Directory Tree

```
.
├── 01-network-discovery
│   ├── 01-metasploit-credentials.md
│   ├── 01-nmap-discovery.md
│   ├── Final_VAPT_Report - 4.docx
│   ├── OS-detection.png
│   ├── full-audit.png
│   ├── greenbone-set-credentials.png
│   ├── greenbone-set-new-target.png
│   ├── greenbone-set-task.png
│   ├── hosts-discovery.png
│   ├── mestasploit-services-1.png
│   ├── metaexploit.png
│   ├── metasploit-credentials-info-1.png
│   ├── metasploit-credentials-info-2.png
│   ├── metasploit-credentials-info-3.png
│   ├── metasploit-credentials-info-4.png
│   ├── metasploit-documents-1.png
│   ├── metasploit-documents-2.png
│   ├── metasploit-exploit.png
│   ├── metasploit-info-victim.png
│   ├── metasploit-setting-advanced.png
│   ├── metasploit-setting.png
│   ├── metaspoloit-setting-attacker.png
│   ├── meterpreter-ps.png
│   ├── meterpreter-sysinfo.png
│   ├── ms17_verify.png
│   ├── netbios-vulns.png
│   ├── netdiscovery.png
│   ├── nmap-script-vuln.png
│   ├── nmap-sn.png
│   ├── python-script.png
│   ├── results.md
│   ├── rpc-scan.png
│   ├── service-scan.png
│   ├── smb-all-vulns.png
│   ├── smb-enumeration.png
│   ├── smb-vuln-scan.png
│   ├── systemd-verification-installation.png
│   ├── topology.png
│   ├── upnp-services.png
│   └── vulnerability-scan.png
├── 02-web-application-security-testing
│   ├── DVWA-evidence.md
│   ├── Deepaks-steps-sql-injection.png
```

```
│   ├── Final_VAPT_Report - 4.docx
│   ├── SQL-injection-1.png
│   ├── SQL-injection-2.png
│   ├── SQL-injection-3.png
│   ├── SQL-injection-4.png
│   ├── SQL-injection-5.png
│   ├── SQL-injection-column-name.png
│   ├── SQL-injection-order-by-1.png
│   ├── SQL-injection-order-by-2.png
│   ├── SQL-injection-order-by-3.png
│   ├── SQL-injection-schema-name.png
│   ├── SQL-injection-table-name.png
│   ├── SQL-injection-user-password-1.png
│   ├── SQL-injection-user-password-2.png
│   ├── SQL-injection-user-password-3.png
│   ├── XSS-alert-img.png
│   ├── XSS-alert-svg.png
│   ├── XSS-alert.png
│   ├── XSS-reflected-.10-cookies.png
│   ├── XSS-reflected-JS-keylogger.png
│   ├── XSS-reflected-malicious-site-1.png
│   ├── XSS-reflected-malicious-site-2.png
│   ├── XSS-reflected-malicious-site.png
│   ├── XSS-stored-cookies-stealing-1.png
│   ├── XSS-stored-cookies-stealing.png
│   ├── dvwa-low-security.png
│   ├── msfvenom-exploit-1.png
│   ├── msfvenom-exploit-2.png
│   ├── msfvenom-exploit-meterpreter.png
│   ├── msfvenom-exploit-msfconsole-show-options.png
│   ├── msfvenom-exploit-upload.png
│   ├── msfvenom-exploit.png
│   ├── php-webshell-basic.png
│   ├── php-webshell-input-1.png
│   ├── php-webshell-input-2.png
│   ├── php-webshell-input.png
│   ├── php-webshell-ls.png
│   ├── php-webshell-upload.png
│   └── php-webshell-whoami.png
├── 03-password-security-testing-cracking
│   ├── Final_VAPT_Report.docx
│   ├── Victim's-admin-in-crackmapexec.png
│   ├── Victim's-admin-in-smbclient.png
│   ├── Victim's-admin-in.png
