3	100	Antivirus Evasion Tactics
1	29	Build Pen Test Infrastructure
3	10	Client-Side Exploits/Testing
4	21	CMD.EXE - Accounts and Groups
4	23	CMD.EXE - Firewall and Registry
4	31	CMD.EXE - FOR Loops
4	26	CMD.EXE - SMB and Services
4	18	CMD.EXE- Analyzing a System
1	116	Collaboration tools
1	51	Command Prompts
1	154	DNS Lookups
2	156	Enumerating Users - Account Names
2	160	Enumerating Users - SIDs
3	4	Exploitation - Why?
1	33	Free Tools and Vuln Resources
1	42	Hack Naked
4	133	Hydra (THC-Hydra)
1	193	Intro to Linux - Account stuff
1	220	Intro to Linux - Building Tools
1	197	Intro to Linux - File System Stuff
1	214	Intro to Linux - Network Stuff
1	224	Intro to Linux - Odds and Ends
1	207	Intro to Linux - Running Programs
1	114	Inventory
1	41	ISP - Network Infrastructure
3	17	Local Privilege Escalation Exploits
1	121	MetaData
3	127	Metasploit Databases
3	26	Metasploit Exploits
3	24	Metasploit File System
3	20	Metasploit Overview
3	30	Metasploit Payloads
3	132	Metasploit Tool Integrations
3	25	Metasploit User Interfaces
3	64	Meterpreter - Commands
3	62	Meterpreter - Intro
3	70	Meterpreter - Pivoting + Extras
3	67	Meterpreter - Target System Interaction
1	22	Methodologies
2	130	Nessus
2	170	Netcat for the Pentester
5	82	Nikto
2	42	Nmap
2	70	Nmap OS Fingerprinting
2	115	Nmap Scripting Engine (NSE)
2	74	Nmap Version Scanning
5	67	Pass-the-Hash Attacks
4	114	Password Attack Tips
5	25	Password Cracking - Cain
5	10	Password Cracking - Distributed Tools
5	4	Password Cracking - John the Ripper
5	45	Password Cracking - Rainbow Tables
4	125	Password Guessing - Account Lockout
4	174	Password Hash Dumping
4	156	Password Representation - Linux
4	160	Password Representation - Obtaining
4	147	Password Representation - Windows
4	111	Passwords - Overview
1	64	Pen Test Overall Process
4	57	Pen Tester's Pledge
1	7	Planning and Recon - Defining Terms
1	15	Planning and Recon - Motivation
2	29	Port Scanning (TCP/UDP)

4	11	Post Exploitation - Local File Pilfering
4	6	Post Exploitation - Moving Files
4	52	Post Exploitation - Run Commands on Remote Windows Machine
4	91	Powershell - Search, I/O, Extras
4	86	Powershell - The Pipeline
4	76	Powershell Basics
1	170	Recon-ng
1	119	Reconnaissance
1	99	Reporting
1	68	Rules of Engagement
2	4	Scanning - Goals and Types
2	8	Scanning - Tips
2	87	Scapy Making/Inspecting/Edit Packets
2	84	Scapy Overview
2	95	Scapy Responses/Reading Packets
2	93	Scapy Sending Packets
1	80	Scoping / Project Scope
1	161	Search Engine Vuln Finding
3	9	Service-Side Exploits
3	174	Shell Vs Terminal - Linux Workarounds
3	163	Shell Vs Terminal - Windows Workarounds
3	149	Shell Vs Terminal Dilemma
2	15	tcpdump
2	24	Traceroute (Linux/Unix)
2	26	Tracert (Windows)
1	18	Types/Phases of Pen Tests
3	104	Veil Framework - Veil Evasion
2	154	Vuln Scanners
2	111	Vulnerability Scanning
5	149	Web Apps - Command Injection
5	110	Web Apps - CSRF (XSRF)
5	108	Web Apps - Injection Attacks Overview
5	79	Web Apps - Overview
5	161	Web Apps - SQL Injection
5	127	Web Apps - XSS
1	150	Website Searches
1	142	Whois Lookups
5	92	ZAP (Zed Attack Proxy)