📁

steps

https://www.varonis.com/blog/dns-cache-poisoning

▼ browser installation

1. install firefox with https://leimao.github.io/blog/Docker-Container-GUI-Display/ on victim
2. https://collabnix.com/running-firefox-in-docker-container/
3. https://github.com/sameersbn/docker-browser-box

1. goto Labsetup folder and list everything
2. `dcbuild` t1 will build the images from the docker-compose file
3. `dcup` t1 will compose the machines with the networks
4. `dockps` t2 in new terminal will list the docker processes or containers
5. open 6 terminals to the right of t2, swap t2 with t3
6. `docksh user-10.9.0.5` t4 open bash for victim user
7. `export PS1="user-10.9.0.5:\w\n\$> "` t4 on victim user
8. `docksh local-dns-server-10.9.0.53` t5 open bash for local DNS server
9. `export PS1="local-dns-server-10.9.0.53:\w\n\$> "` t5 on local DNS server
10. `docksh attacker-ns-10.9.0.153` t6 open bash for attacker NS
11. `export PS1="attacker-ns-10.9.0.153:\w\n\$> "` t6 on attacker NS
12. `docksh seed-attacker` t7 for seed attacker
13. `export PS1="seed-attacker:\w\n\$> "` t7 on seed attacker
14. `docksh seed-router` t8 for seed router
15. `export PS1="seed-router:\w\n\$> "` t8 on seed router

16. `cat /etc/resolv.conf` t4
17. `ls /etc` t5
18. `cd /etc/bind` t5
19. `ls` t5
20. `cat named.conf` t5 to see zone and bindings and forwarders
21. `cat named.conf.options` t5 to show source port and db dumb
22. `ls /var/cache/bind` t5
23. `rndc dumpdb -cache` t5
24. `ls /var/cache/bind` t5 to check dumpdb has been added to cache
25. `cat /var/cache/bind/dump.db` t5
26. `rndc flush` t5 to flush recent cache binding
27. `cd /etc/bind` t6
28. `ls` t6
29. `cat named.conf` t6 to see zone and bindings and forwarders
30. `cat zone_attacker32.com` t6 to see A entries for DNS
31. `cat zone_example.com` t6 to compare IP mappings with attacker domain
32. `cd volumes` t7 attacker
33. `ls` t7 to see existing scripts
34. explain about dig command
35. `dig ns.attacker32.com` t4 victim
36. `dig www.example.com.` t4 victim
37. check on nslookup.com for www.example.com
38. `dig @ns.attacker32.com www.example.com` t4
39. `rndc dumpdb -cache` t5
40. `cat /var/cache/bind/dump.db` t5 with some extra A entries, show how NS for example domain reflect IP

41. `cat /var/cache/bind/dump.db | grep example` t5 to grep example entries
42. `dig www.example.com.` t4 victim
43. `cd volumes` t2
44. `cp dns_sniff_spoof.py task1.py` t2
45. `gedit * &>/dev/null &` t2
46. ==================task 1 start===
47. edit file task1

    ▼ steps to edit file

    1. domain in line 5 to com
    2. pck show in line 6
    3. line 15 rdata='1.1.1.1'
    4. remove authority and additional section
    5. remove ns and change ancount, arcount in DNSpkt
    6. change filter to host last
    7. change interface to attacker machine starting like with `ip a` or `ifconfig` t7 br- having `10.9.0.1` (IP of attacker)

48. `ls` t7
49. `rndc flush` t5
50. `./task1.py` t7
51. `dig www.example.com` t4 victim now show A in answer section should change to 1.1.1.1 that we gave in the task1 script
52. show on t7 that packet has been sent
53. `ip a` t8 copy 10
54. `tc qdisc show dev eth0` t8 from above command to show no queue by default in router
55. `tc qdisc add dev eth0 root netem delay 100ms` t8 to add delay in network traffic

56. `tc qdisc show dev eth0` t8 will show new entry in tc with delay
57. `tc qdisc del dev eth0 root netem` t8
58. `tc qdisc add dev eth0 root netem delay 100ms` t8
59. `tc qdisc show dev eth0` t8 will show new netem ID 8002 instead of 8001
60. `rndc flush` t5
61. `CTRL+c` t7 stop the running script task1
62. ==================task 1 done===14:09
63. `cp task1.py task2.py` t2
64. `gedit task2.py &>/dev/null &` t2
65. edit file task2

    ▼ steps

    1. local DNS server IP copy and paste into task2 filter after host
    2. replace interface of attacker

66. `./task2.py` t7 sent 1 packets
67. `dig www.example.com` t4 show src IP
68. `rndc dumpdb -cache` t5
69. `cat /var/cache/bind/dump.db | grep example` t5 with fake IP address can now be seen
70. `dig www.example.com` t4 show src IP
71. `cp task2.py task3.py` t2
72. `gedit task3.py &>/dev/null &` t2
73. edit file task3

    ▼ steps

    1. change NSsec1 to ns.attacker32.com

74. `CTRL+c` t7 stop the running script task2
75. ==================task 2 done===14:30
76. `rndc flush` t5

77. `./task3.py` t7
78. `dig www.example.com` t4
79. `rndc dumpdb -cache` t5
80. `cat /var/cache/bind/dump.db | grep example` t5 will point to ns attacker now with spoofed IP
81. `dig www.example.com` t4
82. `dig example.com` t4 show answer section
83. `dig ftp.example.com` t4 show in answer section 1.2.3.6
84. `cat /var/cache/bind/dump.db | grep attacker` t5
85. `dig ns.attacker32.com` t4 show in answer section 10.9.0.153
86. show packet sent in t7
87. show zone on top t5
88. ==================new meeting 3 14:40