GSEC1 Cheat Sheet

by datgrlnj2 via cheatography.com/56728/cs/38452/

AircrackNG

aircrack-ng : The primary cracking tool	
aireplay-ng : Tool for injecting and replaying wireless frames	
airmon-ng: Tool to enable and disable wireless interface monitoring	
airodump-ng : Tool to capture wireless frames	
airmon-ng	identify wireless cards
airmon-ng start wlan0	start in monitor mode
airodump-ng wlan0mon	look at available wireless networks and clients
aircrack-ng SEC401_WEP.cap	Crack pcap with WEP
aircrack-ng -w all SEC401_WP-A2PSK.pcap	crack WPA2-PSK with dictionary named "all"

hashcat

hashcat --help | grep "Attack Modes" -A9	show different hash modes
shadow file	$1 for MD5, $5 SHA-256, $6 for SHA-512
hashcat --help |grep "MD5 (Unix)"	
hashcat -m 500 -a 0 -o cracked.txt shadow /usr/share/wordlists/sqlmap.txt	-m 500 MD5 unix, -a 0 straight
cracked hashes stored in hashcat.potfile	
echo -e '$$\n$#\n$@\n$!\n' > sec401-rules	create custom rules file appending $, #, @, !
hashcat -m 500 -r sec401-rules -a 0 -o cracked.txt shadow /usr/share/wordlists/sqlmap.txt	dictionary with rules
python bitcoin2john.py btc_wallet.dat > btc_hash.txt	get SHA-256 hash from btc wallet
hashcat --help | grep Bitcoin	-m 11300 bitcoin/litecoin wallet
hashcat -m 11300 -a 0 -o cracked.txt btc_hash.txt /usr/share/wordlists/sqlmap.txt	
cat cracked.txt | grep bitcoin	

snort

sudo tail snort.conf	last 15 lines of file
alert: The action to take when a match is found	
icmp: The protocol to match on	

snort (cont)

$EXTERNAL_NET any ->: A variable representing any external network such as the Internet and any source port	
$HOME_NET any: A variable representing a trusted internal network and any destination port	
(msg: "COMMUNITY ICMP Linux DoS sctp Exploit": The message to include in the alert	
icode:2; itype:3;: The ICMP Type and Code on which to match	
content:"|28 00 00 50 00 00 00 00 F9 57 1F 30 00 00 00 00 00 00 00 00 00 00 00 00|";: The hexadecimal content included in the packet payload on which to perform a match	
reference:nessus,19777;: A reference to a corresponding Nessus plugin	
classtype:attempted-user;: The vulnerability class type	
sid:100000164; rev:2;): The unique Snort signature ID and revision number	
snort -c /etc/snort/snort.conf -i eth0 -A full	-c is config file, -A alerting full
/var/log/snort	alert and snort.log
xxd	dumps contents of file in hex
snort -c /etc/snort/snort.conf -r /home/sec401/labs/401.4/snort/snort.pcap -A full	run against PCAP

Process Hacker

In process, Modules tab shows DLLs can right click send to VT	
Token tab see the SAT (Security access token)	
Memory tab	
https://www.cjwdev.com/Software/NtfsReports/Download.html	

Powershell scripting

Get-Process	list of running processes
Get-Process -Name lsass | Format-List *	
$PaintApp = Get-Process -Name mspaint	add name to variable
$PaintApp.Kill()	Kill paint app
Get-Process | Select-Object Name,Id,Path | Export-Csv -Path ProcList.csv	Save the Name, Id, and Path properties of all running processes to a comma-delimited text file.
ise .\ProcList.csv	

Powershell scripting (cont)	
Get-Process | Select-Object Name,Id,Path | Out-GridView	output in graphical app
cls	clear clutter
Get-Service	display background service
Clear-DnsClientCache	
Get-Service | Select-Object DisplayName,Status | ConvertTo-Html | Out-File -FilePath Services.html	save list of services to HTML file
dir .\Services.html | Format-List *	
dir | Sort-Object CreationTime | Select-Object CreationTime,FullName	sort the listed files by the date and time they were created
Copy-Item -Path .\Services.html -Destination .\Copied.html	dir *.html
Get-FileHash -Algorithm SHA256 -Path *.html	filehash of all HTML files in current directory
Get-Content -Path .\Copied.html	view contents of a file
Get-Content -Path .\Copied.html	
Get-WmiObject -Query "SELECT * FROM Win32_BIOS" -ComputerName LocalHost	Query BIOS information from a remote computer
Get-WinEvent -ListLog * | Select-Object LogName	see names of all local event logs
Get-WinEvent -LogName System -MaxEvents 10 | Select-Object TimeCreated,Id,Message	get last 10 events from System log, time, ID and message
Get-WinEvent -LogName System -MaxEvents 10 -ComputerName LocalHost | Select-Object TimeCreated,Id,Message | Export-Csv -Path LogData.csv	export to csv file
Get-Help -Full Get-WinEvent	

TCPdump	
FTP and capture first 3 packets	tcpdump -i eth0 port 21 -c 3
-X display hex and ASCII first 4 packets	tcpdump -X -i eth0 port 21 -c 4
-a print ASCII, FTP, specify source	tcpdump -a -i eth0 port 21 and src 10.10.10.20
listen on loopback on port 333	tcpdump -i lo tcp port 333

Applocker	
AppIDSvc (Application Identity)	applocker service
secpol.msc	local security policy-> Application Control Policies -> AppLocker
Publisher	For digitally signed apps. More secure than the Path condition and relatively easy to maintain
Path	The Path condition is conceptually simplistic. With this method you set up allowlists and blocklists based on an application's location on the file system
File Hash	It is seen as a more secure option than using the Path and when the file is not or cannot be digitally signed.
Applocker	create and define rules that apply to security groups and even a single user. Rules can be applied to Windows binaries, DLLs, installers, and various script files, such as .ps1, .cmd, and .js.

Malware analysis

strings -n 14 trojan1 | more	string 14 characters or longer
python -c 'print("A" *100)' > bof	python -c 'print("A" * 1000)' > bof

hping

hping3 --help | more	
-c: The count option enables you to specify the number of packets to send.	
-i: The interval option enables you to specify the time between sending each packet.	
hping3 --help | grep Mode -A7	
hping3 --help | grep "\-\-spoof" -A7 -B1	hping3 --help | grep "\-\-base" -A15 -B1
-a: This option enables you to spoof the source IP address, which you will do soon.	
-t: This option enables you to set the TTL to any wanted value.	
-N: This option enables you to set the IP ID to any wanted value.	
-f: This option enables you to force fragmentation of a packet.	
-s: Set the source port number, which is usually a random ephemeral port.	
-p: Set the destination port number.	
-w: Set the window size.	
-b: Try sending a packet with a bad checksum.	
hping3 -S 10.10.10.10 -p 21 -c 1	SYN packet to TCP port 21 -c 1 packet
hping3 -S 10.10.10.10 -a 10.11.1-2.13 -p 21 -c 1	spoof IP address

secedit

secedit.exe /analyze	review cmd line switches
secedit.exe /analyze /db temp.sdb /cfg SecurityTemplate.inf /log log.txt	compare log settings from template to local computer
look for mismatch in the output	
secedit.exe /configure	review cmd line switches
secedit.exe /configure /db temp.sdb /cfg SecurityTemplate.inf	reconfigure the computer by applying security template
Get-Content .\out.txt | Select-String -Pattern "Mismatch"	
Get-Help -Full Get-Content	Get-Help -Full Select-String

secedit (cont)

Start-Process PowerShell.exe

GPG

gpa &	open GNU privacy assistant
eom sans-logo.png	eom is image viewer

TCPdump

-i Specify from which network interface you would like tcpdump to sniff.
-s Number of bytes "snaplen" to capture per packet. Default is 262,144 bytes.
-c Number of packets to capture before stopping.
-n Don't resolve hostnames or well-known port numbers to their service.
-X Show packet contents in hexadecimal and ASCII.
-XX Show packet contents in hexadecimal and ASCII, as well as the Ethernet header.
-e Display Ethernet header data.

nmap

nmap --help | more	
nmap --help | grep "HOST DISCOVERY" -A10	10 lines after host discovery
nmap --help | grep "SCAN TECHNIQUES" -A8	8 lines after scan techniques
-sS performs a SYN or Stealth scan to each port designated and does not send the final ACK in the 3-way handshake. This is to try to avoid having the connection attempt logged because some older systems do not log the attempt until the 3-way handshake completes.	The --reason option is useful because it specifies how it determined the state of the port. The --packet--trace option shows all packets sent and received.
-sT attempts a TCP connect scan to each port designated and completes the 3-way handshake to see if the port is open	-oA prints the output to the file you specify in normal, XML, and grepable formats.

nmap (cont)	
-sA performs an ACK scan to each port designated. This means that it does not first send a SYN packet as expected and sends a packet only with the ACK flag set. The idea is to try and pass through some filters, wrongly making the assumption that if the ACK flag is set, that it must be from an active TCP session that is permitted. If a system receives an unsolicited packet with the ACK flag set, it will respond back with the RST flag. This does not indicate that a particular port is open, but does indicate that the IP address is active on the network, similar to a ping command.	-oG prints the output to the file you specify in grepable format.
-sW also performs an ACK scan but also interrogates the TCP window size because some systems set the window size to 0 if the port is closed.	-oS prints the output to the file you specify in "script kiddie" format, which is mostly for fun.
-sM performs a Maimon scan and is named after the author Uriel Maimon. This scan technique modifies the TCP flags that proved useful in identifying some BSD-derived operating systems.	-oX prints the output to the file you specify in XML format.

nmap (cont)	
-sU option tells Nmap to scan UDP ports instead of TCP ports. Other scans, such as "Null", "FIN", and "Xmas", each use different combinations of the TCP flags to try and elicit a response. We will not cover every one of the commands because there are far too many, and they are all well documented in the Nmap documentation.	-oN prints the output to the file you specify, exactly how it is displayed on the screen.
nmap --help | grep "PORT SPECIFICATION" -A7	nmap --help | grep "OUT-PUT" -A8
nmap --help | grep "TIMING AND PERF" -A12	--max-rate : This option tells Nmap to send packets no faster than the number specified per second.
-T: This option enables you to choose a value between 0 and 5, each performing the scan at different speeds---the lower the number, the slower the scan is performed.	--min-rate : This option tells Nmap to send packets no slower than the number specified per second.
--max-retries: This option tells Nmap how many times to retransmit probe attempts to a system.	--host-ti-meout: This option tells Nmap how quickly to give up on a host.
nmap -sT --reason 10.10.10.10 -oN scan1.txt	
nmap -sU 10.10.10.10 -p69,161 -oN scan2.txt	UDP scan
nmap -n --packet-trace -sS 10.10.10.10 -p80	
nmap -n -sT -O 10.10.10.10 -p21,80	OS version scanning
nmap -n -sT -A 10.10.10.10 -p21,80	
ls /usr/share/nmap/scripts/p*	scripting engine path
nmap -sU -p161 --script snmp-brute 10.10.10.10 --script-args snmp-brute.communitiesdb=community.lst	
snmpcheck -t 10.10.10.10 -c publ1c | grep "User accounts" -A12	