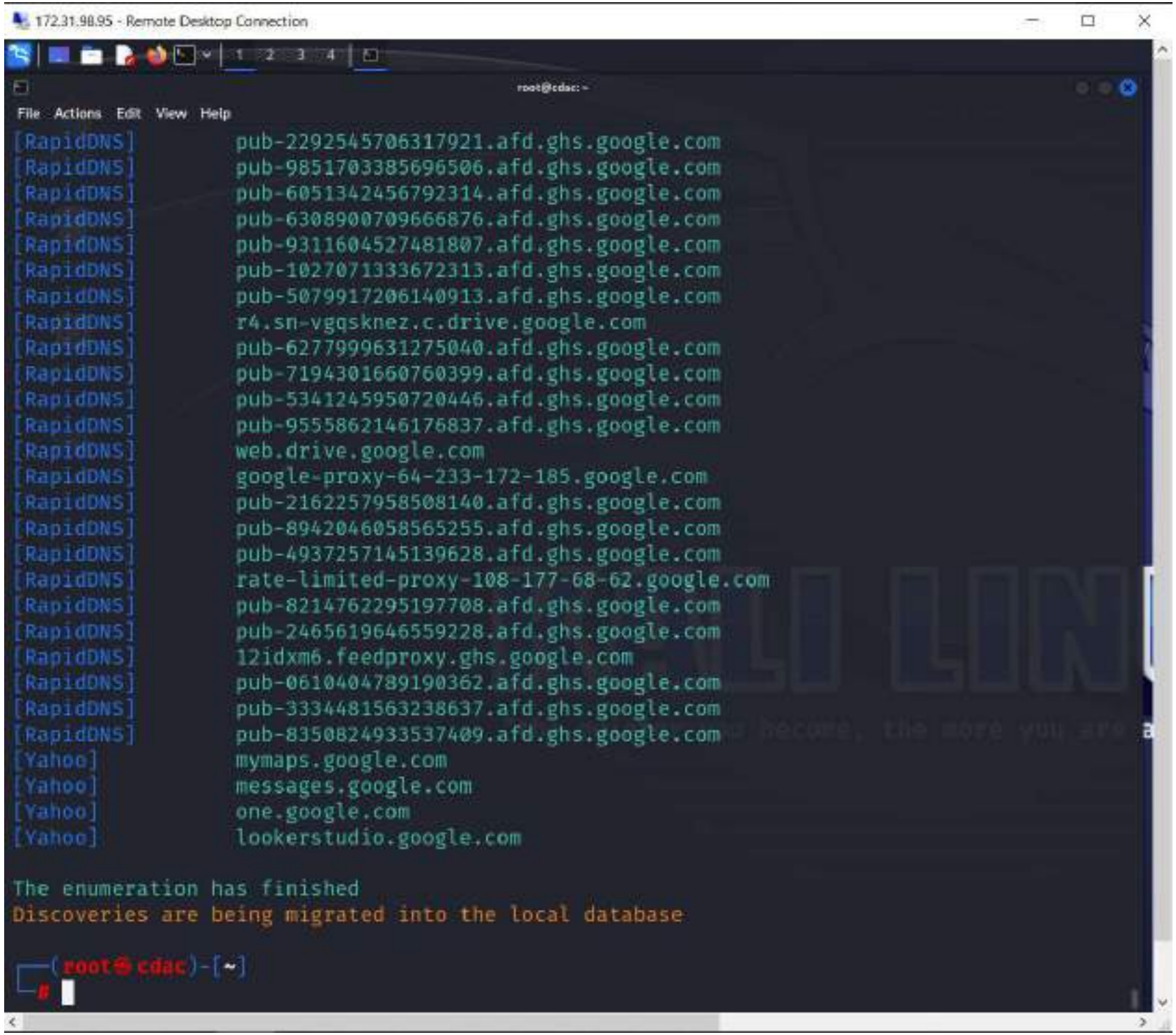

172.31.98.95 - Remote Desktop Connection
1 2 3 4
root@cdac: ~
File Actions Edit View Help
(root㉿cdac)-[~]
amass enum -d testphp.vulnweb.com,google.com -active
ns3.google.com
travel.google.com
mail.google.com
www4.l.google.com
www4.google.com
sandbox.google.com
uberproxy.l.google.com
developers.google.com
m.guts.corp.google.com
calljoy.area120.google.com
bigstore.corp.google.com
m.gutsdev.corp.google.com
login.corp.google.com
www.google.com
proxyconfig.corp.google.com
console.it.cloud.google.com
surveys.google.com
home.google.com
console.in.cloud.google.com
smtp.google.com
store.google.com
dasher.corp.google.com
console.au.cloud.google.com
guidebooks.google.com
mtv-da.ext.google.com

