Penetration Testing Process

Section	Question Number	Answer
Pre-Engagement	Question 1	7
Vulnerability Assessment	Question 1	Predictive
Post-Exploitation	Question 1	3
Post-Exploitation	Question 2	PCI-DSS
Post-Engagement	Question 1	DRAFT

Network Enumeration and NMAP

Section	Question Number	Answer
Host Discovery	Question 1	Windows
Host and Port Scanning	Question 1	7
Host and Port Scanning	Question 2	NIX-NMAP-DEFAULT
Saving the Results	Question 1	31337
Service Enumeration	Question 1	HTB{pr0F7pDv3r510nb4nn3r}
Nmap Scripting Engine	Question 1	HTB{873nniuc71bu6usbs1i96as6dsv26}
Firewall and IDS/IPS Evasion - Easy Lab	Question 1	Ubuntu
Firewall and IDS/IPS Evasion - Medium Lab	Question 1	HTB{GoTtgUnyze9Psw4vGjcuMpHRp}
Firewall and IDS/IPS Evasion - Hard Lab	Question 1	HTB{kjnsdf2n982n1827eh76238s98di1w6}

Getting Started

Section	Question Number	Answer
Service Scanning	Question 1	Apache Tomcat
Service Scanning	Question 2	2323
Service Scanning	Question 3	dceece590f3284c3866305eb2473d099
Web Enumeration	Question 1	HTB{w3b_3num3r4710n_r3v34l5_53cr375}
Public Exploits	Question 1	HTB{my_f1r57_h4ck}

Section	Question Number	Answer
Privilege Escalation	Question 1	HTB{l473r4l_m0v3m3n7_70_4n07h3r_u53r}
Privilege Escalation	Question 2	HTB{pr1v1l363_35c4l4710n_2_r007}
Nibbles - Enumeration	Question 1	2.4.18
Nibbles - Initial Foothold	Question 1	79c03865431abf47b90ef24b9695e148
Nibbles - Privilege Escalation	Question 1	de5e5d6619862a8aa5b9b212314e0cdd
Knowledge Check	Question 1	7002d65b149b0a4d19132a66feed21d8
Knowledge Check	Question 2	f1fba6e9f71efb2630e6e34da6387842

Footprinting

Section	Question Number	Answer
FTP	Question 1	InFreight FTP v1.1
FTP	Question 2	HTB{b7skjr4c76zhsds7fzhd4k3ujg7nhdjre}
SMB	Question 1	Samba smbd 4.6.2
SMB	Question 2	sambashare
SMB	Question 3	HTB{o873nz4xdo873n4zo873zn4fksuhldsf}
SMB	Question 4	DEVOPS
SMB	Question 5	InFreight SMB v3.1
SMB	Question 6	/home/sambauser
NFS	Question 1	HTB{hjglmvtkjhlkfuhgi734zthrie7rjmdze}
NFS	Question 2	HTB{8o7435zhtuih7fztdrzuhdhkfjcn7ghi4357ndcthzuc7rtfghu34}
DNS	Question 1	ns.inlanefreight.htb
DNS	Question 2	HTB{DN5_z0N3_7r4N5F3r_iskdufhcnlu34}
DNS	Question 3	10.129.34.16
DNS	Question 4	win2k.dev.inlanefreight.htb
SMTP	Question 1	InFreight ESMTP v2.11
SMTP	Question 2	robin
IMAP / POP3	Question 1	InlaneFreight Ltd
IMAP / POP3	Question 2	dev.inlanefreight.htb
IMAP / POP3	Question 3	HTB{roncfbw7iszerd7shni7jr2343zhrj}
IMAP / POP3	Question 4	InFreight POP3 v9.188

Section	Question Number	Answer
IMAP / POP3	Question 5	devadmin@inlanefreight.htb
IMAP / POP3	Question 6	HTB{983uzn8jmfgpd8jmof8c34n7zio}
SNMP	Question 1	devadmin@inlanefreight.htb
SNMP	Question 2	Infreight SNMP v0.91
SNMP	Question 3	HTB{5nMp_fl4g_uidhfljnsldiuhbfsdij44738b2u763g}
MySQL	Question 1	MySQL 8.0.27
MySQL	Question 2	ultrices@google.htb
MSSQL	Question 1	ILF-SQL-01
MSSQL	Question 2	Employees
Oracle TNS	Question 1	E066D214D5421CCC
IPMI	Question 1	admin
IPMI	Question 2	trinity
Footprinting Lab - Easy	Question 1	HTB{7nrzise7hednrxihskjed7nzrgkweunj47zngrhdbkjhgdfbjkc7hgj}
Footprinting Lab - Medium	Question 1	lnch7ehrdn43i7AoqVPK4zWR
Footprinting Lab - Hard	Question 1	cr3n4o7rzse7rzhnckhssncif7ds

Information Gathering Web Edition

Section	Question Number	Answer
Utilizing WHOIS	Question 1	292
Utilizing WHOIS	Question 2	admin@dnstinations.com
Digging DNS	Question 1	134.209.24.248
Digging DNS	Question 2	inlanefreight.com
Digging DNS	Question 3	smtpin.vvv.facebook.com.
Subdomain Bruteforcing	Question 1	my.inlanefreight.com
DNS Zone Transfers	Question 1	22
DNS Zone Transfers	Question 2	10.10.34.2
DNS Zone Transfers	Question 3	10.10.200.14
Virtual Hosts	Question 1	web17611.inlanefreight.htb

Section	Question Number	Answer
Virtual Hosts	Question 2	vm5.inlanefreight.htb
Virtual Hosts	Question 3	browse.inlanefreight.htb
Virtual Hosts	Question 4	admin.inlanefreight.htb
Virtual Hosts	Question 5	support.inlanefreight.htb
Fingerprinting	Question 1	2.4.41
Fingerprinting	Question 2	Joomla
Fingerprinting	Question 3	Ubuntu
Creepy Crawlies	Question 1	inlanefreight-comp133.s3.amazonaws.htb
Web Archives	Question 1	74
Web Archives	Question 2	3054
Web Archives	Question 3	http://site.aboutface.com/
Web Archives	Question 4	Palm 0rganizer
Web Archives	Question 5	http://google.stanford.edu/
Web Archives	Question 6	17-December-99
Web Archives	Question 7	3000
Skills Assessment	Question 1	468
Skills Assessment	Question 2	nginx
Skills Assessment	Question 3	e963d863ee0e82ba7080fbf558ca0d3f
Skills Assessment	Question 4	1337testing@inlanefreight.htb
Skills Assessment	Question 5	ba988b835be4aa97d068941dc852ff33

