**EnumerationTool Documentation**

**Location of Tool: //**probably irrelevant

/root/EnumerationTool

**General Purpose:**

This tool is intended to automate full network enumeration using premade tools, custom scripts, and custom programs. The tool also performs extra functions such as file conversions, vulnerability scanning, and database uploading.

**Scripts:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Script Name** | **Location of Script** | **Purpose** | **Inputs** | **Outputs** |
| script.exp | EnumerationTool/Scripts/ | Automate SSH to Switch, execute commands | None | Switch Command outputs. |
| switchPull.sh | EnumerationTool/Scripts/ | Automate SSH connection to switch. | IP, Username, Password | None |
| parseToCsv.py | EnumerationTool/Scripts/ | Use regex to parse switch information for VLANs | Switch running configuration | Switch VLAN information |
| parse\_to\_nmap.py | EnumerationTool/Scripts/ | Parse VLAN information to scan each VLAN with nmap | Parsed Switch VLAN information | Nmap results for all VLANs for a given switch |
| parse\_switch\_info.py | EnumerationTool/Scripts/ | Parse switch information and VLAN IDs | Switch running config | Sw model, IP, VLAN IDs |
| serviceFinder.py | EnumerationTool/Scripts/ | Quick search a given .csv file | .csv file | Search results |
| Logstash\_to\_ElasticSearch.sh | EnumerationTool/Scripts/ | Upload csv files to elasticsearch | .csv file | None |
| Nmap\_xml\_parser.py | EnumerationTool/Scripts/Nmap-Scan-To-Csv/ | Convert nmap xml to csv | Nmap xml results | Nmap csv results |
| switchInfo.py | EnumerationTool/Scripts/ | Use regex to parse switch info | Switch running config | Switch info and vlan IDs |
| Others… | Kali Linux | Dependent on tool | Dependent on tool | Dependent on tool |

**Enumeration Tool Options:**

|  |  |  |
| --- | --- | --- |
| **Option** | **Description** | **Tool/Script/Program** |
| 1 | Scan current subnet for hosts and service | Nmap |
| 2 | Scan current subnet for hosts | Netdiscover |
| 3 | DNS Zone Transfer on a target Domain | Dnsenum |
| 4 | Pull VLAN information from target SW + nmap VLANs | Script.exp, switchpull.sh, parseToCsv.py, parse\_to\_nmap.py |
| 5 | Scan target Server/Domain for Vulnerabilities | Nikto |
| 6 | Scan target IP + Port for FTP vulnerabilities | Nmap |
| 7 | Scan web server/app for directory + file names | Dirbuster |
| 8 | Passive sniffing for interesting files on NIC | Dsniff |
| 9 | Convert a file from XML to CSV | Nmap\_xml\_parser.py |
| 10 | Convert a file from TXT to CSV | “sed” kali tool |
| 11 | Convert a file from XML to HTML | “xsltproc” add on tool |
| 12 | Quick search a CSV file | serviceFinder.py |
| 13 | Upload a CSV file to Elastic | Logstash\_to\_ElasticSearch.sh |