│   ├── Window7-vulnerable.png
│   ├── hashcat-1.png
│   ├── hashdump-1.png
│   ├── hydra-1.png
│   ├── net-users.png
```

```
│   ├── parameters-metasploit.png
│   ├── password-security-evidence.md
│   ├── setting-metasploit.png
│   ├── smb-users-eternalblue.png
│   └── wordlist-10-passwords.png
├── 04-forensics-report
│   ├── 8-jpeg-search
│   │   ├── forensics
│   │   │   └── 8-jpeg-search-forensics
│   │   │       ├── evidence
│   │   │       └── reports
│   │   ├── 8-jpeg-search-forensic-copy.dd
│   │   ├── 8-jpeg-search.dd
│   │   ├── COPYING-GNU.txt
│   │   ├── README.txt
│   │   ├── evidence_md5_hash.txt
│   │   ├── evidence_md5_hash_copy.txt
│   │   ├── index.html
│   │   ├── results.md
│   │   └── results.txt
│   ├── Final_VAPT_Report - 4.docx
│   ├── JPG-files-recovered.png
│   ├── add-host-creation.png
│   ├── add-host.png
│   ├── add-new-image.png
│   ├── alloc-files-file1.png
│   ├── alloc-files-file2.png
│   ├── alloc-files.png
│   ├── analysis-image-1.png
│   ├── analysis-image.png
│   ├── archive-files-file10.png
│   ├── archive-files-file8.png
│   ├── archive-files-file9.png
│   ├── archive-files.png
│   ├── autopsy-init-1.png
│   ├── autopsy-init.png
│   ├── calculated-MD5-in-Autopsy.png
│   ├── case-creation-metadata.png
│   ├── case-directory-creation.png
│   ├── case-structure.png
│   ├── deleted-files-file.png
│   ├── deleted-files-file6-report.png
│   ├── deleted-files-file6.png
│   ├── deleted-files-file7-report.png
│   ├── deleted-files.png
│   ├── directory-to-8-jpeg-search.png
│   ├── forensics-report-evidence.md
│   ├── image-reports.png
│   ├── invalid-file-file3.png
```

```
│   ├── invalid-file-file4.png
│   ├── invalid-file-file5.png
│   ├── invalid-files.png
│   ├── md5-sum-verifation-integrity.png
│   ├── md5sum-8-jpg.png
│   ├── misc-files-file13.png
│   ├── misc-files.png
│   ├── search-jpg-results.png
│   └── search-jpg.png
├── password-security-testing-cracking
│   ├── Final_VAPT_Report.docx
│   ├── Victim's-admin-in-crackmapexec.png
│   ├── Victim's-admin-in-smbclient.png
│   ├── Victim's-admin-in.png
│   ├── Window7-vulnerable.png
│   ├── hashcat-1.png
│   ├── hashdump-1.png
│   ├── hydra-1.png
│   ├── net-users.png
│   ├── parameters-metasploit.png
│   ├── password-security-evidence.md
│   ├── setting-metasploit.png
│   ├── smb-users-eternalblue.png
│   └── wordlist-10-passwords.png
├── resources
│   ├── 01-Final_VAPT_Report.pdf
│   ├── 01-greenbone-report-vulnerabilities.pdf
│   ├── 01-metasploit-credentials.pdf
│   ├── 01-nmap-discovery.pdf
│   ├── 02-4-metasploit-credentials.pdf
│   ├── 02-DVWA-evidence.pdf
│   ├── 02-Final_VAPT_Report.pdf
│   ├── 03-password-security-evidence.pdf
│   ├── 03_Final_VAPT_Report.pdf
│   ├── 04-results.pdf
│   ├── Final_VAPT_Report.docx
│   └── Final_VAPT_Report.pdf
├── CYSACapstoneProjectStatement.pdf
├── README.md
├── project_directory_structure.md
├── test.md
└── test1.html

12 directories, 173 files
```