Vulnerability Assessment

Section	Question Number	Answer
Nessus Skills Assessment	Question 1	wsus
Nessus Skills Assessment	Question 2	172.16.16.100
Nessus Skills Assessment	Question 3	156032

Section	Question Number	Answer
Nessus Skills Assessment	Question 4	VNC Server Unauthenticated Access
Nessus Skills Assessment	Question 5	5900
OpenVAS Skills Assessment	Question 1	Ubuntu
OpenVAS Skills Assessment	Question 2	Anonymous FTP Login Reporting
OpenVAS Skills Assessment	Question 3	172.16.16.160
OpenVAS Skills Assessment	Question 4	Cleartext Transmission of Sensitive Information via HTTP

File Transfer

Section	Question Number	Answer
Windows File Transfer Methods	Question 1	b1a4ca918282fcd96004565521944a3b
Windows File Transfer Methods	Question 2	f458303ea783c224c6b4e7ef7f17eb9d
Linux File Transfer Methods	Question 1	5d21cf3da9c0ccb94f709e2559f3ea50
Linux File Transfer Methods	Question 2	159cfe5c65054bbadb2761cfa359c8b0

Shells & Payloads

Section	Question Number	Answer
Anatomy of a Shell	Question 1	bash&powershell
Anatomy of a Shell	Question 2	Core
Bind Shells	Question 1	443
Bind Shells	Question 2	B1nD_Shells_r_cool
Reverse Shells	Question 1	client
Reverse Shells	Question 2	SHELLS-WIN10
Automating Payloads & Delivery with Metasploit	Question 1	powershell

Section	Question Number	Answer
Automating Payloads & Delivery with Metasploit	Question 2	staffsalaries.txt
Infiltrating Windows	Question 1	.bat
Infiltrating Windows	Question 2	MS17-010
Infiltrating Windows	Question 3	EB-Still-W0rk$
Infiltrating Unix/Linux	Question 1	php
Infiltrating Unix/Linux	Question 2	edgerouter-isp
Laudanum, One Webshell to Rule Them All	Question 1	c:\windows\system32\inetsrv
Laudanum, One Webshell to Rule Them All	Question 2	/usr/share/laudanum/aspx/shell.aspx
Antak Webshell	Question 1	/usr/share/nishang/Antak-WebShell/antak.aspx
Antak Webshell	Question 2	iis apppool\status
PHP Web Shells	Question 1	image/gif
PHP Web Shells	Question 2	ajax-loader.gif
The Live Engagement	Question 1	shells-winsvr
The Live Engagement	Question 2	dev-share
The Live Engagement	Question 3	ubuntu
The Live Engagement	Question 4	php
The Live Engagement	Question 5	B1nD_Shells_r_cool
The Live Engagement	Question 6	shells-winblue
The Live Engagement	Question 7	One-H0st-Down!

Using the Metasploit Framework

Section	Question Number	Answer
Introduction to Metasploit	Question 1	Metasploit Pro
Introduction to Metasploit	Question 2	msfconsole
Modules	Question 1	HTB{MSF-W1nD0w5-3xPL01t4t10n}
Payloads	Question 1	HTB{MSF_Expl01t4t10n}
Sessions & Jobs	Question 1	elFinder

Section	Question Number	Answer
Sessions & Jobs	Question 2	www-data
Sessions & Jobs	Question 3	HTB{5e55ion5_4r3_sw33t}
Meterpreter	Question 1	nt authority\system
Meterpreter	Question 2	cf3a5525ee9414229e66279623ed5c58

Password Attacks

Section	Question Number	Answer
Network Services	Question 1	HTB{That5Novemb3r}
Network Services	Question 2	HTB{Let5R0ck1t}
Network Services	Question 3	HTB{R3m0t3DeskIsw4yT00easy}
Network Services	Question 4	HTB{S4ndM4ndB33}
Password Mutations	Question 1	HTB{P455_Mu7ations}
Password Reuse / Default Passwords	Question 1	superdba:admin
Attacking SAM	Question 1	hklm\sam
Attacking SAM	Question 2	matrix
Attacking SAM	Question 3	frontdesk:Password123
Attacking LSASS	Question 1	lsass.exe
Attacking LSASS	Question 2	Mic@123
Attacking Active Directory & NTDS.dit	Question 1	ntds.dit
Attacking Active Directory & NTDS.dit	Question 2	64f12cddaa88057e06a81b54e73b949b
Attacking Active Directory & NTDS.dit	Question 3	jmarston:P@ssword!
Attacking Active Directory & NTDS.dit	Question 4	Winter2008
Credential Hunting in Windows	Question 1	WellConnected123
Credential Hunting in Windows	Question 2	3z1ePfGbjWPsTfCsZfjy

Section	Question Number	Answer
Credential Hunting in Windows	Question 3	ubuntu:FSadmin123
Credential Hunting in Windows	Question 4	Inlanefreightisgreat2022
Credential Hunting in Windows	Question 5	edgeadmin:Edge@dmin123!
Credential Hunting in Linux	Question 1	TUqr7QfLTLhruhVbCP
Passwd, Shadow & Opasswd	Question 1	J0rd@n5
Pass the Hash (PtH)	Question 1	G3t_4CCE$$_V1@_PTH
Pass the Hash (PtH)	Question 2	DisableRestrictedAdmin
Pass the Hash (PtH)	Question 3	c39f2beb3d2ec06a62cb887fb391dee0
Pass the Hash (PtH)	Question 4	D3V1d_Fl5g_is_Her3
Pass the Hash (PtH)	Question 5	JuL1()_SH@re_fl@g
Pass the Hash (PtH)	Question 6	JuL1()_N3w_fl@g
Pass the Ticket (PtT) from Windows	Question 1	3
Pass the Ticket (PtT) from Windows	Question 2	Learn1ng_M0r3_Tr1cks_with_J0hn
Pass the Ticket (PtT) from Windows	Question 3	P4$$_th3_Tick3T_PSR
Pass the Ticket (PtT) from Linux	Question 1	Gett1ng_Acc3$$_to_LINUX01
Pass the Ticket (PtT) from Linux	Question 2	Linux Admins
Pass the Ticket (PtT) from Linux	Question 3	carlos.keytab
Pass the Ticket (PtT) from Linux	Question 4	C@rl0s_1$_H3r3
Pass the Ticket (PtT) from Linux	Question 5	Mor3_4cce$$_m0r3_Pr1v$
Pass the Ticket (PtT) from Linux	Question 6	Ro0t_Pwn_K3yT4b
Pass the Ticket (PtT) from Linux	Question 7	JuL1()_SH@re_fl@g

Section	Question Number	Answer
Pass the Ticket (PtT) from Linux	Question 8	Us1nG_KeyTab_Like_@_PRO
Protected Files	Question 1	L0veme
Protected Archives	Question 1	HTB{ocnc7r4io8ucsj8eujcm}
Password Attacks Lab - Easy	Question 1	dgb6fzm0ynk@AME9pqu
Password Attacks Lab - Medium	Question 1	HTB{PeopleReuse_PWsEverywhere!}
Password Attacks Lab - Hard	Question 1	HTB{PWcr4ck1ngokokok}

Attacking Common Services

Section	Question Number	Answer
Attacking FTP	Question 1	2121
Attacking FTP	Question 2	robin
Attacking FTP	Question 3	HTB{ATT4CK1NG_F7P_53RV1C3}
Attacking SMB	Question 1	GGJ
Attacking SMB	Question 2	34c8zuNBo91!@28Bszh
Attacking SMB	Question 3	HTB{SMB_4TT4CKS_2349872359}
Attacking SQL Databases	Question 1	princess1
Attacking SQL Databases	Question 2	HTB{!*l0v3*#4$#!n9_4nd_r3$p0nd3r}
Attacking RDP	Question 1	pentest-notes.txt
Attacking RDP	Question 2	DisableRestrictedAdmin
Attacking RDP	Question 3	HTB{RDP_P4$$_Th3_H4$#}
Attacking DNS	Question 1	HTB{LUIHNFAS2871SJK1259991}
Attacking Email Services	Question 1	marlin
Attacking Email Services	Question 2	HTB{w34k_p4$$w0rd}
Attacking Common Services - Easy	Question 1	HTB{t#3r3_4r3_tw0_w4y$_t0_93t_t#3_fl49}
Attacking Common Services - Medium	Question 1	HTB{1qay2wsx3EDC4rfv_M3D1UM}
Attacking Common Services - Hard	Question 1	random.txt

Section	Question Number	Answer
Attacking Common Services - Hard	Question 2	48Ns72!bns74@S84NNNSl
Attacking Common Services - Hard	Question 3	john
Attacking Common Services - Hard	Question 4	HTB{46u$!n9_l!nk3d_$3rv3r$}

Pivoting, Tunneling, and Port Forwarding

Section	Question Number	Answer
The Networking Behind Pivoting	Question 1	eth0
The Networking Behind Pivoting	Question 2	tun0
The Networking Behind Pivoting	Question 3	178.62.64.1
Dynamic Port Forwarding with SSH and SOCKS Tunneling	Question 1	3
Dynamic Port Forwarding with SSH and SOCKS Tunneling	Question 2	N1c3Piv0t
Remote/Reverse Port Forwarding with SSH	Question 1	172.16.5.129
Remote/Reverse Port Forwarding with SSH	Question 2	0.0.0.0
Meterpreter Tunneling & Port Forwarding	Question 1	172.16.5.19,172.16.5.129
Meterpreter Tunneling & Port Forwarding	Question 2	172.16.5.0/255.255.254.0
Socat Redirection with a Reverse Shell	Question 1	False
Socat Redirection with a Bind Shell	Question 1	windows/x64/meterpreter/bind_tcp
Web Server Pivoting with Rpivot	Question 1	Attack Host
Web Server Pivoting with Rpivot	Question 2	Pivot Host
Web Server Pivoting with Rpivot	Question 3	I_L0v3_Pr0xy_Ch@ins
Port Forwarding with Windows: Netsh	Question 1	Jim Flipflop
DNS Tunneling with Dnscat2	Question 1	AC@tinth3Tunnel

Section	Question Number	Answer
SOCKS5 Tunneling with Chisel	Question 1	Th3$eTunne1$@rent8oring!
ICMP Tunneling with SOCKS	Question 1	N3Tw0rkTunnelV1sion!
RDP and SOCKS Tunneling with SocksOverRDP	Question 1	H0pping@roundwithRDP!
Skills Assessment	Question 1	webadmin
Skills Assessment	Question 2	mlefay:Plain Human work!
Skills Assessment	Question 3	172.16.5.35
Skills Assessment	Question 4	S1ngl3-Piv07-3@sy-Day
Skills Assessment	Question 5	vfrank
Skills Assessment	Question 6	N3tw0rk-H0pp1ng-f0R-FuN
Skills Assessment	Question 7	3nd-0xf-Th3-R@inbow!

Using Web Proxies

Section	Question Number	Answer
Intercepting Web Requests	Question 1	HTB{1n73rc3p73d_1n_7h3_m1ddl3}
Repeating Requests	Question 1	HTB{qu1ckly_r3p3471n6_r3qu3575}
Encoding/Decoding	Question 1	HTB{3nc0d1n6_n1nj4}
Proxying Tools	Question 1	msf test file
Burp Intruder	Question 1	HTB{burp_1n7rud3r_fuzz3r!}
ZAP Fuzzer	Question 1	HTB{fuzz1n6_my_f1r57_c00k13}
ZAP Scanner	Question 1	HTB{5c4nn3r5_f1nd_vuln5_w3_m155}
Skills Assessment - Using Web Proxies	Question 1	HTB{d154bl3d_bu770n5_w0n7_570p_m3}
Skills Assessment - Using Web Proxies	Question 2	3dac93b8cd250aa8c1a36fffc79a17a
Skills Assessment - Using Web Proxies	Question 3	HTB{burp_1n7rud3r_n1nj4!}
Skills Assessment - Using Web Proxies	Question 4	CFIDE