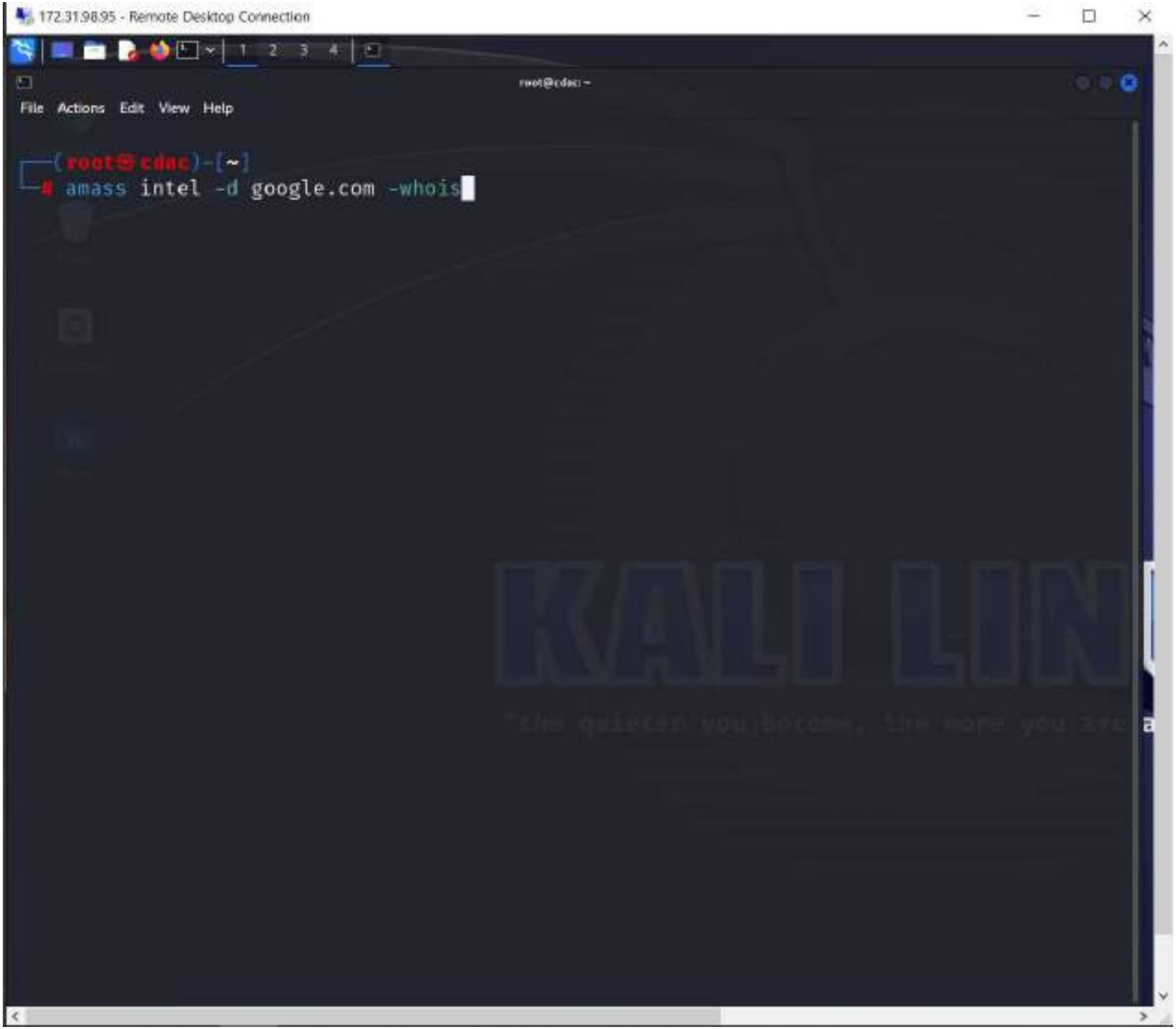

172.31.98.95 - Remote Desktop Connection
1 2 3 4
root@edac: ~
File Actions Edit View Help
m.guts.corp.google.com
calljoy.area120.google.com
bigstore.corp.google.com
m.gutsdev.corp.google.com
login.corp.google.com
www.google.com
proxyconfig.corp.google.com
console.it.cloud.google.com
surveys.google.com
home.google.com
console.in.cloud.google.com
smtp.google.com
store.google.com
dasher.corp.google.com
console.au.cloud.google.com
guidebooks.google.com
mtv-da.ext.google.com
takeout.google.com
google-proxy-66-102-7-190.google.com
ns2.google.com
datally.google.com
crowdsource.google.com
da-cbf-7.da.ext.google.com
photos.google.com
tools.l.google.com
console.eu.cloud.google.com

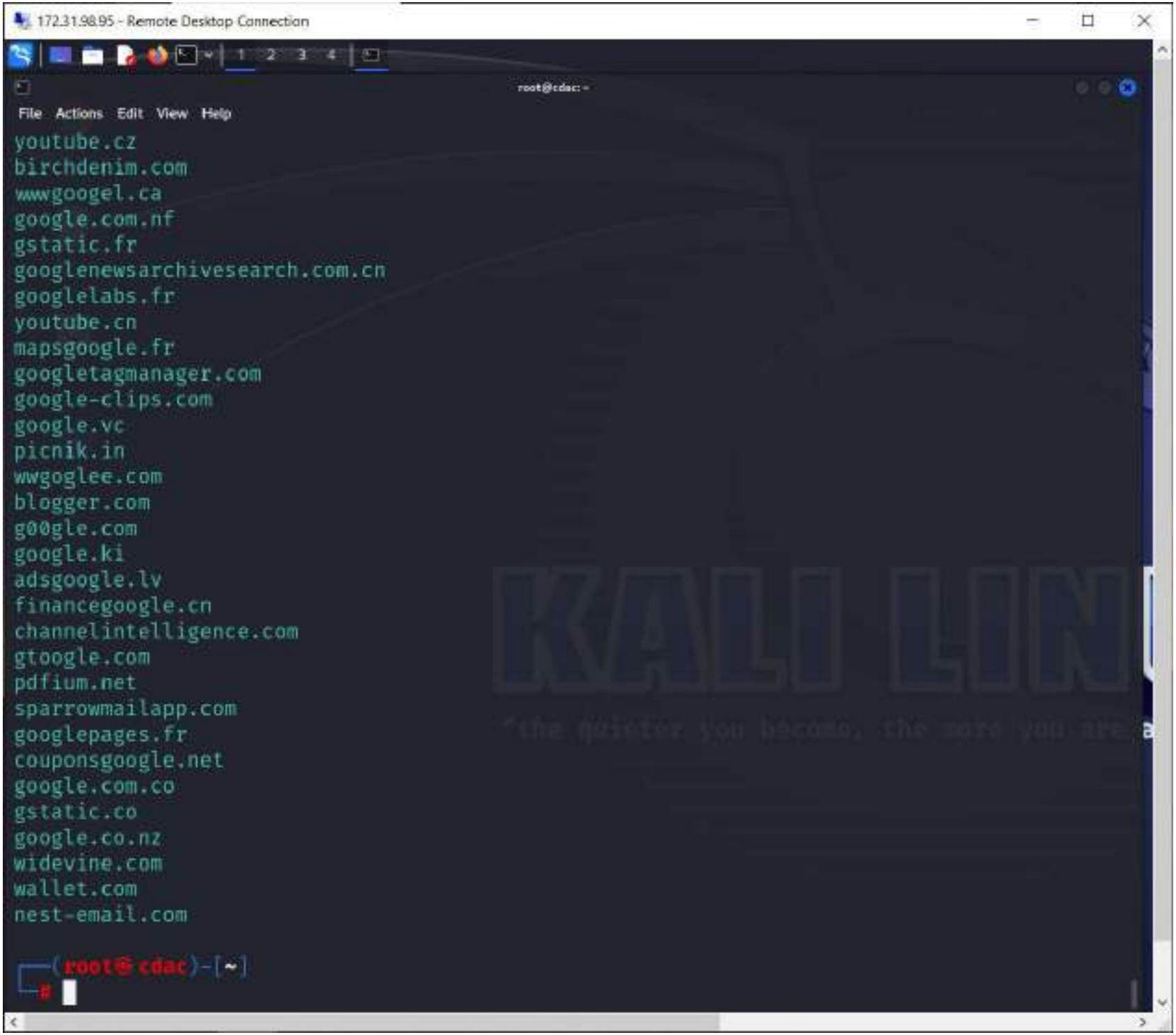

172.31.98.95 - Remote Desktop Connection
1 2 3 4
root@cdac: ~
File Actions Edit View Help
(root㉿cdac)-[~]
amass enum -brute -src -d google.com -demo

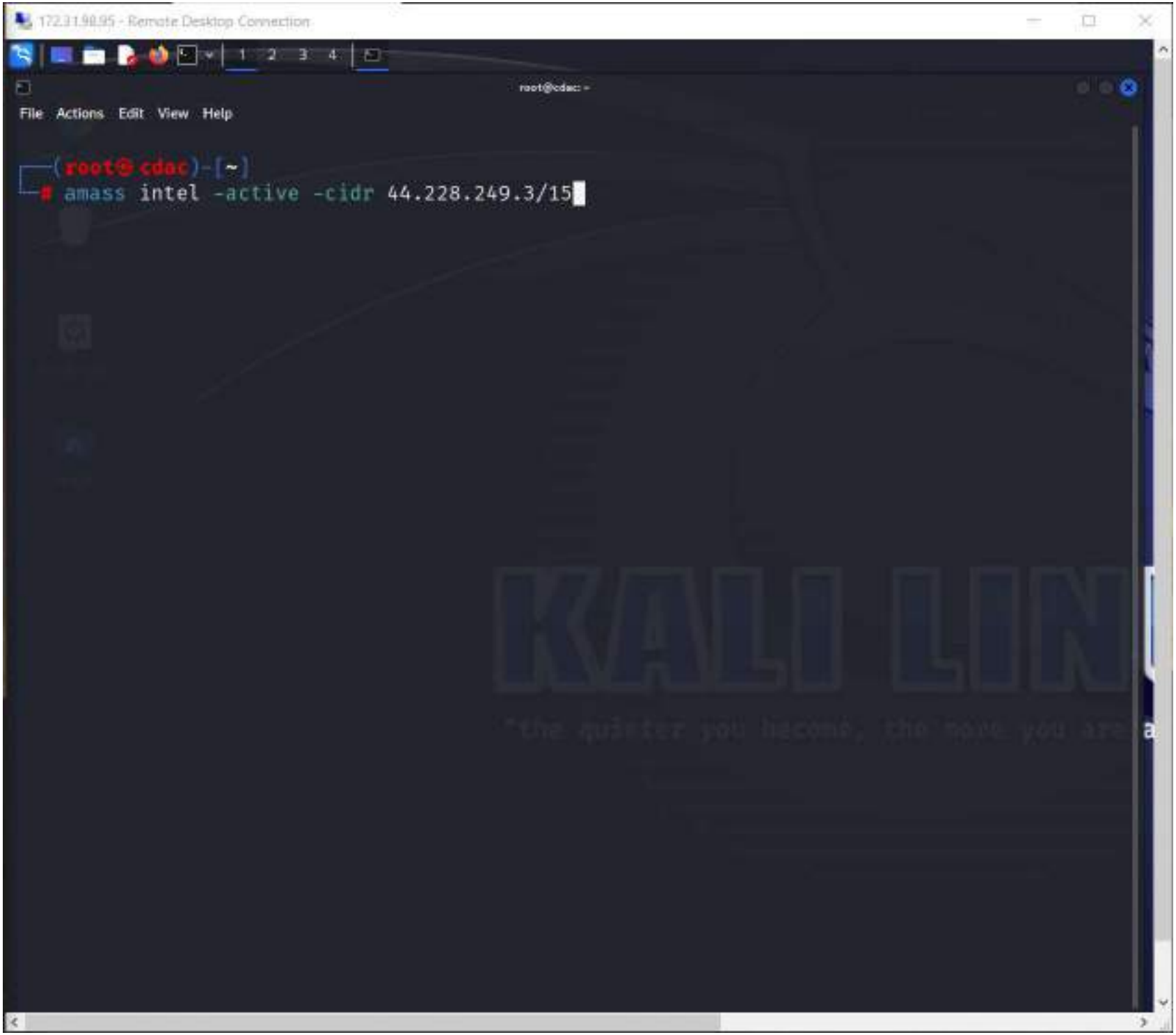

172.31.98.95 - Remote Desktop Connection
root@cdac: ~
File Actions Edit View Help
(root㉿cdac)-[~]
amass enum -brute -src -d google.com -demo
[AlienVault] picasaweb.x.xxxxxx.xxx
[AlienVault] r3.xx-xxxxxxxx.x.xxxx.xxxxxx.xxx
[AlienVault] r1.xx-xxxxxxxx.x.xxxx.xxxxxx.xxx
[AlienVault] r1---sn-vgqsrnz7.x.xxxx.xxxxxx.xxx
[DNSSpy] ipv6.x.xxxxxx.xxx
[Brute Forcing] classroom.xxxxxx.xxx
[Crtsh] gmail-smtp-in.x.xxxxxx.xxx
[AlienVault] r4.xx-xxxxxxxx.x.xxxx.xxxxxx.xxx
[Brute Forcing] privacy.xxxxxx.xxx
[AlienVault] drive-data-export.xxxxxxxxxxx.xxxxxx.xxx
[AlienVault] r4---sn-vgqsknly.x.xxxx.xxxxxx.xxx
[AlienVault] mts.x.xxxxxx.xxx
[AlienVault] r4.xx-xxxxxxxx.x.xxxx.xxxxxx.xxx
[Crtsh] aspmx.x.xxxxxx.xxx
[DNSSpy] corp.xxxxxx.xxx
[AlienVault] mail-il1-x134.xxxxxx.xxx
[RapidDNS] rate-limited-proxy-72-14-199-229.xxxxxx.xxx
[Crtsh] developer.xxxxxx.xxx
[AlienVault] takeout.xxxxxx.xxx

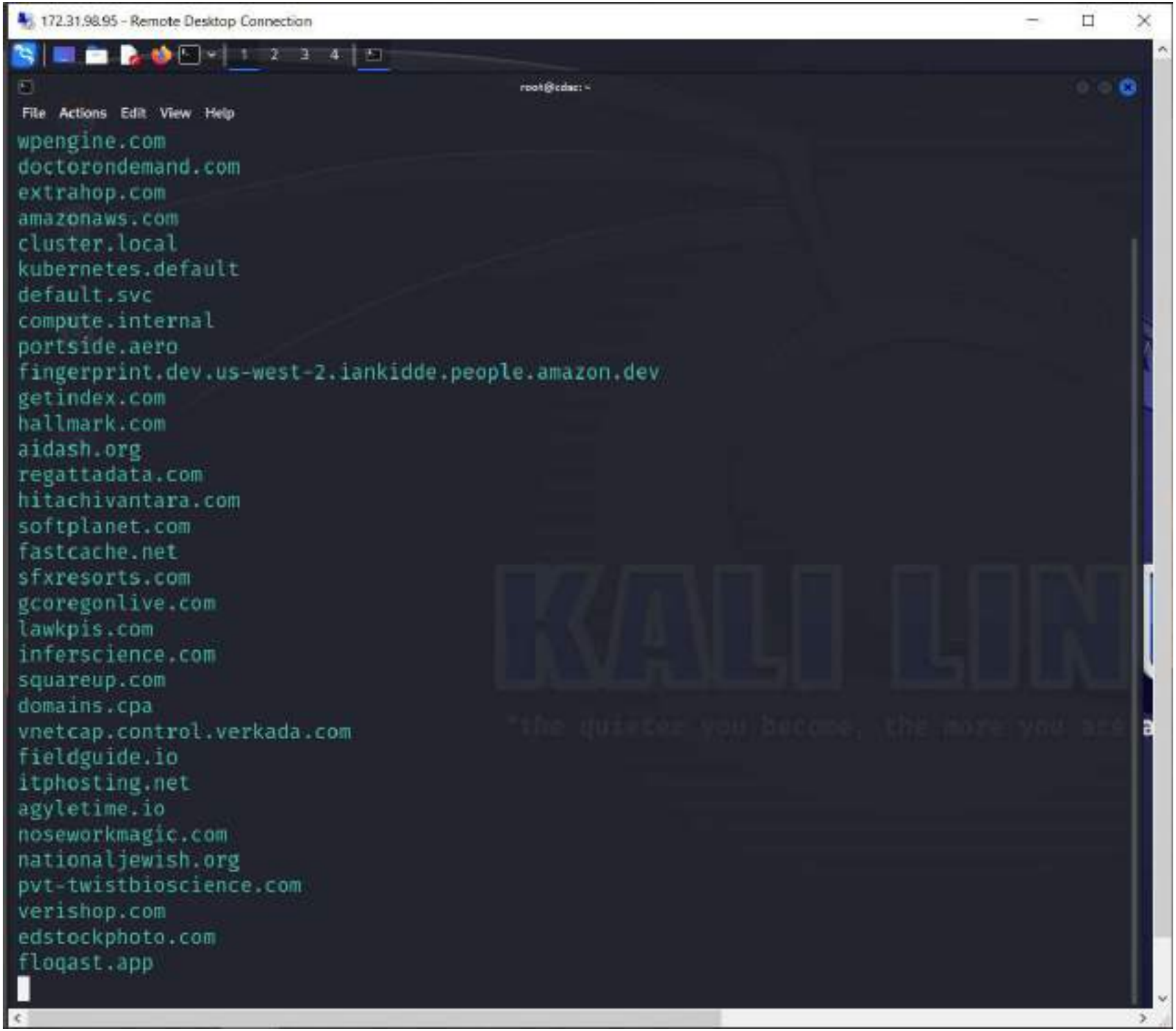

172.31.98.95 - Remote Desktop Connection
1 2 3 4
root@cdac: ~
File Actions Edit View Help
(root㉿cdac)-[~]
amass enum -passive -d google.com -src

