# Nmap 7.80 scan initiated Fri Oct 29 20:35:09 2021 as: nmap -Pn --script vuln -oN 192.168.1.110-vuln.txt 192.168.1.110

Nmap scan report for 192.168.1.110

Host is up (0.00073s latency).

Not shown: 995 closed ports

PORT STATE SERVICE

22/tcp open ssh

|\_clamav-exec: ERROR: Script execution failed (use -d to debug)

80/tcp open http

|\_clamav-exec: ERROR: Script execution failed (use -d to debug)

| http-csrf:

| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.1.110

| Found the following possible CSRF vulnerabilities:

|

| Path: http://192.168.1.110:80/

| Form id:

| Form action: https://spondonit.us12.list-manage.com/subscribe/post?u=1462626880ade1ac87bd9c93a&id=92a4423d01

|

| Path: http://192.168.1.110:80/service.html

| Form id:

| Form action: https://spondonit.us12.list-manage.com/subscribe/post?u=1462626880ade1ac87bd9c93a&id=92a4423d01

|

| Path: http://192.168.1.110:80/index.html

| Form id:

|\_ Form action: https://spondonit.us12.list-manage.com/subscribe/post?u=1462626880ade1ac87bd9c93a&id=92a4423d01

|\_http-dombased-xss: Couldn't find any DOM based XSS.

| http-enum:

| /wordpress/: Blog

| /wordpress/wp-login.php: Wordpress login page.

| /css/: Potentially interesting directory w/ listing on 'apache/2.4.10 (debian)'

| /img/: Potentially interesting directory w/ listing on 'apache/2.4.10 (debian)'

| /js/: Potentially interesting directory w/ listing on 'apache/2.4.10 (debian)'

| /manual/: Potentially interesting folder

|\_ /vendor/: Potentially interesting directory w/ listing on 'apache/2.4.10 (debian)'

|\_http-stored-xss: Couldn't find any stored XSS vulnerabilities.

111/tcp open rpcbind

|\_clamav-exec: ERROR: Script execution failed (use -d to debug)

139/tcp open netbios-ssn

|\_clamav-exec: ERROR: Script execution failed (use -d to debug)

445/tcp open microsoft-ds

|\_clamav-exec: ERROR: Script execution failed (use -d to debug)

MAC Address: 00:15:5D:00:04:10 (Microsoft)

Host script results:

|\_smb-vuln-ms10-054: false

|\_smb-vuln-ms10-061: false

| smb-vuln-regsvc-dos:

| VULNERABLE:

| Service regsvc in Microsoft Windows systems vulnerable to denial of service

| State: VULNERABLE

| The service regsvc in Microsoft Windows 2000 systems is vulnerable to denial of service caused by a null deference

| pointer. This script will crash the service if it is vulnerable. This vulnerability was discovered by Ron Bowes

| while working on smb-enum-sessions.

|\_

# Nmap done at Fri Oct 29 20:35:54 2021 -- 1 IP address (1 host up) scanned in 44.82 seconds