Attacking Web Applications with Ffuf

Section	Question Number	Answer
Directory Fuzzing	Question 1	forum
Page Fuzzing	Question 1	HTB{bru73_f0r_c0mm0n_p455w0rd5}
Recursive Fuzzing	Question 1	HTB{fuzz1n6_7h3_w3b!}
Sub-domain Fuzzing	Question 1	customer.inlanefreight.com
Filtering Results	Question 1	test.academy.htb
Parameter Fuzzing - GET	Question 1	user
Value Fuzzing	Question 1	HTB{p4r4m373r_fuzz1n6_15_k3y!}
Skills Assessment - Web Fuzzing	Question 1	archive, test, faculty
Skills Assessment - Web Fuzzing	Question 2	.php, .php7, .phps
Skills Assessment - Web Fuzzing	Question 3	http://faculty.academy.htb:PORT/courses/linux-security.php7
Skills Assessment - Web Fuzzing	Question 4	user username
Skills Assessment - Web Fuzzing	Question 5	HTB{w3b_fuzz1n6_m4573r}

Login Brute Forcing

Section	Question Number	Answer
Brute Force Attacks	Question 1	HTB{Brut3_F0rc3_1s_P0w3rfu1}
Dictionary Attacks	Question 1	HTB{Brut3_F0rc3_M4st3r}
Basic HTTP Authentication	Question 1	HTB{th1s_1s_4_f4k3_fl4g}
Login Forms	Question 1	HTB{W3b_L0gin_Brut3F0rc3}
Web Services	Question 1	qqww1122
Web Services	Question 2	HTB{SSH_and_FTP_Bruteforce_Success}
Custom Wordlists	Question 1	HTB{W3b_L0gin_Brut3F0rc3_Cu5t0m}
Skills Assessment Part 1	Question 1	Admin123
Skills Assessment Part 1	Question 2	satwossh

Section	Question Number	Answer
Skills Assessment Part 2	Question 1	thomas
Skills Assessment Part 2	Question 2	HTB{brut3f0rc1ng_succ3ssful}

SQL Injection Fundamentals

Section	Question Number	Answer
Intro to MySQL	Question 1	employees
SQL Statements	Question 1	d005
Query Results	Question 1	Mitchem
SQL Operators	Question 1	654
Subverting Query Logic	Question 1	202a1d1a8b195d5e9a57e434cc16000c
Using Comments	Question 1	cdad9ecdf6f14b45ff5c4de32909caec
Union Clause	Question 1	663
Union Injection	Question 1	root@localhost
Database Enumeration	Question 1	9da2c9bcdf39d8610954e0e11ea8f45f
Reading Files	Question 1	dB_pAssw0rd_iS_flag!
Writing Files	Question 1	d2b5b27ae688b6a0f1d21b7d3a0798cd
Skills Assessment - SQL Injection Fundamentals	Question 1	528d6d9cedc2c7aab146ef226e918396

SQLMap Essentials

Section	Question Number	Answer
SQLMap Overview	Question 1	UNION query-based
Running SQLMap on an HTTP Request	Question 1	HTB{700_much_c0n6r475_0n_p057_r3qu357}
Running SQLMap on an HTTP Request	Question 2	HTB{c00k13_m0n573r_15_7h1nk1n6_0f_6r475}
Running SQLMap on an HTTP Request	Question 3	HTB{j450n_v00rh335_53nd5_6r475}
Attack Tuning	Question 1	HTB{700_much_r15k_bu7_w0r7h_17}

Section	Question Number	Answer
Attack Tuning	Question 2	HTB{v1nc3_mcm4h0n_15_4570n15h3d}
Attack Tuning	Question 3	HTB{un173_7h3_un173d}
Database Enumeration	Question 1	HTB{c0n6r475_y0u_kn0w_h0w_70_run_b451c_5qlm4p_5c4n}
Advanced Database Enumeration	Question 1	PARAMETER_STYLE
Advanced Database Enumeration	Question 2	Enizoom1609
Bypassing Web Application Protections	Question 1	HTB{y0u_h4v3_b33n_c5rf_70k3n1z3d}
Bypassing Web Application Protections	Question 2	HTB{700_much_r4nd0mn355_f0r_my_74573}
Bypassing Web Application Protections	Question 3	HTB{y37_4n07h3r_r4nd0m1z3}
Bypassing Web Application Protections	Question 4	HTB{5p3c14l_ch4r5_n0_m0r3}
OS Exploitation	Question 1	HTB{5up3r_u53r5_4r3_p0w3rful!}
OS Exploitation	Question 2	HTB{n3v3r_run_db_45_db4}
Skills Assessment	Question 1	HTB{n07_50_h4rd_r16h7?!}

Cross-Site Scripting (XSS)

Section	Question Number	Answer
Stored XSS	Question 1	HTB{570r3d_f0r_3v3ry0n3_70_533}
Reflected XSS	Question 1	HTB{r3fl3c73d_b4ck_2_m3}
DOM XSS	Question 1	HTB{pur3ly_cl13n7_51d3}
XSS Discovery	Question 1	email
XSS Discovery	Question 2	reflected
Phishing	Question 1	HTB{r3f13c73d_cr3d5_84ck_2_m3}
Session Hijacking	Question 1	HTB{4lw4y5_53cur3_y0ur_c00k135}
Skills Assessment	Question 1	HTB{cr055_5173_5cr1p71n6_n1nj4}

File Inclusion

Section	Question Number	Answer
Local File Inclusion (LFI)	Question 1	barry
Local File Inclusion (LFI)	Question 2	HTB{n3v3r_trut_u3r_!nput}
Basic Bypasses	Question 1	HTB{64$!c_f!lt3r$*w0nt*$t0p_lf!}
PHP Filters	Question 1	HTB{n3v3r_$t0r3_pl4!nt3xt_cr3d$}
PHP Wrappers	Question 1	HTB{d!$46l3_r3m0t3_url_!nclud3}
Remote File Inclusion (RFI)	Question 1	99a8fc05f033f2fc0cf9a6f9826f83f4
LFI and File Uploads	Question 1	HTB{upl04d+lf!+3x3cut3=rc3}
Log Poisoning	Question 1	/var/www/html
Log Poisoning	Question 2	HTB{1095_5#0u1d_n3v3r_63_3xp053d}
Automated Scanning	Question 1	HTB{4u70m47!0n_f!nd5_#!dd3n_93m5}
File Inclusion Prevention	Question 1	/etc/php/7.4/apache2/php.ini
File Inclusion Prevention	Question 2	security
Skills Assessment - File Inclusion	Question 1	a9a892dbc9faf9a014f58e007721835e

File Upload Attacks

Section	Question Number	Answer
Absent Validation	Question 1	fileuploadsabsentverification
Upload Exploitation	Question 1	HTB{g07_my_f1r57_w3b_5h3ll}
Client-Side Validation	Question 1	HTB{cl13n7_51d3_v4l1d4710n_w0n7_570p_m3}
Blacklist Filters	Question 1	HTB{1_c4n_n3v3r_b3_bl4ckl1573d}
Whitelist Filters	Question 1	HTB{1_wh173l157_my53lf}
Type Filters	Question 1	HTB{m461c4l_c0n73n7_3xpl0174710n}
Limited File Uploads	Question 1	HTB{my_1m4635_4r3_l37h4l}
Limited File Uploads	Question 2	./images/
Skills Assessment - File Upload Attacks	Question 1	HTB{m4573r1ng_upl04d_3xpl0174710n}

Command Injections

Section	Question Number	Answer
Detection	Question 1	Please match the requested format.
Injecting Commands	Question 1	17
Other Injection Operators	Question 1	
Identifying Filters	Question 1	new-line
Bypassing Space Filters	Question 1	1613
Bypassing Other Blacklisted Characters	Question 1	1nj3c70r
Bypassing Blacklisted Commands	Question 1	HTB{b451c_f1l73r5_w0n7_570p_m3}
Advanced Command Obfuscation	Question 1	/usr/share/mysql/debian_create_root_user.sql
Skills Assessment	Question 1	HTB{c0mm4nd3r_1nj3c70r}

Web Attacks

Section	Question Number	Answer
Bypassing Basic Authentication	Question 1	HTB{4lw4y5_c0v3r_4ll_v3rb5}
Bypassing Security Filters	Question 1	HTB{b3_v3rb_c0n51573n7}
Mass IDOR Enumeration	Question 1	HTB{4ll_f1l35_4r3_m1n3}
Bypassing Encoded References	Question 1	HTB{h45h1n6_1d5_w0n7_570p_m3}
IDOR in Insecure APIs	Question 1	eb4fe264c10eb7a528b047aa983a4829
Chaining IDOR Vulnerabilities	Question 1	HTB{1_4m_4n_1d0r_m4573r}
Local File Disclosure	Question 1	UTM1NjM0MmRzJ2dmcTIzND0wMXJnZXdmc2RmCg
Advanced File Disclosure	Question 1	HTB{3rr0r5_c4n_l34k_d474}
Blind Data Exfiltration	Question 1	HTB{1_d0n7_n33d_0u7pu7_70_3xf1l7r473_d474}

Section	Question Number	Answer
Web Attacks - Skills Assessment	Question 1	HTB{m4573r_w3b_4774ck3r}

Attacking Common Applications

Section	Question Number	Answer
Application Discovery & Enumeration	Question 1	ew.db
Application Discovery & Enumeration	Question 2	Pages by Similarity
WordPress - Discovery & Enumeration	Question 1	0ptions_ind3xeS_ftw!
WordPress - Discovery & Enumeration	Question 2	WP Sitemap Page
WordPress - Discovery & Enumeration	Question 3	1.6.4
Attacking WordPress	Question 1	doug
Attacking WordPress	Question 2	jessica1
Attacking WordPress	Question 3	webadmin
Attacking WordPress	Question 4	l00k_ma_unAuth_rc3!
Joomla - Discovery & Enumeration	Question 1	3.10.0
Joomla - Discovery & Enumeration	Question 2	turnkey
Attacking Joomla	Question 1	j00mla_c0re_d1rtrav3rsal!
Drupal - Discovery & Enumeration	Question 1	7.30
Attacking Drupal	Question 1	DrUp@l_drUp@l_3veryWh3Re!
Tomcat - Discovery & Enumeration	Question 1	10.0.10
Tomcat - Discovery & Enumeration	Question 2	admin-gui
Attacking Tomcat	Question 1	tomcat
Attacking Tomcat	Question 2	root

Section	Question Number	Answer
Attacking Tomcat	Question 3	t0mcat_rc3_ftw!
Jenkins - Discovery & Enumeration	Question 1	2.303.1
Attacking Jenkins	Question 1	f33ling_gr00000vy!
Splunk - Discovery & Enumeration	Question 1	8.2.2
Attacking Splunk	Question 1	l00k_ma_no_AutH!
PRTG Network Monitor	Question 1	18.1.37.13946
PRTG Network Monitor	Question 2	WhOs3_m0nit0ring_wH0?
osTicket	Question 1	Inlane_welcome!
Gitlab - Discovery & Enumeration	Question 1	13.10.2
Gitlab - Discovery & Enumeration	Question 2	postgres
Attacking GitLab	Question 1	DEMO
Attacking GitLab	Question 2	s3cure_y0ur_Rep0s!
Attacking Tomcat CGI	Question 1	feldspar\omen
Attacking CGI Applications - Shellshock	Question 1	Sh3ll_Sh0cK_123
Attacking Thick Client Applications	Question 1	username:password
Exploiting Web Vulnerabilities in Thick-Client Applications	Question 1	107.252.188.60
ColdFusion - Discovery & Enumeration	Question 1	Server Monitor
Attacking ColdFusion	Question 1	arctic\tolis
IIS Tilde Enumeration	Question 1	transfer.aspx
Attacking LDAP	Question 1	w3.css
Web Mass Assignment Vulnerabilities	Question 1	active
Attacking Applications Connecting to Services	Question 1	uname:pass
Other Notable Applications	Question 1	Weblogic

Section	Question Number	Answer
Other Notable Applications	Question 2	w3b_l0gic_RCE!
Attacking Common Applications - Skills Assessment I	Question 1	tomcat
Attacking Common Applications - Skills Assessment I	Question 2	8080
Attacking Common Applications - Skills Assessment I	Question 3	9.0.0.M1
Attacking Common Applications - Skills Assessment I	Question 4	f55763d31a8f63ec935abd07aee5d3d0
Attacking Common Applications - Skills Assessment II	Question 1	http://blog.inlanefreight.local
Attacking Common Applications - Skills Assessment II	Question 2	VirtualHost
Attacking Common Applications - Skills Assessment II	Question 3	monitoring.inlanefreight.local
Attacking Common Applications - Skills Assessment II	Question 4	Nagios
Attacking Common Applications - Skills Assessment II	Question 5	oilaKglm7M09@CPL&^lC
Attacking Common Applications - Skills Assessment II	Question 6	afe377683dce373ec2bf7eaf1e0107eb
Attacking Common Applications - Skills Assessment III	Question 1	P4s5w0rd!

Attacking Enterprise Network

Section	Question Number	Answer
Environment Enumeration	Question 1	HTB{1nt3rn4l_5cr1p7_l34k}
Linux Services & Internals Enumeration	Question 1	3.11
Credential Hunting	Question 1	W0rdpr3ss_sekur1ty!
Path Abuse	Question 1	/tmp
Escaping Restricted Shells	Question 1	HTB{35c4p3_7h3_r3stricted_5h311}
Special Permissions	Question 1	/bin/sed

Section	Question Number	Answer
Special Permissions	Question 2	/usr/bin/facter
Sudo Rights Abuse	Question 1	/usr/bin/openssl
Privileged Groups	Question 1	ch3ck_th0se_gr0uP_m3mb3erSh1Ps!
Capabilities	Question 1	HTB{c4paBili7i3s_pR1v35c}
Vulnerable Services	Question 1	91927dad55ffd22825660da88f2f92e0
Cron Job Abuse	Question 1	14347a2c977eb84508d3d50691a7ac4b
LXD	Question 1	HTB{C0nT41n3rs_uhhh}
Docker	Question 1	HTB{D0ck3r_Pr1vE5c}
Logrotate	Question 1	HTB{l0G_r0t7t73N_00ps}
Miscellaneous Techniques	Question 1	fc8c065b9384beaa162afe436a694acf
Kernel Exploits	Question 1	46237b8aa523bc7e0365de09c0c0164f
Shared Libraries	Question 1	6a9c151a599135618b8f09adc78ab5f1
Shared Object Hijacking	Question 1	2.27
Python Library Hijacking	Question 1	HTB{3xpl0i7iNG_Py7h0n_lI8R4ry_HIjiNX}
Sudo	Question 1	HTB{SuD0_e5c4l47i0n_1id}
Polkit	Question 1	HTB{p0Lk1tt3n}
Dirty Pipe	Question 1	HTB{D1rTy_DiR7Y}
Linux Local Privilege Escalation - Skills Assessment	Question 1	LLPE{d0n_ov3rl00k_h1dden_f1les!}
Linux Local Privilege Escalation - Skills Assessment	Question 2	LLPE{ch3ck_th0se_cmd_l1nes!}
Linux Local Privilege Escalation - Skills Assessment	Question 3	LLPE{h3y_l00k_a_fl@g!}
Linux Local Privilege Escalation - Skills Assessment	Question 4	LLPE{im_th3_m@nag3r_n0w}
Linux Local Privilege Escalation - Skills Assessment	Question 5	LLPE{0ne_sudo3r_t0_ru13_th3m_@ll!}

Linux Privilege Escalation

Section	Question Number	Answer
Environment Enumeration	Question 1	HTB{1nt3rn4l_5cr1p7_l34k}

Section	Question Number	Answer
Linux Services & Internals Enumeration	Question 1	3.11
Credential Hunting	Question 1	W0rdpr3ss_sekur1ty!
Path Abuse	Question 1	/tmp
Escaping Restricted Shells	Question 1	HTB{35c4p3_7h3_r3stricted_5h311}
Special Permissions	Question 1	/bin/sed
Special Permissions	Question 2	/usr/bin/facter
Sudo Rights Abuse	Question 1	/usr/bin/openssl
Privileged Groups	Question 1	ch3ck_th0se_gr0uP_m3mb3erSh1Ps!
Capabilities	Question 1	HTB{c4paBili7i3s_pR1v35c}
Vulnerable Services	Question 1	91927dad55ffd22825660da88f2f92e0
Cron Job Abuse	Question 1	14347a2c977eb84508d3d50691a7ac4b
LXD	Question 1	HTB{C0nT41n3rs_uhhh}
Docker	Question 1	HTB{D0ck3r_Pr1vE5c}
Logrotate	Question 1	HTB{l0G_r0t7t73N_00ps}
Miscellaneous Techniques	Question 1	fc8c065b9384beaa162afe436a694acf
Kernel Exploits	Question 1	46237b8aa523bc7e0365de09c0c0164f
Shared Libraries	Question 1	6a9c151a599135618b8f09adc78ab5f1
Shared Object Hijacking	Question 1	2.27
Python Library Hijacking	Question 1	HTB{3xpl0i7iNG_Py7h0n_lI8R4ry_HIjiNX}
Sudo	Question 1	HTB{SuD0_e5c4l47i0n_1id}
Polkit	Question 1	HTB{p0Lk1tt3n}
Dirty Pipe	Question 1	HTB{D1rTy_DiR7Y}
Linux Local Privilege Escalation - Skills Assessment	Question 1	LLPE{d0n_ov3rl00k_h1dden_f1les!}
Linux Local Privilege Escalation - Skills Assessment	Question 2	LLPE{ch3ck_th0se_cmd_l1nes!}
Linux Local Privilege Escalation - Skills Assessment	Question 3	LLPE{h3y_l00k_a_fl@g!}
Linux Local Privilege Escalation - Skills Assessment	Question 4	LLPE{im_th3_m@nag3r_n0w}

Section	Question Number	Answer
Linux Local Privilege Escalation - Skills Assessment	Question 5	LLPE{0ne_sudo3r_t0_ru13_th3m_@ll!}

Windows Privilege Escalation

Section	Question Number	Answer
Situational Awareness	Question 1	172.16.20.45
Situational Awareness	Question 2	powershell_ise.exe
Initial Enumeration	Question 1	SeTakeOwnershipPrivilege
Initial Enumeration	Question 2	sarah
Initial Enumeration	Question 3	tomcat8
Initial Enumeration	Question 4	sccm_svc
Initial Enumeration	Question 5	console
Communication with Processes	Question 1	filezilla server
Communication with Processes	Question 2	NT SERVICE\MSSQL$SQLEXPRESS01
SeImpersonate and SeAssignPrimaryToken	Question 1	F3ar_th3_p0tato!
SeDebugPrivilege	Question 1	64f12cddaa88057e06a81b54e73b949b
SeTakeOwnershipPrivilege	Question 1	1m_th3_f1l3_0wn3r_n0W!
Windows Built-in Groups	Question 1	Car3ful_w1th_gr0up_m3mberSh1p!
Event Log Readers	Question 1	W1ntergreen_gum_2021!
DnsAdmins	Question 1	Dll_abus3_ftw!
Print Operators	Question 1	Pr1nt_0p3rat0rs_ftw!
Server Operators	Question 1	S3rver_0perators_@ll_p0werfull!
User Account Control	Question 1	I_bypass3d_Uac!
Weak Permissions	Question 1	Aud1t_th0se_s3rv1ce_p3rms!
Kernel Exploits	Question 1	D0nt_fall_b3h1nd_0n_Patch1ng!
Vulnerable Services	Question 1	Aud1t_th0se_th1rd_paRty_s3rvices!
Credential Hunting	Question 1	Pr0xyadm1nPassw0rd!
Credential Hunting	Question 2	3ncryt10n_w0nt_4llw@ys_s@v3_y0u
Other Files	Question 1	1qazXSW@3edc!

Section	Question Number	Answer
Further Credential Theft	Question 1	S3cret_db_p@ssw0rd!
Further Credential Theft	Question 2	amanda
Further Credential Theft	Question 3	lLVCadm1n1qazZAQ!
Further Credential Theft	Question 4	Ftpuser!
Citrix Breakout	Question 1	CitR1X_Us3R_Esc@p3
Citrix Breakout	Question 2	C1tr!x_3sC@p3_@dm!n
Interacting with Users	Question 1	Password1
Pillaging	Question 1	mRemoteNG
Pillaging	Question 2	Princess01!
Pillaging	Question 3	HTB{Stealing_Cookies_To_AccessWebSites}
Pillaging	Question 4	Superbackup!
Pillaging	Question 5	BAC9DC5B7B4BEC1D83E0E9C04B477F26
Miscellaneous Techniques	Question 1	!QAZXSW@3edc
Windows Server	Question 1	L3gacy_st1ill_pr3valent!
Windows Desktop Versions	Question 1	Cm0n_l3ts_upgRade_t0_win10!
Windows Privilege Escalation Skills Assessment - Part I	Question 1	3199986&3200970
Windows Privilege Escalation Skills Assessment - Part I	Question 2	car3ful_st0rinG_cr3d$
Windows Privilege Escalation Skills Assessment - Part I	Question 3	Ev3ry_sysadm1ns_n1ghtMare!
Windows Privilege Escalation Skills Assessment - Part I	Question 4	5e5a7dafa79d923de3340e146318c31a
Windows Privilege Escalation Skills Assessment - Part II	Question 1	Inl@n3fr3ight_sup3rAdm1n!
Windows Privilege Escalation Skills Assessment - Part II	Question 2	el3vatEd_1nstall$_v3ry_r1sky
Windows Privilege Escalation Skills Assessment - Part II	Question 3	password1

Documentation & Reporting

Section	Question Number	Answer
Notetaking & Organization	Question 1	Tmux
Notetaking & Organization	Question 2	[Ctrl] + [B] + [Shift] + [%]
Types of Reports	Question 1	Vulnerability Assessment
Types of Reports	Question 2	Black Box
Components of a Report	Question 1	Executive Summary
Components of a Report	Question 2	False
How to Write Up a Finding	Question 1	Bad
Documentation & Reporting Practice Lab	Question 1	d0c_pwN_r3p0rt_reP3at!
Documentation & Reporting Practice Lab	Question 2	16e26ba33e455a8c338142af8d89ffbc
Documentation & Reporting Practice Lab	Question 3	Reporter1!
Documentation & Reporting Practice Lab	Question 4	Backup Operators

Attacking Enterprise Networks

Section	Question Number	Answer
External Information Gathering	Question 1	1337_HTB_DNS
External Information Gathering	Question 2	HTB{DNs_ZOn3_Tr@nsf3r}
External Information Gathering	Question 3	flag.inlanefreight.local
External Information Gathering	Question 4	monitoring
Service Enumeration & Exploitation	Question 1	HTB{0eb0ab788df18c3115ac43b1c06ae6c4}
Web Enumeration & Exploitation	Question 1	HTB{8f40ecf17f681612246fa5728c159e46}
Web Enumeration & Exploitation	Question 2	HTB{57c7f6d939eeda90aa1488b15617b9fa}

Section	Question Number	Answer
Web Enumeration & Exploitation	Question 3	HTB{e7134abea7438e937b87608eab0d979c}
Web Enumeration & Exploitation	Question 4	1fbea4df249ac4f4881a5da387eb297cf
Web Enumeration & Exploitation	Question 5	HTB{1nS3cuR3_c00k135}
Web Enumeration & Exploitation	Question 6	HTB{49f0bad299687c62334182178bfd75d8}
Web Enumeration & Exploitation	Question 7	HTB{32596e8376077c3ef8d5cf52f15279ba}
Web Enumeration & Exploitation	Question 8	HTB{dbca4dc5d99cdb3311404ea74921553c}
Web Enumeration & Exploitation	Question 9	HTB{bdd8a93aff53fd63a0a14de4eba4cbc1}
Initial Access	Question 1	b447c27a00e3a348881b0030177000cd
Post-Exploitation Persistence	Question 1	a34985b5976072c3c148abc751671302
Internal Information Gathering	Question 1	bf22a1d0acfca4af517e1417a80e92d1
Exploitation & Privilege Escalation	Question 1	0e20798f695ab0d04bc138b22344cea8
Exploitation & Privilege Escalation	Question 2	K33p_0n_sp00fing!
Lateral Movement	Question 1	!qazXSW@
Lateral Movement	Question 2	lucky7
Lateral Movement	Question 3	33a9d46de4015e7b3b0ad592a9394720
Lateral Movement	Question 4	1squints2
Active Directory Compromise	Question 1	Repeat09
Active Directory Compromise	Question 2	7c09eb1fff981654a3bb3b4a4e0d176a
Active Directory Compromise	Question 3	fd1f7e5564060258ea787ddbb6e6afa2
Post-Exploitation	Question 1	3c4996521690cc76446894da2bf7dd8f

Section	Question Number	Answer
Post-Exploitation	Question 2	206c03861986c0e264438cb6e8e90a19