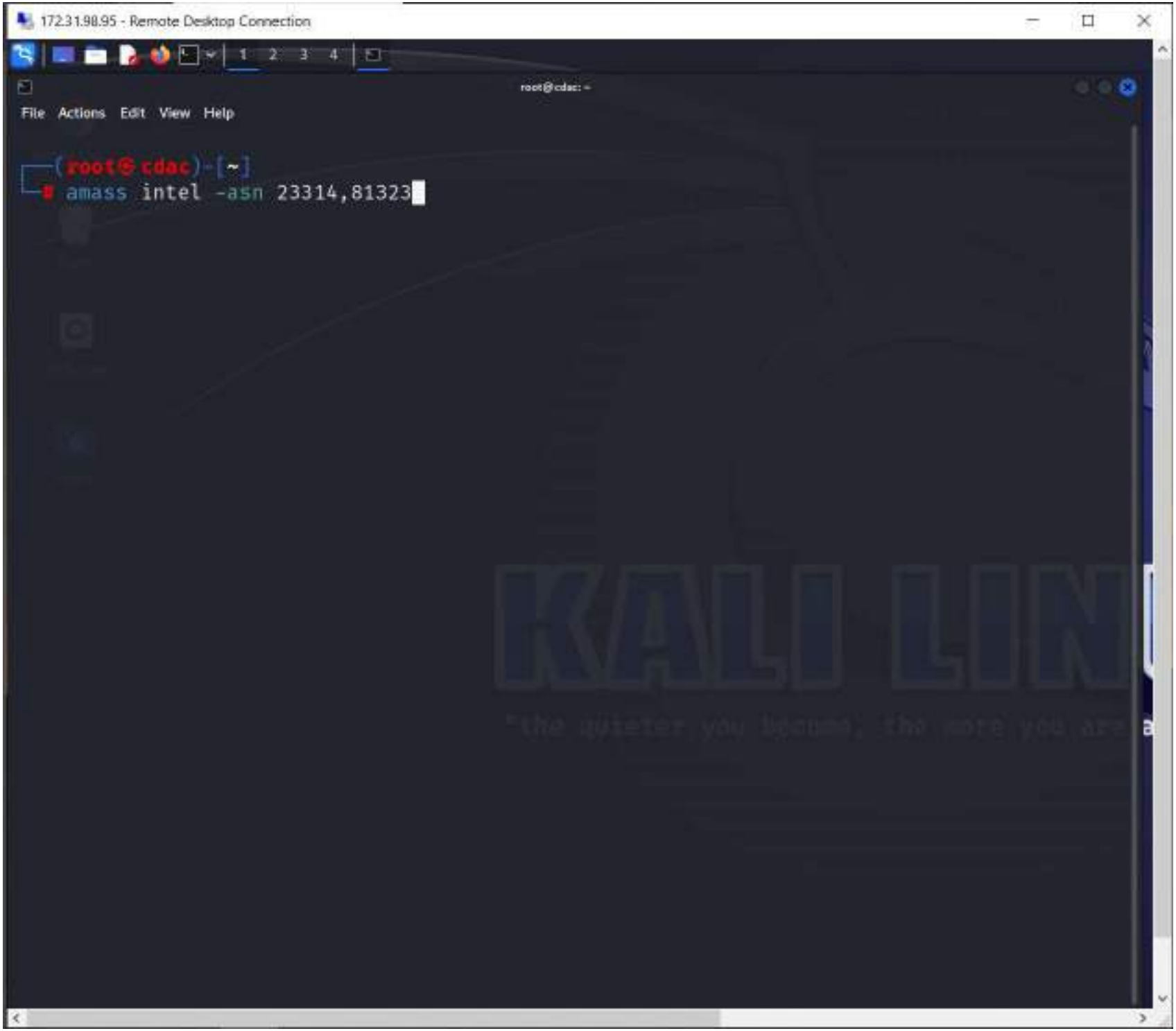

172.31.98.95 - Remote Desktop Connection
root@cdac: ~
File Actions Edit View Help
[RapidDNS] pub-2292545706317921.afd.ghs.google.com
[RapidDNS] pub-9851703385696506.afd.ghs.google.com
[RapidDNS] pub-6051342456792314.afd.ghs.google.com
[RapidDNS] pub-6308900709666876.afd.ghs.google.com
[RapidDNS] pub-9311604527481807.afd.ghs.google.com
[RapidDNS] pub-1027071333672313.afd.ghs.google.com
[RapidDNS] pub-5079917206140913.afd.ghs.google.com
[RapidDNS] r4.sn-vgqsknez.c.drive.google.com
[RapidDNS] pub-6277999631275040.afd.ghs.google.com
[RapidDNS] pub-7194301660760399.afd.ghs.google.com
[RapidDNS] pub-5341245950720446.afd.ghs.google.com
[RapidDNS] pub-9555862146176837.afd.ghs.google.com
[RapidDNS] web.drive.google.com
[RapidDNS] google-proxy-64-233-172-185.google.com
[RapidDNS] pub-2162257958508140.afd.ghs.google.com
[RapidDNS] pub-8942046058565255.afd.ghs.google.com
[RapidDNS] pub-4937257145139628.afd.ghs.google.com
[RapidDNS] rate-limited-proxy-108-177-68-62.google.com
[RapidDNS] pub-8214762295197708.afd.ghs.google.com
[RapidDNS] pub-2465619646559228.afd.ghs.google.com
[RapidDNS] 12idxm6.feedproxy.ghs.google.com
[RapidDNS] pub-0610404789190362.afd.ghs.google.com
[RapidDNS] pub-3334481563238637.afd.ghs.google.com
[RapidDNS] pub-8350824933537409.afd.ghs.google.com
[Yahoo] mymaps.google.com
[Yahoo] messages.google.com
[Yahoo] one.google.com
[Yahoo] lookerstudio.google.com
The enumeration has finished
Discoveries are being migrated into the local database
(root㉿cdac)-[~]
#

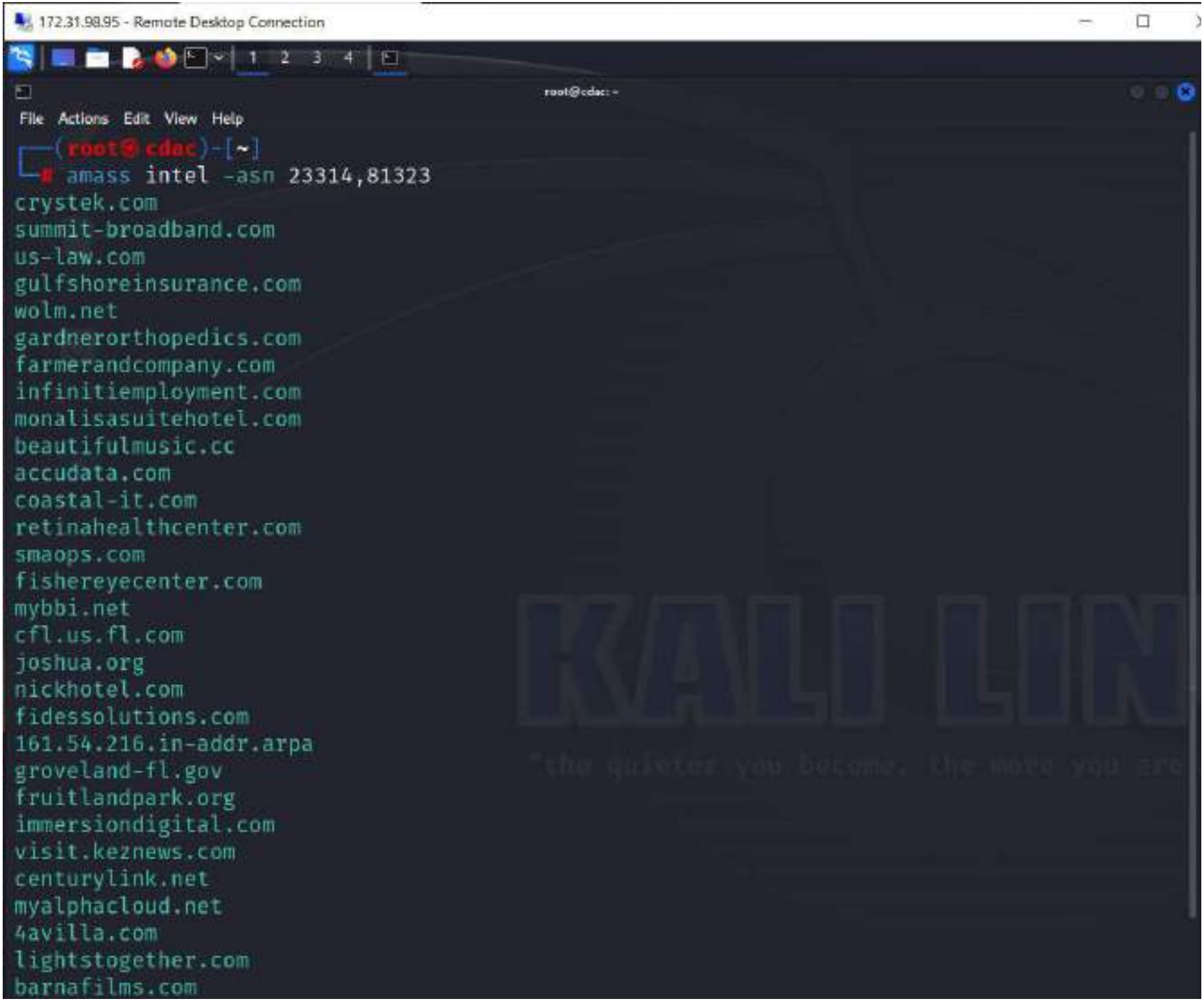

172.31.98.95 - Remote Desktop Connection
1 2 3 4
root@cdac: ~
File Actions Edit View Help
┌──(root㉿cdac)-[~]
└─# amass intel -d google.com -whois

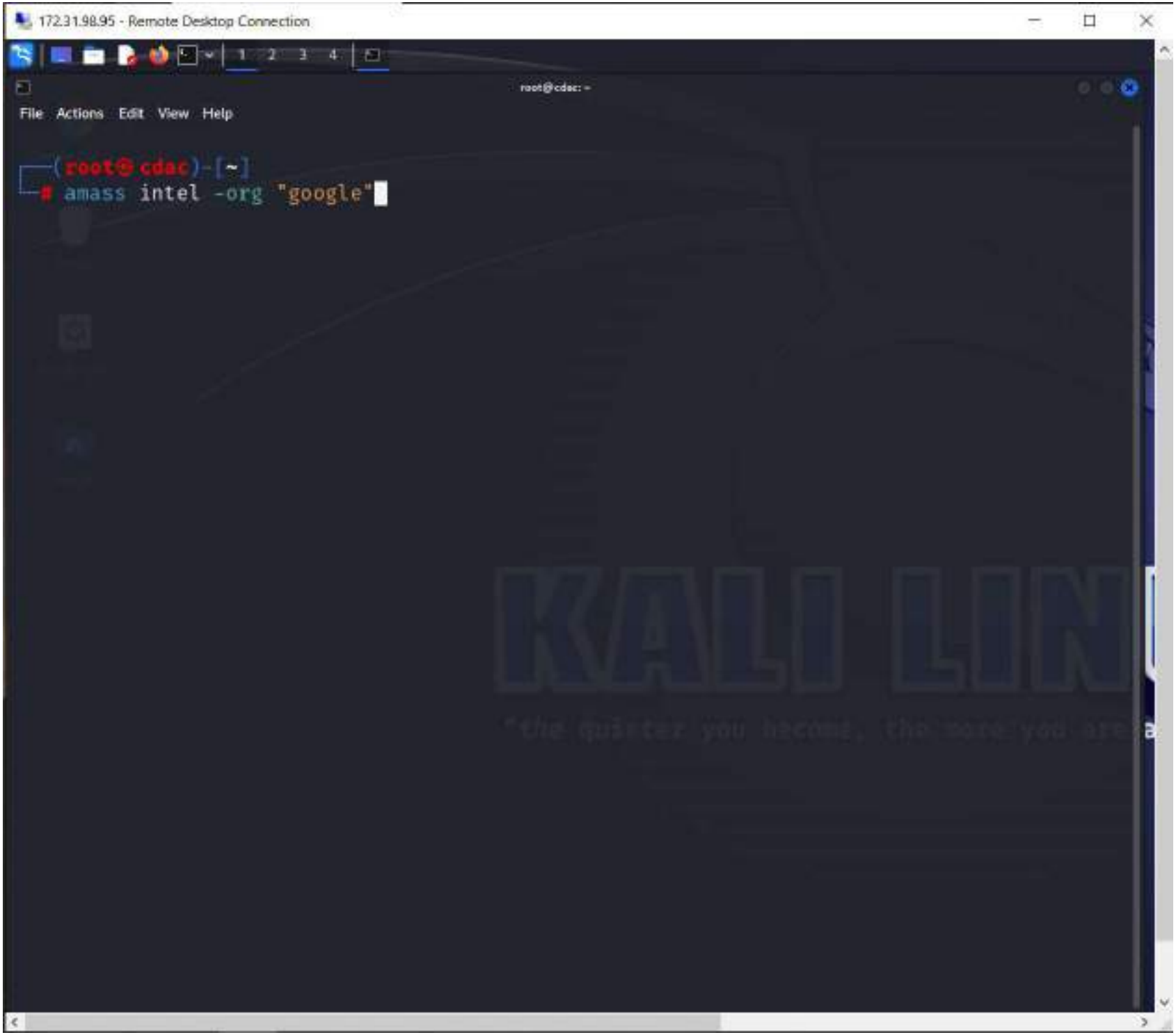

172.31.98.95 - Remote Desktop Connection
root@cdac: ~
File Actions Edit View Help
youtube.cz
birchdenim.com
wwwgoogel.ca
google.com.nf
gstatic.fr
googlenewsarchivesearch.com.cn
googlelabs.fr
youtube.cn
mapsgoogle.fr
googletagmanager.com
google-clips.com
google.vc
picnik.in
wwgoglee.com
blogger.com
g00gle.com
google.ki
adsgoogle.lv
financegoogle.cn
channelintelligence.com
gtoogle.com
pdfium.net
sparrowmailapp.com
googlepages.fr
couponsgoogle.net
google.com.co
gstatic.co
google.co.nz
widevine.com
wallet.com
nest-email.com
root@cdac)-[~]
#

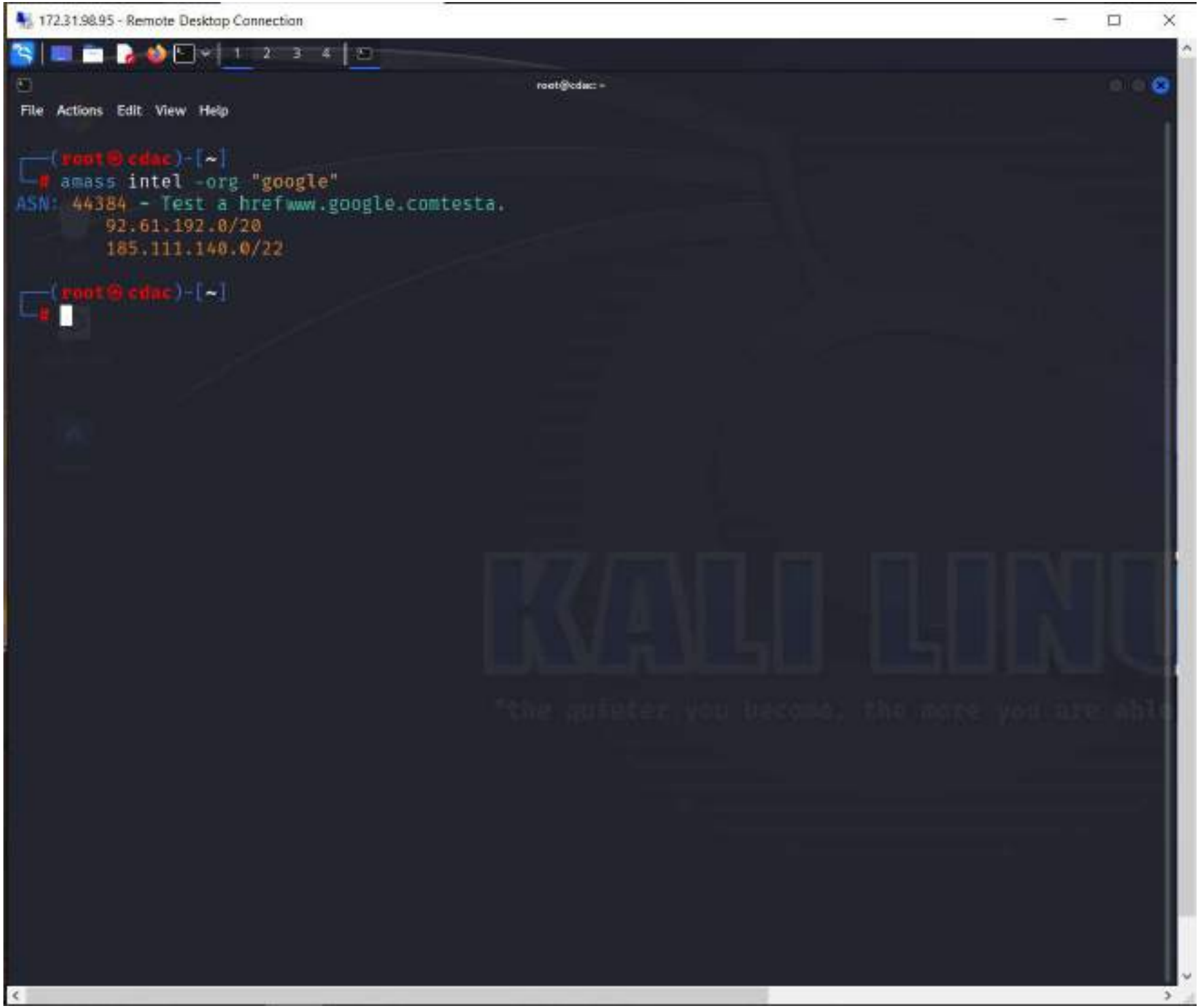

172.31.98.95 - Remote Desktop Connection
1 2 3 4
root@cdac: ~
File Actions Edit View Help
(root㉿cdac)-[~]
amass intel -active -cidr 44.228.249.3/15

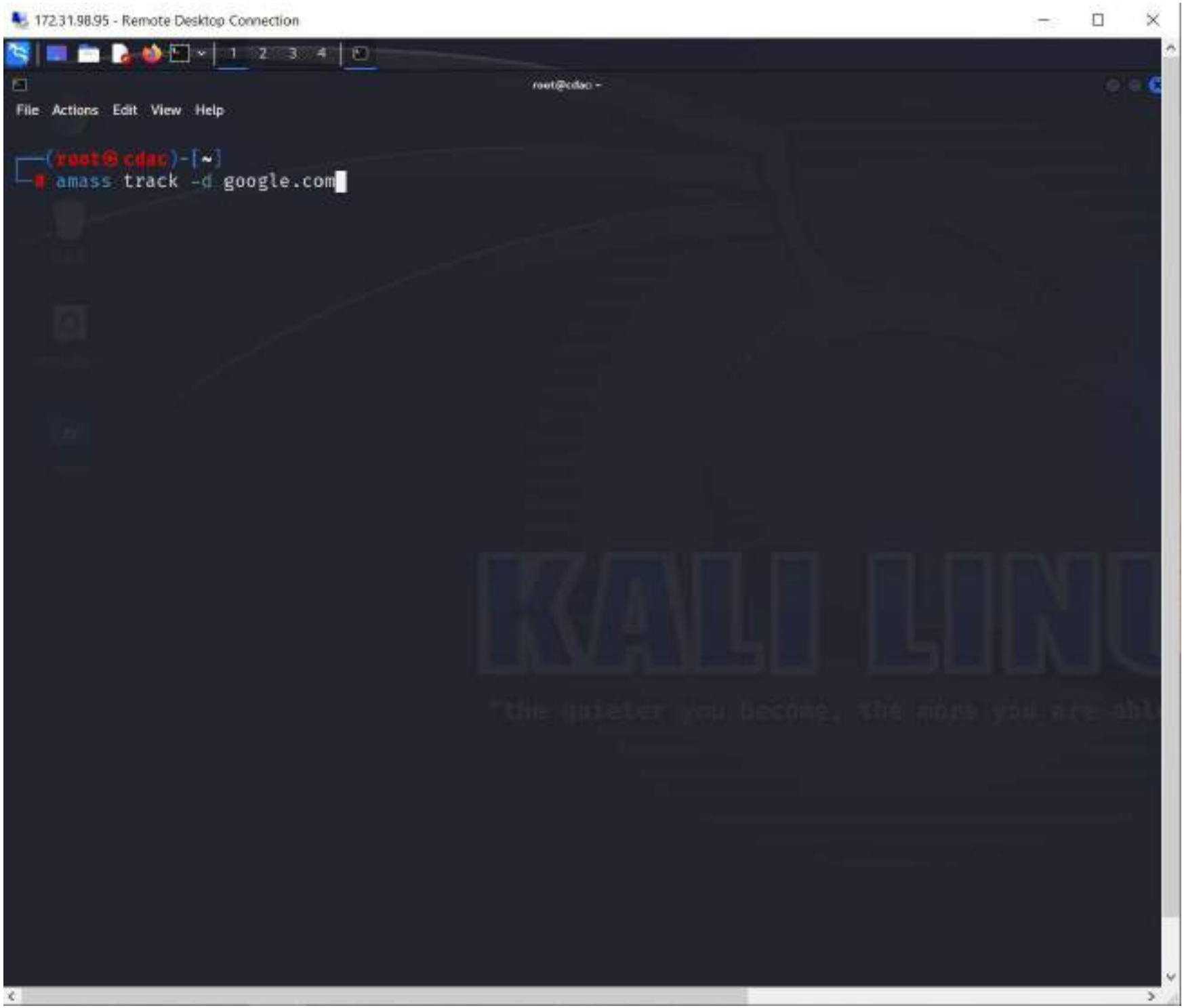

172.31.98.95 - Remote Desktop Connection
1 2 3 4
root@cdac: ~
File Actions Edit View Help
wpengine.com
doctorondemand.com
extrahop.com
amazonaws.com
cluster.local
kubernetes.default
default.svc
compute.internal
portside.aero
fingerprint.dev.us-west-2.iankidde.people.amazon.dev
getindex.com
hallmark.com
aidash.org
regattadata.com
hitachivantara.com
softplanet.com
fastcache.net
sfxresorts.com
gcoregonlive.com
lawkpis.com
inferscience.com
squareup.com
domains.cpa
vnetcap.control.verkada.com
fieldguide.io
itphosting.net
agyletime.io
noseworkmagic.com
nationaljewish.org
pvt-twistbioscience.com
verishop.com
edstockphoto.com
floqast.app

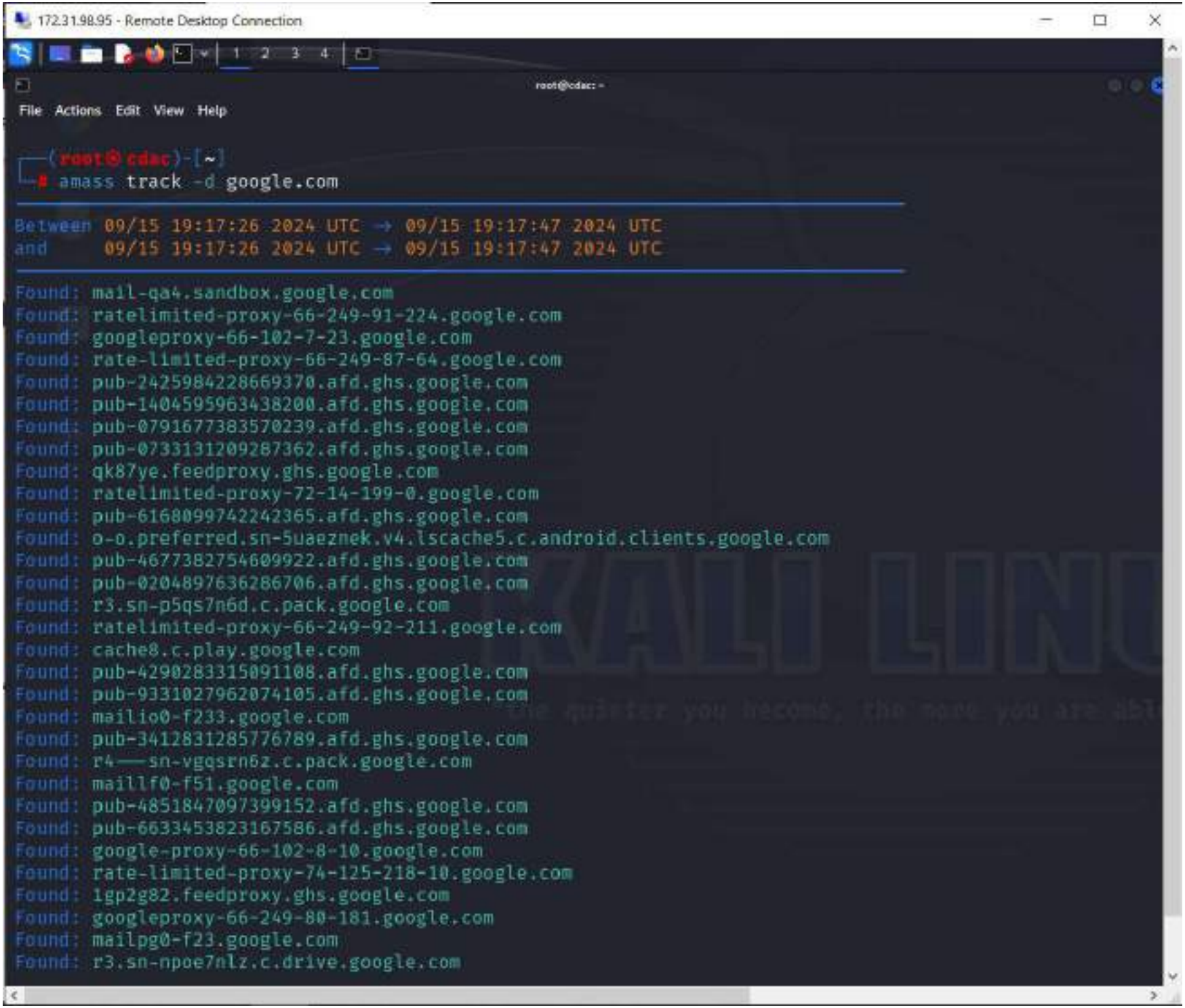

172.31.98.95 - Remote Desktop Connection
1 2 3 4
root@cdac: ~
File Actions Edit View Help
(root㉿cdac)-[~]
amass intel -asn 23314,81323

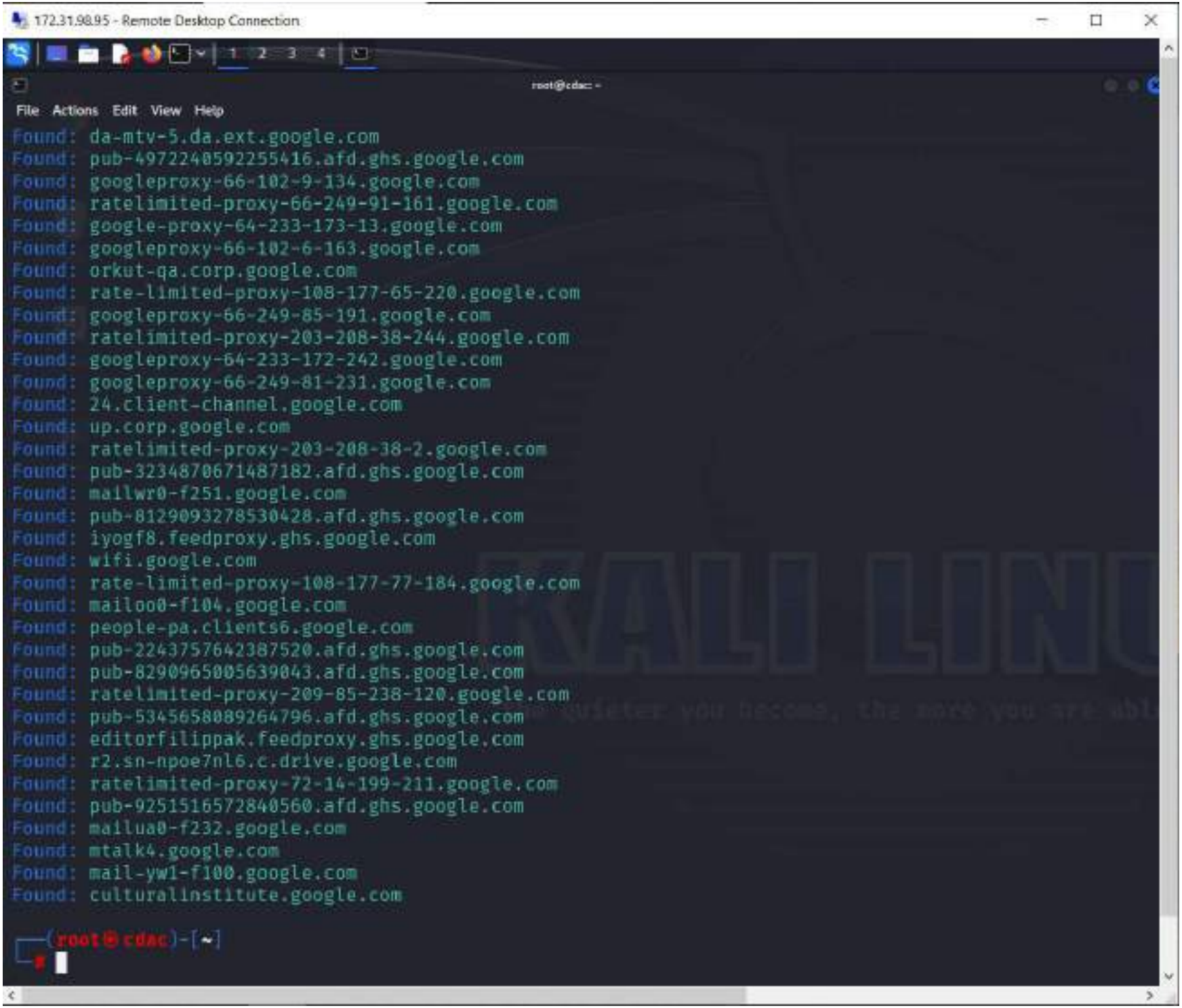

172.31.98.95 - Remote Desktop Connection
1 2 3 4
root@cdac: ~
File Actions Edit View Help
(root㉿cdac)-[~]
amass intel -asn 23314,81323
crystek.com
summit-broadband.com
us-law.com
gulfshoreinsurance.com
wolm.net
gardnerorthopedics.com
farmerandcompany.com
infinitiemployment.com
monalisasuitehotel.com
beautifulmusic.cc
accudata.com
coastal-it.com
retinahealthcenter.com
smaops.com
fishereyecenter.com
mybbi.net
cfl.us.fl.com
joshua.org
nickhotel.com
fidessolutions.com
161.54.216.in-addr.arpa
groveland-fl.gov
fruitlandpark.org
immersiondigital.com
visit.keznews.com
centurylink.net
myalphacloud.net
4avilla.com
lightstogether.com
barnafilms.com


172.31.98.95 - Remote Desktop Connection
1 2 3 4
root@cdac: ~
File Actions Edit View Help
(root㉿cdac)-[~]
amass intel -org "google"


172.31.98.95 - Remote Desktop Connection
1 2 3 4
root@cdac: ~
File Actions Edit View Help
┌──(root㉿cdac)-[~]
└─# amass intel -org "google"
ASN: 44384 - Test a hrefwww.google.comtesta.
92.61.192.0/20
185.111.140.0/22
┌──(root㉿cdac)-[~]
└─#


172.31.98.95 - Remote Desktop Connection
1 2 3 4
root@cdac: ~
File Actions Edit View Help
(root㉿cdac)-[~]
amass track -d google.com


172.31.98.95 - Remote Desktop Connection
1 2 3 4
root@cdac: ~
File Actions Edit View Help
┌──(root㉿cdac)-[~]
└─# amass track -d google.com
Between 09/15 19:17:26 2024 UTC → 09/15 19:17:47 2024 UTC
and 09/15 19:17:26 2024 UTC → 09/15 19:17:47 2024 UTC
Found: mail-qa4.sandbox.google.com
Found: ratelimited-proxy-66-249-91-224.google.com
Found: googleproxy-66-102-7-23.google.com
Found: rate-limited-proxy-66-249-87-64.google.com
Found: pub-2425984228669370.afd.ghs.google.com
Found: pub-1404595963438200.afd.ghs.google.com
Found: pub-0791677383570239.afd.ghs.google.com
Found: pub-0733131209287362.afd.ghs.google.com
Found: qk87ye.feedproxy.ghs.google.com
Found: ratelimited-proxy-72-14-199-0.google.com
Found: pub-6168099742242365.afd.ghs.google.com
Found: o-o.preferred.sn-5uaeznek.v4.lscache5.c.android.clients.google.com
Found: pub-4677382754609922.afd.ghs.google.com
Found: pub-0204897636286706.afd.ghs.google.com
Found: r3.sn-p5qs7n6d.c.pack.google.com
Found: ratelimited-proxy-66-249-92-211.google.com
Found: cache8.c.play.google.com
Found: pub-4290283315091108.afd.ghs.google.com
Found: pub-9331027962074105.afd.ghs.google.com
Found: mailio0-f233.google.com
Found: pub-3412831285776789.afd.ghs.google.com
Found: r4---sn-vgqsrn6z.c.pack.google.com
Found: maillf0-f51.google.com
Found: pub-4851847097399152.afd.ghs.google.com
Found: pub-6633453823167586.afd.ghs.google.com
Found: google-proxy-66-102-8-10.google.com
Found: rate-limited-proxy-74-125-218-10.google.com
Found: igp2g82.feedproxy.ghs.google.com
Found: googleproxy-66-249-80-181.google.com
Found: mailpg0-f23.google.com
Found: r3.sn-npoe7nlz.c.drive.google.com


172.31.98.95 - Remote Desktop Connection
root@cdac: ~
File Actions Edit View Help
Found: da-mtv-5.da.ext.google.com
Found: pub-4972240592255416.afd.ghs.google.com
Found: googleproxy-66-102-9-134.google.com
Found: ratelimited-proxy-66-249-91-161.google.com
Found: google-proxy-64-233-173-13.google.com
Found: googleproxy-66-102-6-163.google.com
Found: orkut-qa.corp.google.com
Found: rate-limited-proxy-108-177-65-220.google.com
Found: googleproxy-66-249-85-191.google.com
Found: ratelimited-proxy-203-208-38-244.google.com
Found: googleproxy-64-233-172-242.google.com
Found: googleproxy-66-249-81-231.google.com
Found: 24.client-channel.google.com
Found: up.corp.google.com
Found: ratelimited-proxy-203-208-38-2.google.com
Found: pub-3234870671487182.afd.ghs.google.com
Found: mailwr0-f251.google.com
Found: pub-8129093278530428.afd.ghs.google.com
Found: iyogf8.feedproxy.ghs.google.com
Found: wifi.google.com
Found: rate-limited-proxy-108-177-77-184.google.com
Found: mailoo0-f104.google.com
Found: people-pa.clients6.google.com
Found: pub-2243757642387520.afd.ghs.google.com
Found: pub-8290965005639043.afd.ghs.google.com
Found: ratelimited-proxy-209-85-238-120.google.com
Found: pub-5345658089264796.afd.ghs.google.com
Found: editorfilippak.feedproxy.ghs.google.com
Found: r2.sn-npoe7nl6.c.drive.google.com
Found: ratelimited-proxy-72-14-199-211.google.com
Found: pub-9251516572840560.afd.ghs.google.com
Found: mailua0-f232.google.com
Found: mtalk4.google.com
Found: mail-yw1-f100.google.com
Found: culturalinstitute.google.com
(root㉿cdac)-[~]
#