sysman@ubuntu20:~$ nmap -iL subnets.txt -T4 -oN scan\_results.txt

Starting Nmap 7.80 ( https://nmap.org ) at 2024-10-15 15:05 UTC

Nmap scan report for 92.50.237.82

Host is up (0.0039s latency).

Not shown: 995 closed ports

PORT STATE SERVICE

22/tcp filtered ssh

23/tcp filtered telnet

1720/tcp filtered h323q931

5060/tcp filtered sip

5061/tcp filtered sip-tls

Nmap scan report for 46.61.182.161

Host is up (0.0035s latency).

Not shown: 995 closed ports

PORT STATE SERVICE

22/tcp filtered ssh

23/tcp filtered telnet

1720/tcp filtered h323q931

5060/tcp filtered sip

5061/tcp filtered sip-tls

Nmap scan report for 195.43.34.179

Host is up (0.019s latency).

Not shown: 999 filtered ports

PORT STATE SERVICE

80/tcp open http

Nmap scan report for 195.43.34.6

Host is up (0.015s latency).

Not shown: 995 closed ports

PORT STATE SERVICE

22/tcp filtered ssh

23/tcp filtered telnet

443/tcp filtered https

444/tcp filtered snpp

5061/tcp filtered sip-tls

Nmap scan report for 195.43.34.17

Host is up (0.015s latency).

Not shown: 997 closed ports

PORT STATE SERVICE

22/tcp filtered ssh

23/tcp filtered telnet

443/tcp open https

Nmap scan report for 195.43.34.19

Host is up (0.015s latency).

Not shown: 996 closed ports

PORT STATE SERVICE

22/tcp filtered ssh

23/tcp filtered telnet

443/tcp open https

5061/tcp filtered sip-tls

Nmap scan report for 195.43.34.20

Host is up (0.016s latency).

Not shown: 997 closed ports

PORT STATE SERVICE

22/tcp filtered ssh

23/tcp filtered telnet

443/tcp open https

Nmap scan report for 195.43.34.28

Host is up (0.022s latency).

Not shown: 999 filtered ports

PORT STATE SERVICE

443/tcp open https

Nmap scan report for 195.43.34.90

Host is up (0.015s latency).

Not shown: 998 closed ports

PORT STATE SERVICE

22/tcp filtered ssh

23/tcp filtered telnet

Nmap scan report for 195.43.34.91

Host is up (0.016s latency).

Not shown: 998 closed ports

PORT STATE SERVICE

22/tcp filtered ssh

23/tcp filtered telnet

Nmap scan report for 195.43.34.174

Host is up (0.019s latency).

Not shown: 999 filtered ports

PORT STATE SERVICE

443/tcp open https

Nmap scan report for 95.167.235.67

Host is up (0.072s latency).

Not shown: 998 filtered ports

PORT STATE SERVICE

80/tcp open http

443/tcp open https

Nmap scan report for 84.42.98.253

Host is up (0.038s latency).

Not shown: 998 filtered ports

PORT STATE SERVICE

80/tcp open http

443/tcp open https

Nmap scan report for 188.19.69.58

Host is up (0.028s latency).

Not shown: 899 closed ports, 99 filtered ports

PORT STATE SERVICE

80/tcp open http

443/tcp open https

Nmap scan report for 95.167.234.11

Host is up (0.033s latency).

Not shown: 999 filtered ports

PORT STATE SERVICE

443/tcp open https

Nmap scan report for 95.167.235.129

Host is up (0.041s latency).

All 1000 scanned ports on 95.167.235.129 are closed

Nmap scan report for 94.25.119.66

Host is up (0.034s latency).

All 1000 scanned ports on 94.25.119.66 are closed

Nmap scan report for 195.43.32.1

Host is up (0.044s latency).

All 1000 scanned ports on 195.43.32.1 are closed

Nmap scan report for 195.43.32.2

Host is up (0.034s latency).