Active Directory Enumeration & Attacks

Section	Question Number	Answer
External Recon and Enumeration Principles	Question 1	HTB{5Fz6UPNUFFzqjdg0AzXyxCjMZ}
Initial Enumeration of the Domain	Question 1	ACADEMY-EA-DC01.INLANEFREIGHT.LOCAL
Initial Enumeration of the Domain	Question 2	172.16.5.130
LLMNR/NBT-NS Poisoning - from Linux	Question 1	backupagent
LLMNR/NBT-NS Poisoning - from Linux	Question 2	h1backup55
LLMNR/NBT-NS Poisoning - from Linux	Question 3	transporter@4
LLMNR/NBT-NS Poisoning - from Windows	Question 1	security#1
Enumerating & Retrieving Password Policies	Question 1	7
Enumerating & Retrieving Password Policies	Question 2	8
Password Spraying - Making a Target User List	Question 1	56
Internal Password Spraying - from Linux	Question 1	sgage
Internal Password Spraying - from Windows	Question 1	dbranch
Credentialed Enumeration - from Linux	Question 1	mmorgan
Credentialed Enumeration - from Linux	Question 2	10
Credentialed Enumeration - from Windows	Question 1	13

Section	Question Number	Answer
Credentialed Enumeration - from Windows	Question 2	Test-AdminAccess
Credentialed Enumeration - from Windows	Question 3	sa
Credentialed Enumeration - from Windows	Question 4	ILFREIGHTDB01!
Living Off the Land	Question 1	4.18.2109.6
Living Off the Land	Question 2	adunn
Living Off the Land	Question 3	HTB{LD@P_I$_W1ld}
Kerberoasting - from Linux	Question 1	!SapperFi2
Kerberoasting - from Linux	Question 2	Account Operators
Kerberoasting - from Windows	Question 1	svc_vmwaresso
Kerberoasting - from Windows	Question 2	Virtual01
Access Control List (ACL) Abuse Primer	Question 1	DACL
Access Control List (ACL) Abuse Primer	Question 2	GenericAll
ACL Enumeration	Question 1	00299570-246d-11d0-a768-00aa006e0529
ACL Enumeration	Question 2	ResolveGUIDs
ACL Enumeration	Question 3	GenericWrite
ACL Enumeration	Question 4	GenericAll
ACL Enumeration	Question 5	Self-Membership
ACL Abuse Tactics	Question 1	SyncMaster757
DCSync	Question 1	syncron
DCSync	Question 2	Mycleart3xtP@ss!
DCSync	Question 3	4bb3b317845f0954200a6b0acc9b9f9a
Privileged Access	Question 1	bdavis
Privileged Access	Question 2	ACADEMY-EA-DC01
Privileged Access	Question 3	1m_the_sQl_@dm1n_n0w!
Bleeding Edge Vulnerabilities	Question 1	2021-42278&2021-42287

Section	Question Number	Answer
Bleeding Edge Vulnerabilities	Question 2	D0ntSl@ckonN0P@c!
Miscellaneous Misconfigurations	Question 1	ygroce
Miscellaneous Misconfigurations	Question 2	Pass@word
Domain Trusts Primer	Question 1	LOGISTICS.INLANEFREIGHT.LOCAL
Domain Trusts Primer	Question 2	FREIGHTLOGISTICS.LOCAL
Domain Trusts Primer	Question 3	BiDirectional
Attacking Domain Trusts - Child -> Parent Trusts - from Windows	Question 1	S-1-5-21-2806153819-209893948-922872689
Attacking Domain Trusts - Child -> Parent Trusts - from Windows	Question 2	S-1-5-21-3842939050-3880317879-2865463114-519
Attacking Domain Trusts - Child -> Parent Trusts - from Windows	Question 3	f@ll1ng_l1k3_d0m1no3$
Attacking Domain Trusts - Child -> Parent Trusts - from Linux	Question 1	49a074a39dd0651f647e765c2cc794c7
Attacking Domain Trusts - Cross-Forest Trust Abuse - from Windows	Question 1	1logistics
Attacking Domain Trusts - Cross-Forest Trust Abuse - from Linux	Question 1	sapsso
Attacking Domain Trusts - Cross-Forest Trust Abuse - from Linux	Question 2	pabloPICASSO
Attacking Domain Trusts - Cross-Forest Trust Abuse - from Linux	Question 3	burn1ng_d0wn_th3_f0rest!
Additional AD Auditing Techniques	Question 1	COMPLETE
AD Enumeration & Attacks - Skills Assessment Part I	Question 1	JusT_g3tt1ng_st@rt3d!

Section	Question Number	Answer
AD Enumeration & Attacks - Skills Assessment Part I	Question 2	svc_sql
AD Enumeration & Attacks - Skills Assessment Part I	Question 3	lucky7
AD Enumeration & Attacks - Skills Assessment Part I	Question 4	spn$*r0ast1ng_on*@n_0p3n_f1re
AD Enumeration & Attacks - Skills Assessment Part I	Question 5	tpetty
AD Enumeration & Attacks - Skills Assessment Part I	Question 6	Sup3rS3cur3D0m@inU2eR
AD Enumeration & Attacks - Skills Assessment Part I	Question 7	DCSync
AD Enumeration & Attacks - Skills Assessment Part I	Question 8	r3plicat1on_m@st3r!
AD Enumeration & Attacks - Skills Assessment Part II	Question 1	AB920
AD Enumeration & Attacks - Skills Assessment Part II	Question 2	weasal
AD Enumeration & Attacks - Skills Assessment Part II	Question 3	aud1t_gr0up_m3mbersh1ps!
AD Enumeration & Attacks - Skills Assessment Part II	Question 4	BR086
AD Enumeration & Attacks - Skills Assessment Part II	Question 5	Welcome1
AD Enumeration & Attacks - Skills Assessment Part II	Question 6	D@ta_bAse_adm1n!
AD Enumeration & Attacks - Skills Assessment Part II	Question 7	s3imp3rs0nate_cl@ssic
AD Enumeration & Attacks - Skills Assessment Part II	Question 8	exc3ss1ve_adm1n_r1ights!
AD Enumeration & Attacks - Skills Assessment Part II	Question 9	CT059
AD Enumeration & Attacks - Skills Assessment Part II	Question 10	charlie1
AD Enumeration & Attacks - Skills Assessment Part II	Question 11	acLs_f0r_th3_w1n!

Section	Question Number	Answer
AD Enumeration & Attacks - Skills Assessment Part II	Question 12	7eba70412d81c1cd030d72a3e8dbe05f