Scans Output

|  |
| --- |
| Nmap Scan Output |
| Scan Information: ====================================================================== Scan Arguments: nmap -v -p- -A -oX 10.10.239.111/output/outputNmap.xml 10.10.239.111 Scan Start Time: Tue May 30 14:15:05 2023 Scan Version: 7.93 ====================================================================== Host Information: Host Address: 10.10.239.111 ====================================================================== Open Ports: ---------------------------------------------------------------------------------------------------------------------- Port: 22 Protocol: tcp Service Name: ssh Service Product: OpenSSH Service Version: 7.2p2 Ubuntu 4ubuntu2.8 Scripts ran: -> ssh-hostkey:   2048 cea31283ad8abd1e2c86059861cb258b (RSA)  256 f6ffdcb5b9b03c6c55d2234c8bd310bc (ECDSA)  256 b8cde6a0ab618ba786eeb60e6967c952 (ED25519) ---------------------------------------------------------------------------------------------------------------------- Port: 80 Protocol: tcp Service Name: http Service Product: Apache httpd Service Version: 2.4.18 Scripts ran: -> http-methods:   Supported Methods: GET HEAD POST OPTIONS -> http-title: Site doesn't have a title (text/html). -> http-server-header: Apache/2.4.18 (Ubuntu) ---------------------------------------------------------------------------------------------------------------------- Port: 1234 Protocol: tcp Service Name: http Service Product: Apache Tomcat/Coyote JSP engine Service Version: 1.1 Scripts ran: -> http-title: Apache Tomcat/7.0.88 -> http-favicon: Apache Tomcat -> http-methods:   Supported Methods: GET HEAD POST OPTIONS -> http-server-header: Apache-Coyote/1.1 ---------------------------------------------------------------------------------------------------------------------- Port: 8009 Protocol: tcp Service Name: ajp13 Service Product: Apache Jserv Service Version: None Scripts ran: -> ajp-methods: Failed to get a valid response for the OPTION request ---------------------------------------------------------------------------------------------------------------------- ====================================================================== |

|  |
| --- |
| Nikto Scan Output |
| Scan Information: ====================================================================== Target IP: 10.10.239.111 Target hostname: 10.10.239.111 Target port: 80 Scan start time: 2023-05-30 14:15:52 ====================================================================== Items: ---------------------------------------------------------------------------------------------------------------------- Method: GET Description: /: The anti-clickjacking X-Frame-Options header is not present. URI: / Reference: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options ---------------------------------------------------------------------------------------------------------------------- Method: GET Description: /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. URI: / Reference: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/ ---------------------------------------------------------------------------------------------------------------------- Method: HEAD Description: Apache/2.4.18 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch. URI: / Reference: Reference not available ---------------------------------------------------------------------------------------------------------------------- Method: GET Description: /: Server may leak inodes via ETags, header found with file /, inode: a8, size: 583d315d43a92, mtime: gzip. URI: / Reference: CVE-2003-1418 ---------------------------------------------------------------------------------------------------------------------- Method: OPTIONS Description: OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, OPTIONS . URI: / Reference: Reference not available ---------------------------------------------------------------------------------------------------------------------- Method: GET Description: /icons/README: Apache default file found. URI: /icons/README Reference: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/ ---------------------------------------------------------------------------------------------------------------------- ====================================================================== |

|  |
| --- |
| Dirbuster Scan Output |
| ----------------- DIRB v2.22  By The Dark Raver -----------------  OUTPUT\_FILE: 10.10.239.111/output/outputDirb.txt START\_TIME: Tue May 30 14:20:15 2023 URL\_BASE: http://10.10.239.111/ WORDLIST\_FILES: /usr/share/dirb/wordlists/common.txt  -----------------  GENERATED WORDS: 4612  ---- Scanning URL: http://10.10.239.111/ ---- ==> DIRECTORY: http://10.10.239.111/guidelines/ + http://10.10.239.111/index.html (CODE:200|SIZE:168) + http://10.10.239.111/protected (CODE:401|SIZE:460) + http://10.10.239.111/server-status (CODE:403|SIZE:301)  ---- Entering directory: http://10.10.239.111/guidelines/ ---- + http://10.10.239.111/guidelines/index.html (CODE:200|SIZE:51)  ----------------- END\_TIME: Tue May 30 14:25:05 2023 DOWNLOADED: 9224 - FOUND: 4 |

Captured Screenshots

|  |
| --- |
| Screenshot: 10.10.239.111/screenshots/http...10.10.239.111.guidelines.index.html.png |
|  |

|  |
| --- |
| Screenshot: 10.10.239.111/screenshots/http...10.10.239.111.protected.png |
|  |

|  |
| --- |
| Screenshot: 10.10.239.111/screenshots/http...10.10.239.111.index.html.png |
|  |

Created wordlist

Unfortunately  
ToolsRUs  
is  
down  
for  
upgrades  
Other  
parts  
of  
the  
website  
is  
still  
functional  
Hey  
bob  
did  
you  
update  
that  
TomCat  
server

Discovered credentials

bob:bubbles