All 1000 scanned ports on 195.43.32.2 are closed

Nmap scan report for 195.43.32.3

Host is up (0.051s latency).

All 1000 scanned ports on 195.43.32.3 are closed

Nmap scan report for 195.43.32.5

Host is up (0.033s latency).

All 1000 scanned ports on 195.43.32.5 are closed

Nmap scan report for 195.43.32.6

Host is up (0.033s latency).

All 1000 scanned ports on 195.43.32.6 are closed

Nmap scan report for 195.43.32.45

Host is up (0.035s latency).

Not shown: 998 filtered ports

PORT STATE SERVICE

443/tcp open https

5061/tcp open sip-tls

Nmap scan report for 195.43.32.46

Host is up (0.035s latency).

Not shown: 999 filtered ports

PORT STATE SERVICE

443/tcp open https

Nmap scan report for 195.43.32.47

Host is up (0.036s latency).

Not shown: 999 filtered ports

PORT STATE SERVICE

443/tcp open https

Nmap scan report for 195.43.32.71

Host is up (0.037s latency).

Not shown: 999 filtered ports

PORT STATE SERVICE

80/tcp open http

Nmap scan report for 95.167.234.130

Host is up (0.0035s latency).

Not shown: 995 closed ports

PORT STATE SERVICE

23/tcp filtered telnet

1720/tcp filtered h323q931

5060/tcp filtered sip

5061/tcp filtered sip-tls

8291/tcp filtered unknown

Nmap scan report for 188.254.103.90

Host is up (0.0033s latency).

Not shown: 995 closed ports

PORT STATE SERVICE

23/tcp filtered telnet

1720/tcp filtered h323q931

5060/tcp filtered sip

5061/tcp filtered sip-tls

8291/tcp filtered unknown

Nmap done: 1217 IP addresses (28 hosts up) scanned in 23.01 seconds

Web

Discovered open port 80/tcp on 195.43.34.179

Discovered open port 443/tcp on 195.43.34.28

Discovered open port 443/tcp on 195.43.34.17

Discovered open port 443/tcp on 195.43.34.19

Discovered open port 443/tcp on 195.43.34.20 ??????

Discovered open port 443/tcp on 195.43.34.174 ?????

Discovered open port 443/tcp on 95.167.235.67

Discovered open port 80/tcp on 95.167.235.67 + ???????

Discovered open port 80/tcp on 84.42.98.253 +

Discovered open port 443/tcp on 84.42.98.253-blog.it-kb.ru +

Discovered open port 443/tcp on 188.19.69.58 + нифига

Discovered open port 80/tcp on 188.19.69.58 + нифига

Discovered open port 443/tcp on 95.167.234.11 + МС сервер нифига

Discovered open port 443/tcp on 195.43.32.45 +- нифига

Discovered open port 443/tcp on 195.43.32.46 ?

Discovered open port 80/tcp on 195.43.32.71 ASP.net + нифига(xss может быть)

Discovered open port 443/tcp on 195.43.32.47 - нифига

Fuzzing

Target: https://**95.167.234.11**/

[09:11:52] Starting:

[09:12:41] 301 - 227B - /aspnet\_client -> https://95.167.234.11/aspnet\_client/

Added to the queue: aspnet\_client/

[09:14:45] Starting: aspnet\_client/

Task Completed

Target: http://**195.43.32.71**/

[11:37:06] Starting:

[11:37:37] 302 - 130B - /ADMIN -> /ADMIN/ALogin

[11:37:37] 302 - 130B - /admin -> /admin/ALogin

[11:37:37] 302 - 130B - /Admin -> /Admin/ALogin

[11:37:38] 302 - 130B - /Admin/ -> /Admin/ALogin

[11:37:38] 302 - 130B - /admin/ -> /admin/ALogin

[11:37:39] 302 - 130B - /admin/index -> /admin/ALogin

[11:38:10] 301 - 151B - /content -> http://195.43.32.71/content/

Added to the queue: content/

[11:38:21] 200 - 31KB - /favicon.ico

[11:38:22] 301 - 149B - /files -> http://195.43.32.71/files/

Added to the queue: files/

[11:38:23] 301 - 149B - /fonts -> http://195.43.32.71/fonts/

Added to the queue: fonts/

[11:38:27] 200 - 1KB - /home

[11:38:38] 301 - 148B - /logs -> http://195.43.32.71/logs/

Added to the queue: logs/

[11:39:02] 301 - 151B - /scripts -> http://195.43.32.71/scripts/

Added to the queue: scripts/

[11:39:04] 301 - 152B - /services -> http://195.43.32.71/services/

Added to the queue: services/

[11:39:23] 301 - 149B - /video -> http://195.43.32.71/video/

Added to the queue: video/

[11:39:32] Starting: content/

[11:39:36] 301 - 154B - /content/js -> http://195.43.32.71/content/js/

Added to the queue: content/js/

[11:40:37] 301 - 155B - /content/css -> http://195.43.32.71/content/css/

Added to the queue: content/css/

[11:40:48] 301 - 157B - /content/fonts -> http://195.43.32.71/content/fonts/

Added to the queue: content/fonts/

[11:40:54] 301 - 155B - /content/img -> http://195.43.32.71/content/img/

Added to the queue: content/img/

[11:41:08] 301 - 158B - /content/mobile -> http://195.43.32.71/content/mobile/

Added to the queue: content/mobile/

[11:41:31] 301 - 158B - /content/shared -> http://195.43.32.71/content/shared/

Added to the queue: content/shared/

[11:41:57] Starting: files/

[11:44:25] Starting: fonts/

[11:47:05] Starting: logs/

[11:48:40] 200 - 641KB - /logs/logfile.txt

[11:49:39] Starting: scripts/

[11:50:30] 301 - 155B - /scripts/app -> http://195.43.32.71/scripts/app/

Added to the queue: scripts/app/

[11:52:07] Starting: services/

[11:54:39] Starting: video/

[11:57:07] Starting: content/js/

[11:58:15] 200 - 3KB - /content/js/demo.js

[11:58:56] 301 - 162B - /content/js/plugins -> http://195.43.32.71/content/js/plugins/

Added to the queue: content/js/plugins/

[11:59:34] Starting: content/css/

[12:01:40] 301 - 161B - /content/css/skins -> http://195.43.32.71/content/css/skins/

Added to the queue: content/css/skins/

[12:02:05] Starting: content/fonts/

[12:04:30] Starting: content/img/

[12:07:14] Starting: content/mobile/

[12:08:05] 301 - 163B - /content/mobile/apps -> http://195.43.32.71/content/mobile/apps/

Added to the queue: content/mobile/apps/

[12:08:38] 301 - 165B - /content/mobile/images -> http://195.43.32.71/content/mobile/images/

Added to the queue: content/mobile/images/

[12:08:48] 301 - 164B - /content/mobile/logos -> http://195.43.32.71/content/mobile/logos/

Added to the queue: content/mobile/logos/

[12:08:58] 301 - 167B - /content/mobile/overview -> http://195.43.32.71/content/mobile/overview/

Added to the queue: content/mobile/overview/

[12:09:17] 301 - 165B - /content/mobile/shared -> http://195.43.32.71/content/mobile/shared/

Added to the queue: content/mobile/shared/

[12:09:45] Starting: content/shared/

[12:11:02] 301 - 164B - /content/shared/fonts -> http://195.43.32.71/content/shared/fonts/

Added to the queue: content/shared/fonts/

[12:11:07] 301 - 164B - /content/shared/icons -> http://195.43.32.71/content/shared/icons/

Added to the queue: content/shared/icons/

[12:11:08] 301 - 165B - /content/shared/images -> http://195.43.32.71/content/shared/images/

