滲透測試項目與技術

**網路滲透測試**

參考書目

[1]Kali Linux高級滲透測試

[2] Kali Linux滲透測試的藝術

http://www.waterlike.com.tw/bookdata.asp?NO=TP3C155025

[3] Nmap滲透測試指南

http://www.waterlike.com.tw/bookdata.asp?NO=TP3C15C102

[4] Kali Linux滲透測試工具 第二版

http://www.books.com.tw/products/0010696823

[5]安全測試指南（第4版）

http://www.books.com.tw/products/CN11362505

確定目標與偵察技術

|  |  |  |
| --- | --- | --- |
| 測試項目 | 技術 | 參考 |
| 開源情報 | Google Hacking  Yandex搜尋引擎 | [1]2.2 |
| DNS偵察 | WHOIS  Dnswalk  Fierce  dnsmap | [1]2.3 |
| 映射路由到目標 | Traceroute | [1]2.3 |
| 隱形掃描策略 | Metasploit  Tor  Privoxy | [1]3.1 |
| 識別網路基礎設施 | Ldb  Nmap  Shodan搜尋引擎 | [1] 3.2 |
| 列舉主機 | Alive6  Nmap  Nping | [1] 3.2 |
| 指紋識別操作系統 | Nmap  Xprobe2 | [1]3.4 |
| 確定主動服務 | Nmap  Netcat | [1]3.4 |

目標測試與分析

|  |  |  |
| --- | --- | --- |
| 測試項目 | 技術 | 參考 |
| DNS記錄分析 | 4.3.1 host  4.3.2 dig  4.3.3 dnsenum  4.3.4 dnsdict6  4.3.5 fierce  4.3.6 DMitry  4.3.7 Maltego | [2] |
| 路由信息分析 | tcptraceroute  tctrace | [2] |
| 服務枚舉 SMB | smb-check-vulns.nse |  |
| 服務枚舉 SNMP | onesixtyone  snmpcheck | [2]6.4.2 |
| 服務枚舉 VPN枚舉 |  | [2]6.5 |
| 指紋識別操作系統 |  | [1] 3.4.2  [3]4.9 作業系統探測 |
| 確定服務 |  | [1] 3.4.3 |
| 信息收集測試工具集 | httprint  httprecon  Netcraft  Desenmascarame | [5]ch4 4.11 |

漏洞利用與攻擊

|  |  |  |
| --- | --- | --- |
| 測試項目 | 技術 | 參考 |
| 漏洞檢測 |  | [2] ch9 9.1 |
| 漏洞和exploit資料庫 |  | [2] ch9 9.2 |
| 漏洞利用程式工具集 | MSFConsole  MSFCLI | [2] ch9 9.3 |
| MySQL列舉資料庫 | mysql-databases.nse | [3]8.1 |
| 列舉MySQL變數 | mysql-variables.nse | [3]8.2 |
| 檢查MySQL密碼 | mysql-empty-password.nse | [3]8.3 |
| 審計MySQL密碼 | mysql-brute.nse | [3]8.4 |
| 審計MySQL安全配置 | mysql-audit.nse | [3]8.5 |
| 審計Oracle密碼 | oracle-brute.nse | [3]8.6 |
| 審計msSQL密碼 | ms-sql-brute.nse | [3]8.7 |
| 檢查msSQL空密碼 | ms-sql-empty-password.nse | [3]8.8 |
| 讀取msSQL資料 | ms-sql-tables.nse | [3]8.9 |
| msSQL執行系統命令 | ms-sql-xp-cmdshell.nse | [3]8.10 |
| 審計PgSQL密碼 | pgsql-brute.nse | [3]8.11 |
| 審計HTTP身份驗證 | http-brute.nse | [3]9.1 |
| 審計FTP伺服器 | ftp-brute.nse | [3]9.2 |
| 審計Wordpress程式 | http-wordpress-brute.nse | [3]9.3 |
| 審計Joomla程式 | http-joomla-brute.nse | [3]9.4 |
| 審計郵件伺服器 | pop3-brute.nse | [3]9.5 |
| 審計SMB口令 | smb-brute.nse | [3]9.6 |
| 審計VNC伺服器 | vnc-brute.nse | [3]9.7 |
| 審計SMTP伺服器 | smtp-brute.nse | [3]9.8 |
| 檢測Stuxnet蠕蟲 | stuxnet-detect.nse | [3]9.9 |
| SNMP安全審計 | snmp-info.nse  snmp-brute.nse  snmp-sysdescr.nse  snmp-interfaces.nse  snmp-netstat.nse  snmp-processes.nse  snmp-hh3c-logins.nse  snmp-win32-users.nse  snmp-win32-services.nse | [3]9.10 |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

