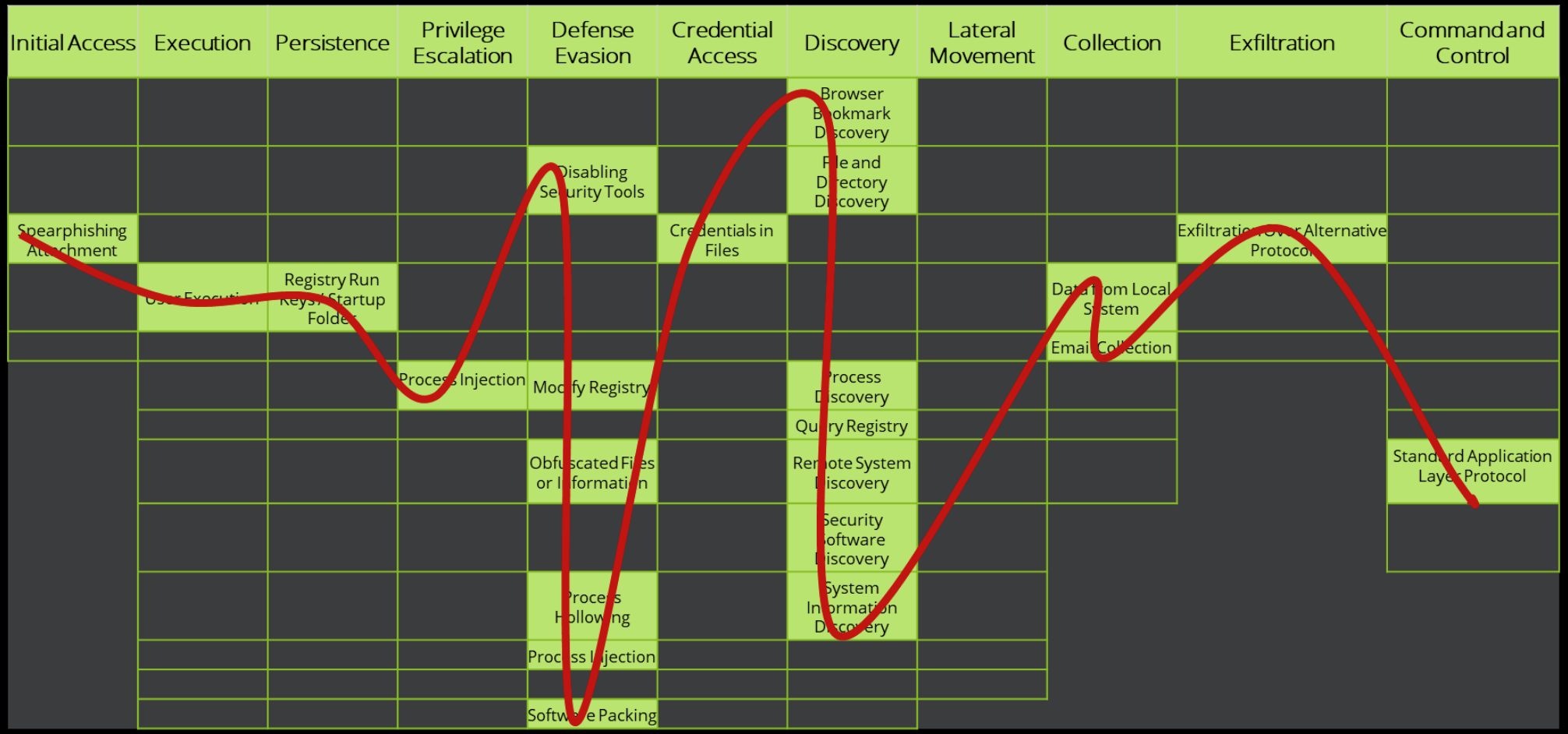
Ideas for Ethical Hacking Exercises

Santiago Hernández Ramos
@santiagohramos

Initial Access	T1192 - Spearphishing Attachment			
Execution	T1204 - User Execution			
Persistence	T1060 - Registry Run Keys / Startup Folder			
Privilege escalation	T1055 - Process Injection	T1093 - Process Hollowing		
Defense evasion	T1027 - Obfuscated Files or Information	T1112 - Modify Registry	T1045 - Software Packing	T1089 - Disabling Security Tools
Credential Access	T1081 - Credentials in Files			
Discovery	T1082 - System Information Discovery	T1018 - Remote System Discovery	T1057 - Process Discovery	T1063 - Security Software Discovery
Collection	T1005 - Data from Local System	T1114 - Email Collection		
Exfiltration	T1048 - Exfil. Over Alternative Protocol			
Command & Control	T1071 - Standard App Layer Protocol			


Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Exfiltration
Command and Control
Browser Bookmark Discovery
Disabling Security Tools
File and Directory Discovery
Spearphishing Attachment
Credentials in Files
Exfiltration Over Alternative Protocol
Registry Run Keys / Startup Folder
Data from Local System
Email Collection
Process Injection
Modify Registry
Process Discovery
Query Registry
Obfuscated Files or Information
Remote System Discovery
Standard Application Layer Protocol
Security Software Discovery
Process Hollowing
System Information Discovery
Process Injection
Software Packing