Added to the queue: content/shared/images/

[12:11:21] 301 - 163B - /content/shared/menu -> http://195.43.32.71/content/shared/menu/

Added to the queue: content/shared/menu/

[12:12:16] Starting: scripts/app/

[12:13:19] 200 - 575B - /scripts/app/common.js

[12:14:47] Starting: content/js/plugins/

[12:15:44] 301 - 172B - /content/js/plugins/Bootstrap -> http://195.43.32.71/content/js/plugins/Bootstrap/

Added to the queue: content/js/plugins/Bootstrap/

[12:17:18] Starting: content/css/skins/

[12:19:47] Starting: content/mobile/apps/

[12:22:13] Starting: content/mobile/images/

[12:25:01] Starting: content/mobile/logos/

[12:28:11] Starting: content/mobile/overview/

[12:31:21] Starting: content/mobile/shared/

[12:34:04] 301 - 171B - /content/mobile/shared/skins -> http://195.43.32.71/content/mobile/shared/skins/

Added to the queue: content/mobile/shared/skins/

[12:34:32] Starting: content/shared/fonts/

[12:37:48] Starting: content/shared/icons/

[12:38:14] 301 - 167B - /content/shared/icons/16 -> http://195.43.32.71/content/shared/icons/16/

Added to the queue: content/shared/icons/16/

[12:40:34] 301 - 171B - /content/shared/icons/sports -> http://195.43.32.71/content/shared/icons/sports/

Added to the queue: content/shared/icons/sports/

[12:41:12] Starting: content/shared/images/

[12:43:13] 301 - 171B - /content/shared/images/logos -> http://195.43.32.71/content/shared/images/logos/

Added to the queue: content/shared/images/logos/

[12:43:28] 301 - 172B - /content/shared/images/photos -> http://195.43.32.71/content/shared/images/photos/

Added to the queue: content/shared/images/photos/

[12:44:22] Starting: content/shared/menu/

[12:47:31] Starting: content/js/plugins/Bootstrap/

[12:50:06] Starting: content/mobile/shared/skins/

[12:52:47] Starting: content/shared/icons/16/

[12:55:18] Starting: content/shared/icons/sports/

[12:57:52] Starting: content/shared/images/logos/

[13:00:38] Starting: content/shared/images/photos/

Task Completed

Target: http://**188.19.69.58**/

[09:20:11] Starting:

[### ] 16% 1913/11731 105/s job:1/1 errors:292Exception in thread Thread-23:

[09:25:19] 301 - 178B - /admin -> http://188.19.69.58/admin/

Added to the queue: admin/

[09:33:47] 200 - 2KB - /examples/jsp/%252e%252e/%252e%252e/manager/html/

Added to the queue: examples/jsp/%252e%252e/%252e%252e/manager/html/

[09:35:44] 200 - 612B - /index.html

[09:38:47] 301 - 178B - /oauth -> http://188.19.69.58/oauth/

Added to the queue: oauth/

[09:47:51] Starting: admin/

[09:49:48] 200 - 2KB - /admin/examples/jsp/%252e%252e/%252e%252e/manager/html/

Added to the queue: admin/examples/jsp/%252e%252e/%252e%252e/manager/html/

[09:52:09] Starting: examples/jsp/%252e%252e/%252e%252e/manager/html/

[09:56:31] Starting: oauth/

[09:58:21] 200 - 2KB - /oauth/examples/jsp/%252e%252e/%252e%252e/manager/html/

Added to the queue: oauth/examples/jsp/%252e%252e/%252e%252e/manager/html/

[10:00:57] Starting: admin/examples/jsp/%252e%252e/%252e%252e/manager/html/

[10:05:37] Starting: oauth/examples/jsp/%252e%252e/%252e%252e/manager/html/

Task Completed

===============================================================

Gobuster v3.6

by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

===============================================================

[+] Domain: it-kb.ru

[+] Threads: 10

[+] Timeout: 1s

[+] Wordlist: Desktop/directory-list-2.3-big.txt

===============================================================

Starting gobuster in DNS enumeration mode

===============================================================

Found: blog.it-kb.ru

Found: forum.it-kb.ru

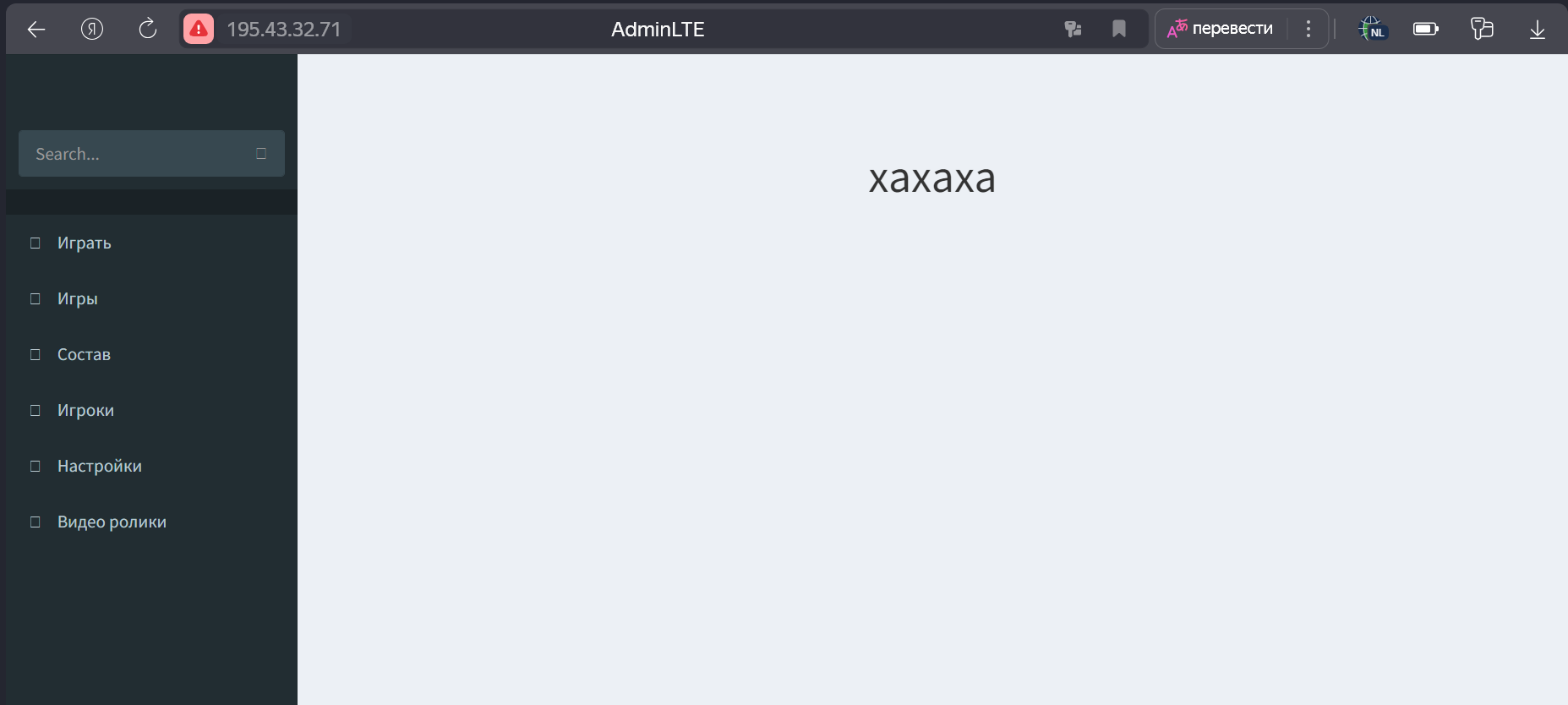
Found: wiki.it-kb.ru

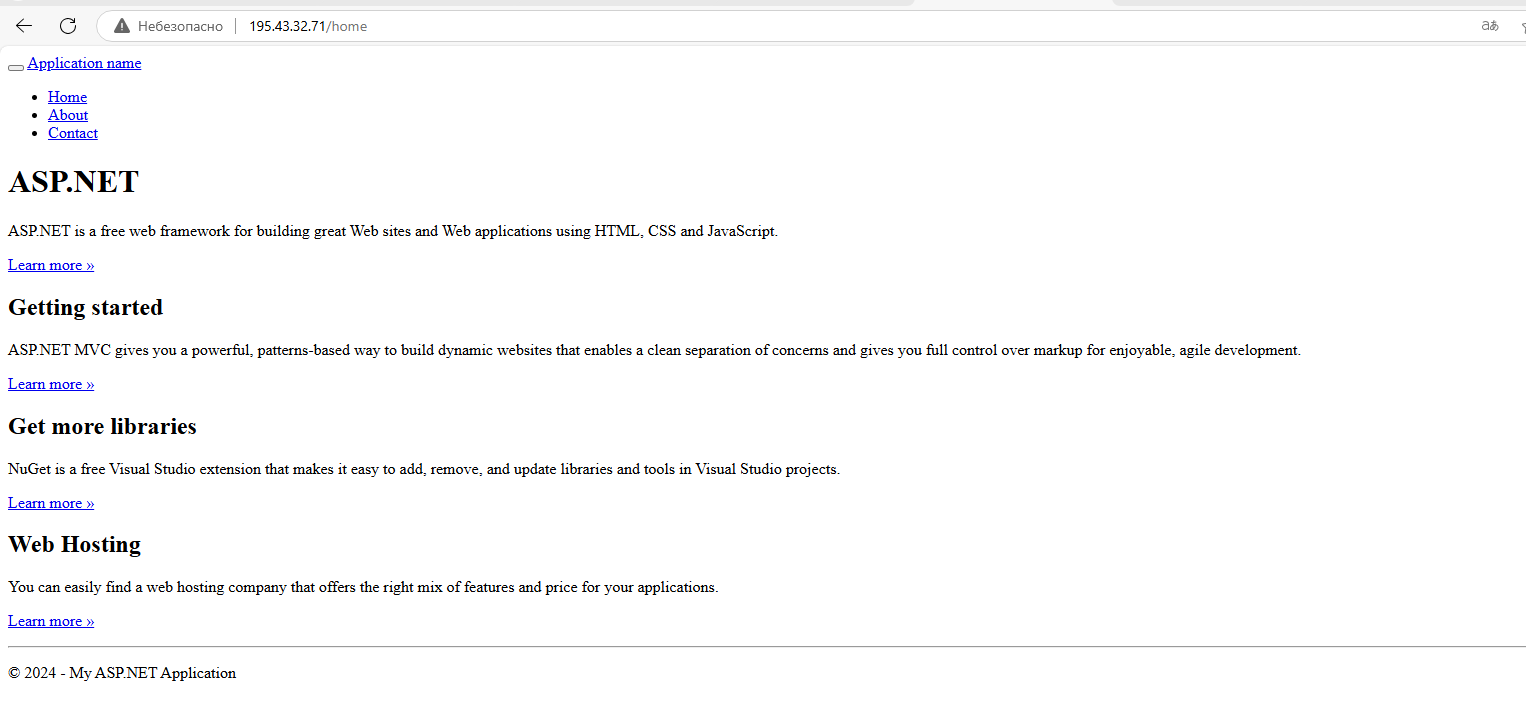
Found: test.it-kb.ru

Found: Blog.it-kb.ru

Found: WWW.it-kb.ru

Found: Wiki.it-kb.ru





Blog.it-kb.ru/ wp-json/wp/v2/users/





