

## TABLE OF CONTENTS

Notes for the reader-----	01
Pentest Flow Chart-----	02
Recon (Web Based)-----	03
whois-----	04
way back machine-----	04
Google dorks-----	04
Shodan-----	04
DNSDumpster-----	04
Recon (CLI)-----	05
The Harvester-----	06
Dmitry-----	06
Recon (DNS)-----	07
Dig-----	08
DNSEnum-----	08
NSLookup-----	09
DNSRecon-----	09
Scanning and Enumeration (General)-----	10
Nmap-----	11
Nping-----	12
Nmap (Metasploit)-----	13
UnicornsCan-----	15
Netcat-----	15
Netdiscover-----	16
Dmitry-----	16
HPing3-----	17
Masscan-----	18
Enum4Linux-----	18
Scanning and Enumeration (SNMP)-----	19
Onesixtyone-----	20
Nmap(SNMP scripts)-----	20
SNMPwalk-----	21
Scanning and Enumeration (Null Session)-----	22
RPCClient-----	23
Nmap(Null Session)-----	23
Net use-----	23

<b>Scanning and Enumeration (SMB)</b>	<b>24</b>
Nbtscan	25
SMBClient	25
NMBLookup	26
Metasploit	26
<b>Scanning and Enumeration (Cisco)</b>	<b>27</b>
CGE	28
CISCO-Torch	29
<b>Scanning and Enumeration (web)</b>	<b>30</b>
wfuzz	31
Dirb	31
Metasploit	32
Dirsearch	32
WPScan	33
Recon-NG	34
Lynis	35
Skipfish	36
Oscanner	37
SIDGuesser	37
Nikto	38
Golismo	39
<b>Scanning and Enumeration (wifi)</b>	<b>40</b>
Pyrit	41
Reaver	41
Cowpatty	42
Airmon	42
Kismet	42
<b>Exploitation</b>	<b>43</b>
Metasploit	44
Net use	44
Powershell	45
Powershell Empire	45
Listeners	46
SET	46
PSEXec	47
BeEF	47

<b>Exploitation (Bruteforcing)</b>	<b>48</b>
Hydra	49
Medusa	50
<b>Exploitation (web)</b>	<b>51</b>
SQLI table	52
Wfuzz	52
SQLMap	53
XSSer	54
Manual XSS	54
Manual RFI	55
Manual LFI	55
Hydra	56
URL encoding	57
<b>Internal Recon (Windows)</b>	<b>58</b>
CLI information gathering	59
GUI information gathering	60
<b>Internal Recon (Linux)</b>	<b>61</b>
CLI information gathering	62
<b>Internal Recon (Network traffic)</b>	<b>63</b>
TCPDump	64
NETSH	65
<b>Establishing a Foothold (Linux)</b>	<b>66</b>
Spawning TTY shell	67
Reverse shells	68
Creating a user	70
Adding users to a group	70
Scheduling tasks	70
<b>Establishing a Foothold (Windows)</b>	<b>72</b>
Creating a user	73
Adding users to a group	73
Scheduling tasks	74
Persistence	74
<b>Privilege Escalation (Windows)</b>	<b>75</b>
Powershell Empire	76
Mimikatz	76
Locate/leverage world writable files	77
Locating passwords	77
Unquoted service path exploitation	78

<b>Privilege Escalation (Linux)</b>	<b>79</b>
Locate/leverage world writable files	80
UNIX-privesc-check	80
<b>Privilege Escalation (Both)</b>	<b>81</b>
Metasploit	82
Preparing Linux hashes for cracking	82
John	82
searchsploit	83
<b>Pivoting</b>	<b>84</b>
Proxychains	85
Metasploit	85
SSH port forwarding	86
<b>Data transfer</b>	<b>87</b>
Python file hosting	88
Downloading files (Linux)	88
Downloading files (windows)	88
SCP	88
Netcat webserver	88
TFTP	88
Connecting to shares	88
<b>Notepad</b>	<b>89</b>