提升許可權

|  |  |  |
| --- | --- | --- |
| 測試項目 | 技術 | 參考 |
| 利用本地端漏洞 |  | [2] |
| 密碼攻擊 | Hydra  hydra-gtk  patator  ncrack  john  johnny | [4]ch12 |
| 網路欺騙工具 | DNSChef  Arpspoof  Ettercap | [2]ch10 |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

保持控制

|  |  |  |
| --- | --- | --- |
| 測試項目 | 技術 | 參考 |
| 作業系統後門 | 11.1.1 Cymothoa  11.1.2 Intersect  11.1.3 Meterpreter後門 | [2] |
| 隧道工具 | 11.2.1 dns2tcp  11.2.2 iodine  11.2.3 ncat  11.2.4 proxychains  11.2.5 ptunnel  11.2.6 socat  11.2.7 sslh  11.2.8 stunnel4 | [2] |
| 創建Web後門 | 11.3.1 WeBaCoo  11.3.2 weevely  11.3.3 PHP Meterpreter | [2]11.3 |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**網站滲透測試**

[1]Web滲透測試：使用Kali Linux

http://www.waterlike.com.tw/bookdata.asp?NO=TP3C14A030

[2]安全測試指南（第4版）

http://www.books.com.tw/products/CN11362505

[3] XSS跨站腳本攻擊剖析與防御

<http://www.3dwoo.com/showBookDetail.asp?nb=36531>

確定目標與偵察技術

|  |  |  |
| --- | --- | --- |
| 測試項目 | 技術 | 參考 |
| 公司網站 |  | [1] ch2 |
| Web歷史歸檔網站 |  | [1] ch2 |
| 區域互聯網註冊管理機構 |  | [1] ch2 |
| 電子化資料收集、分析及檢索(EDGAR) |  | [1] ch2 |
| 社交媒體資源 |  | [1] ch2 |
| 信任關係 |  | [1] ch2 |
| 招聘廣告 |  | [1] ch2 |
| 實體位置 |  | [1] ch2 |
| Shodan搜尋引擎 |  | [1] ch2 |
| Google Hacking |  | [1] ch2 |
| Google Hacking資料庫 |  | [1] ch2 |
| 研究網路 | HTTrack  Ping,Traceroute  Dig  Fierce  maltego | [1] ch2 |
| 主機掃描 | Nessus  Nmap  Zenmap  FOCA | [1] ch2  [1] ch4 4.4 |
| 審查Web伺服器元件泄露 | curl  wget  rockspider  Burp suite | [2]ch4 4.3 |
| 枚舉Web伺服器的應用 | Nmap  Nessus  Nikto | [2]ch4 4.4 |
| 詮釋和數據挖掘泄露 | Wget  Eyeballs  Curl | [2]ch4 4.5 |
| 識別應用的入口 | Zed Attack Proxy  WebScarab  Burp Suite  CAT | [2]ch4 4.6 |
| 識別Web應用框架 | WhatWeb | [2]ch4 4.8 |
| HTTP方法測試方法 | Wget  Sarn Spade  Spikeproxy  Xenu  curl | [2]ch5 5.6 |
| HTTP強制安全傳輸測試方法 |  |  |

漏洞利用與攻擊

|  |  |  |
| --- | --- | --- |
| 測試項目 | 技術 | 參考 |
| 漏洞評估 | Webshag  Skipfish  ProxyStrike  Vega  Owasp-zap  websploit | [1] ch3 3.1 |
| 漏洞利用 | Metasploit  W3af | [1] ch3 3.2 |
| 利用電子郵件系統漏洞 | Fierce  Netcat | [1] ch3 3.3 |
| 暴力破解攻擊 | Hydra  DirBuster  WebSlayer  Patator | [1] ch3 3.4 |
| 破解密碼 | John the Ripper | [1] ch3 3.5 |
| 中間人攻擊 | SSLStrip | [1] ch3 3.6 |
| 客戶端攻擊 | 社交工程工具集(SET)  MITM代理服務器 | [1] ch4 |
| 獲取和破解用戶密碼 | Crunch  RainbowCrack  Johnny  Hashcat&oclHashcat  Samdump2  Chntpw  Ophcrack  Hash-identifier  Dictstat  Findmyhash  Phrasendrescher  cmosPwd  creddump | [1] ch4 4.6  [1] ch4 4.7 |
| Web會話工具 | Firesheep  Web developer  Greasemonkey  Cookie injector  Coolies manager+  Cookie cadger  Wiershark  Hamster  Dsniff&arpspoof  Ettercap  Driftnet | [1] ch5 5.3 |
| SQL注入(SQL Injection) | Sqlmap  Havij  Domain SQL Injector  Vega  Hexjector  Orascan  Francois Larouche  Northem Monkee | [1] ch5 5.4  [2]ch10 10.5 |
| SQL盲注(SQL Blind Injection) | BBQSQL  SQLMap  BSQLinjector  Bsqlbf  SQLBrute |  |
| 數字型SQL注入(Numeric SQL Injection) | Sqlmap  sqlninja |  |
| 字串型SQL注入(String SQL Injection) | Sqlmap |  |
| SQLMap攻擊類型 | boolean-based blind  time-based blind  error-based  UNION query-based  stacked queries  out-of-band |  |
| HTTP方法竄改測試 |  | [2]ch10 10.3 |
| HTTP參數污染測試 | ModSecurity | [2]ch10 10.4 |
| SQL注入測試 | SQLmap  Orascan  Francois Larouche  Northem Monkee | [2]ch10 10.5 |
| CSS注入測試 |  | [2]ch14 14.5 |
| Reflected XSS | OWASP CAL9000  HackVertor  WebScarab  XSS-Proxy  Ratproxy  Burp Proxy | [2]ch10 10.1 |
| Stored XSS | BeEF  Backframe  XSS Assistant | [2]ch10 10.2 |
| XSS Cookie竊取攻擊 | Live HTTP Headers  Anehta  Burp Suite | [3]2.1 |
| XSS 會話劫持 | Tamper Data  XSS ShellAttackAPI  Anehta | [3]2.2 |
| XSS網絡釣魚 | Anehta | [3]2.3 |
| XSS 客戶端信息刺探 | FiddlerXSS-Proxy  Anehta | [3]2.5 |
| CSRF站外類型 | CSRF Request Builder  CSRFTester |  |
| CSRF站內類型 | CSRF Request Builder  CSRFTester |  |
| LDAP測試方法 | Softerra LDAP Browser | [2]ch10 10.6 |
| XML注入測試 |  | [2]ch10 10.8 |
| XPath 注入測試 | Burp Suite | [2]ch10 10.10 |
| lMAP/SMTP 注入測試 |  | [2]ch10 10.11 |
| 程式碼注入測試 |  | [2]ch10 10.12 |
| 指令注入測試 | OS Command injection | [2]ch10 10.13 |
| 緩衝區注入測試 | ollydbg | [2]ch10 10.14 |
| 客戶端URL重新定向測試 |  | [2]ch14 14.4 |

提升許可權

|  |  |  |
| --- | --- | --- |
| 測試項目 | 技術 | 參考 |
| 提升權限 | Meterpreter  pwdump |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

保持控制

|  |  |  |
| --- | --- | --- |
| 測試項目 | 技術 | 參考 |
| 創建Web後門 | Ingreslock  Cknife |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**無線網路滲透測試**

[1]Kali Linux無線網絡滲透測試詳解

<http://www.waterlike.com.tw/bookdata.asp?NO=TP3C162010>

[2]實戰無線網路入侵偵測

http://m.sanmin.com.tw/product/index/005239961

確定目標與偵察技術

|  |  |  |
| --- | --- | --- |
| 測試項目 | 技術 | 參考 |
| 無線網路探索 | Nmap  Zenmap | [2]3.1 |
| 無線網路掃描 | Airodump-ng  kismet | [1]3.4 |
| 嗅探無線網路 | Wireshark  Ettercap  Dsniff  Jasager | [2]3.4  [2]7.6 |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

漏洞利用與攻擊

|  |  |  |
| --- | --- | --- |
| 測試項目 | 技術 | 參考 |
| 破解WPS | Reaver  Wifite  Fem WiFi Cracker | [1]7.3 |
| 破解WEP | Airmon-ng | [2]4.2 |
| 破解WPA、WPA2 | Airmon-ng | [2]4.2 |
| 偽造MAC | macchanger | [2]4.2 |
| 偽造惡意基地台 | Karmetasploit | [2]7.5 |
|  |  |  |
|  |  |  |

提升許可權

|  |  |  |
| --- | --- | --- |
| 測試項目 | 技術 | 參考 |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

保持控制

|  |  |  |
| --- | --- | --- |
| 測試項目 | 技術 | 參考 |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |