Red Team

Assumed Breach Model

[HackBahia]

Yuri Maia

- Red Team => Morphus
- Twitter / Github => @g0ttfrid
- Linkedin => in/yurimaia

Agenda

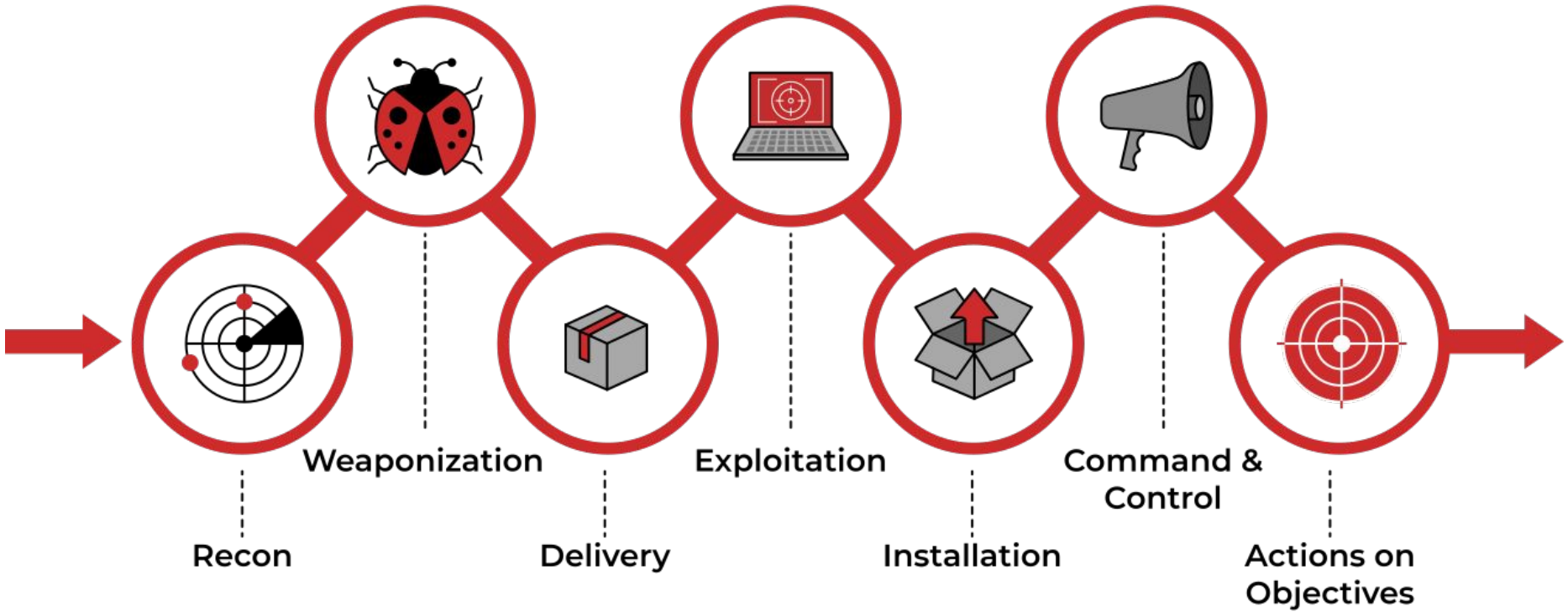
- Red Team
- Cyber Kill Chain
- Planning
- Execution

Red Team Development and Operations

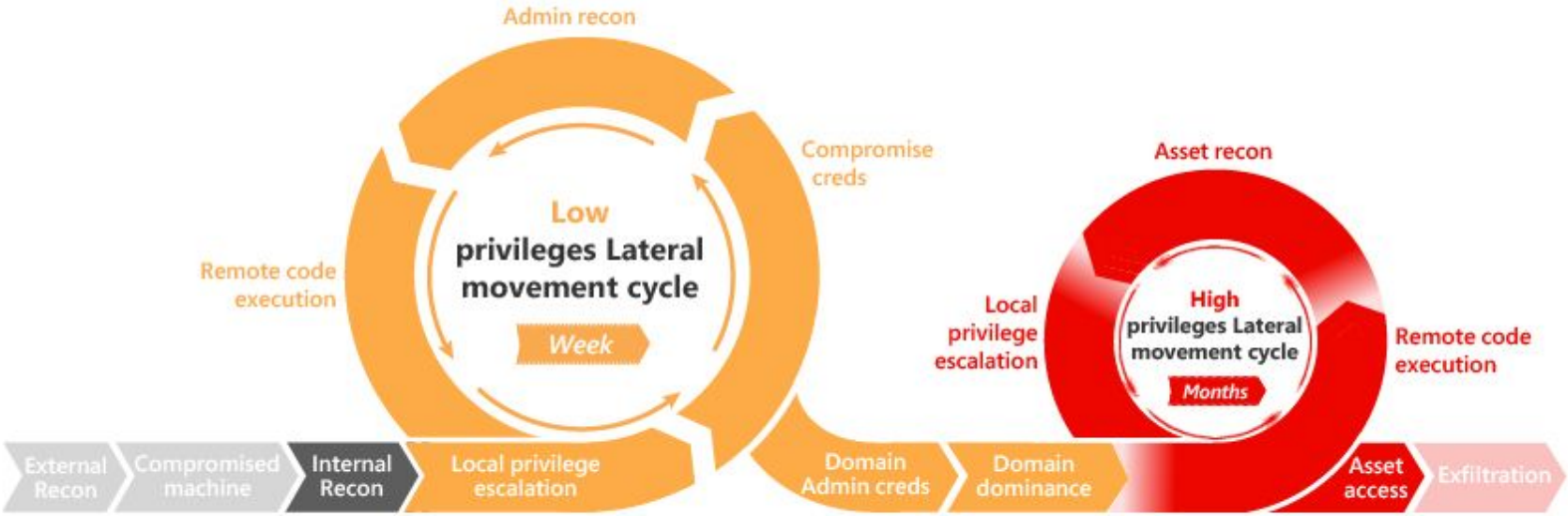
Red Teaming is the process of using tactics, techniques and procedures (TTPs) to emulate a real-world threat, with the goal of measuring the effectiveness of the people, processes and technologies used to defend an environment.

https://redteam.guide/

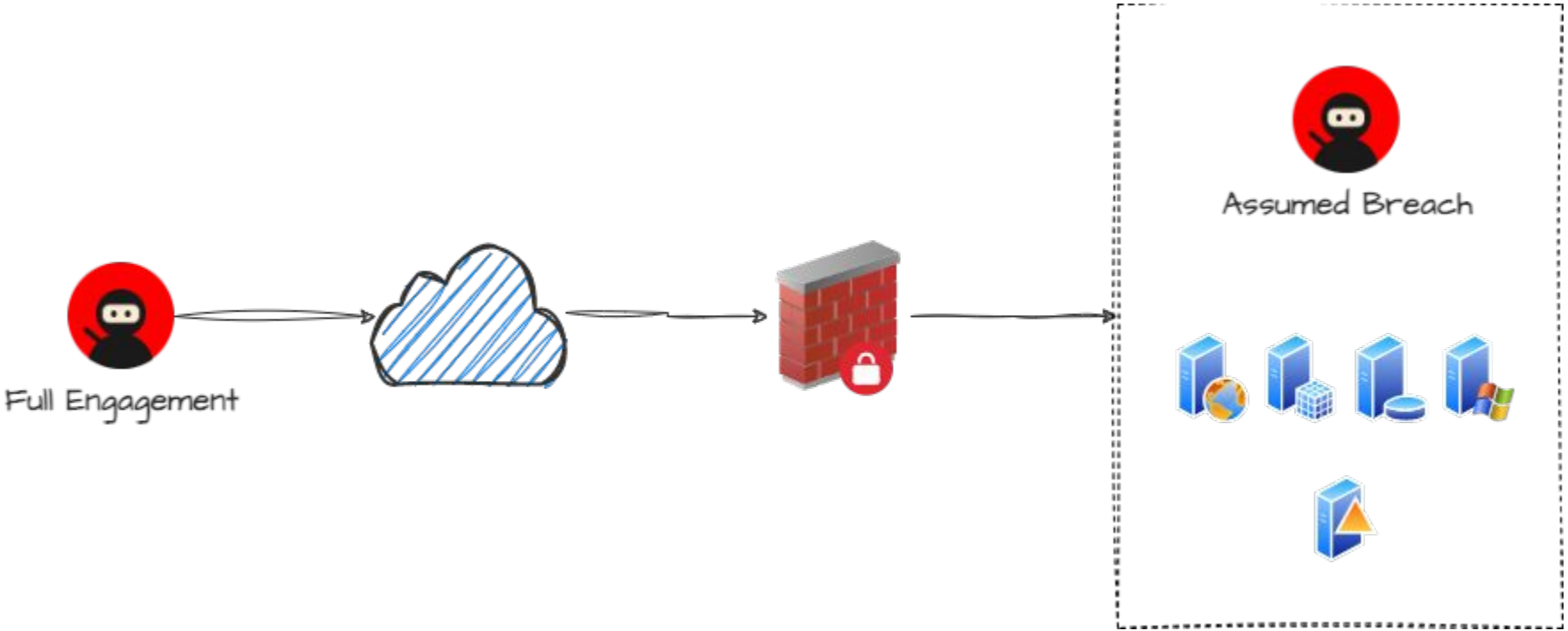
Cyber Kill Chain (Lockheed Martin)



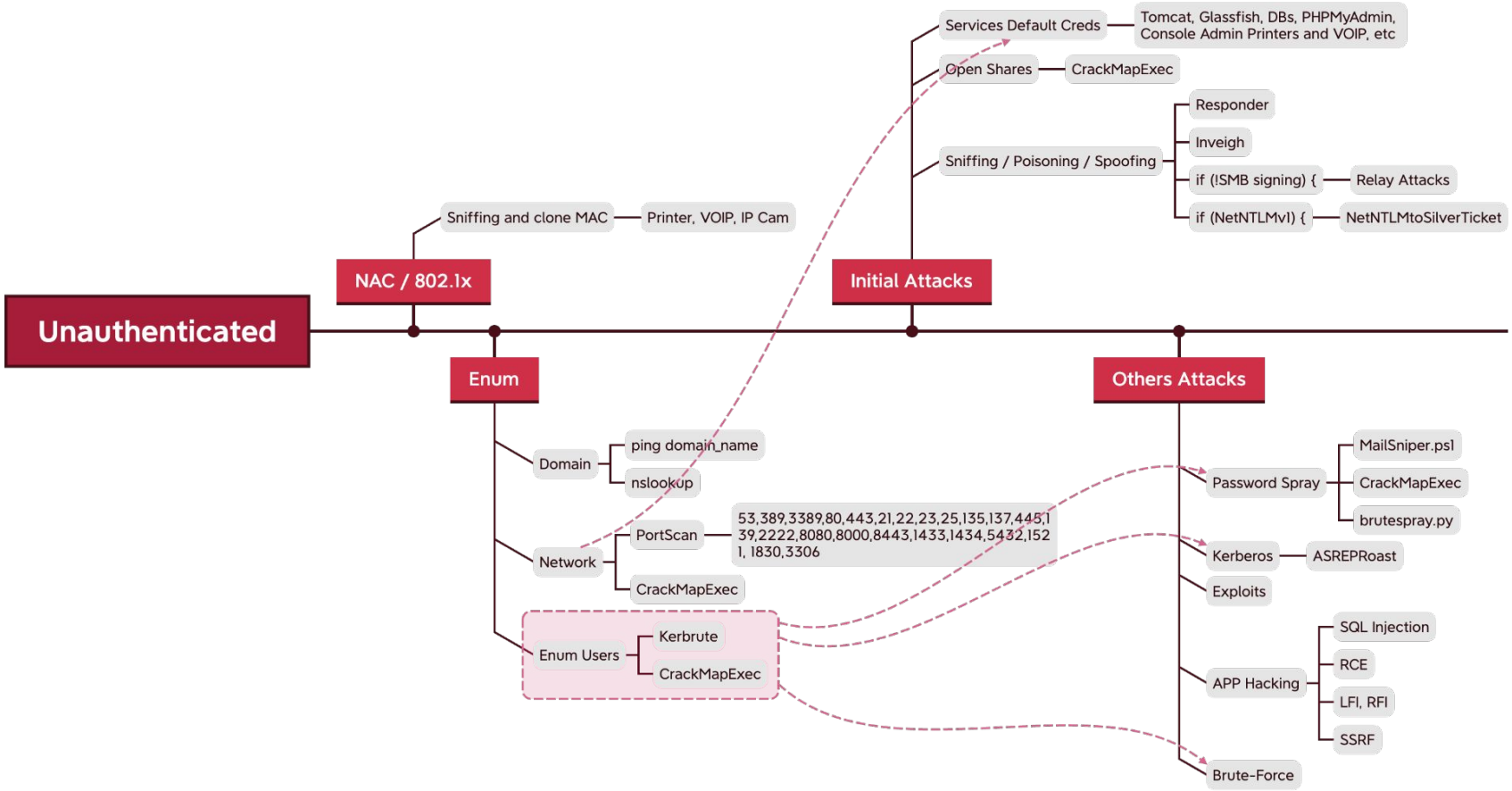
Cyber Kill Chain (Microsoft)

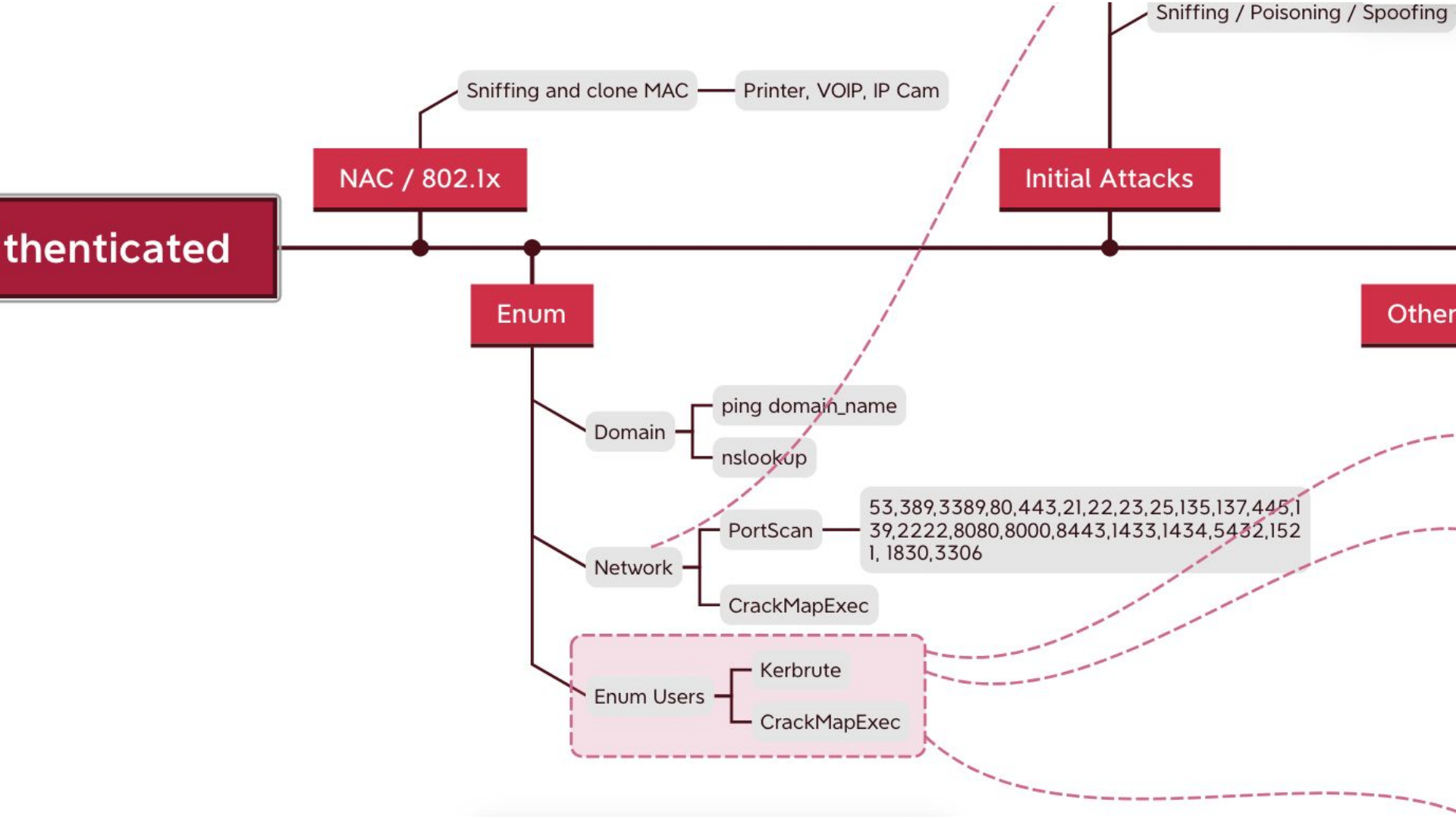


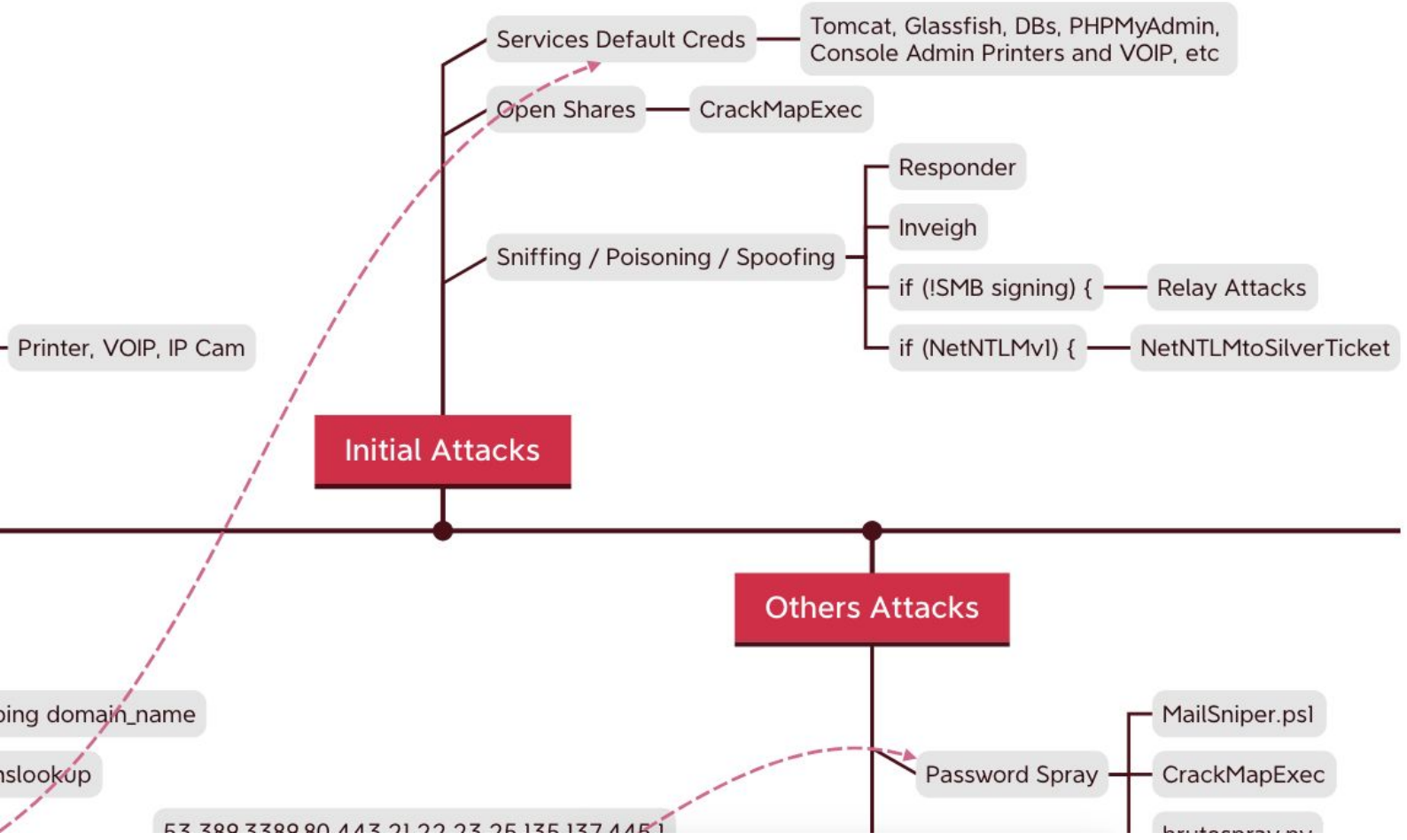
Planning - Model

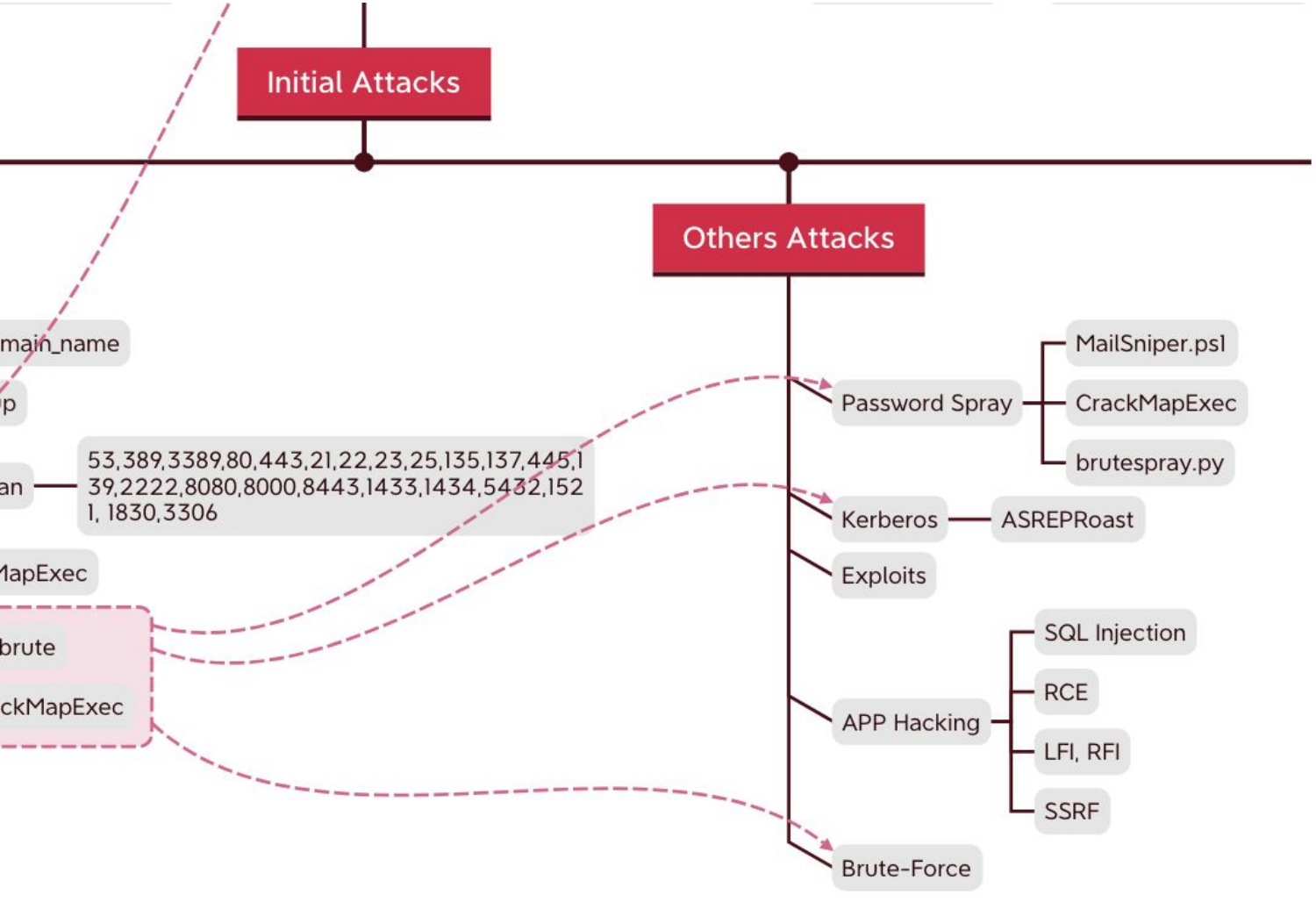


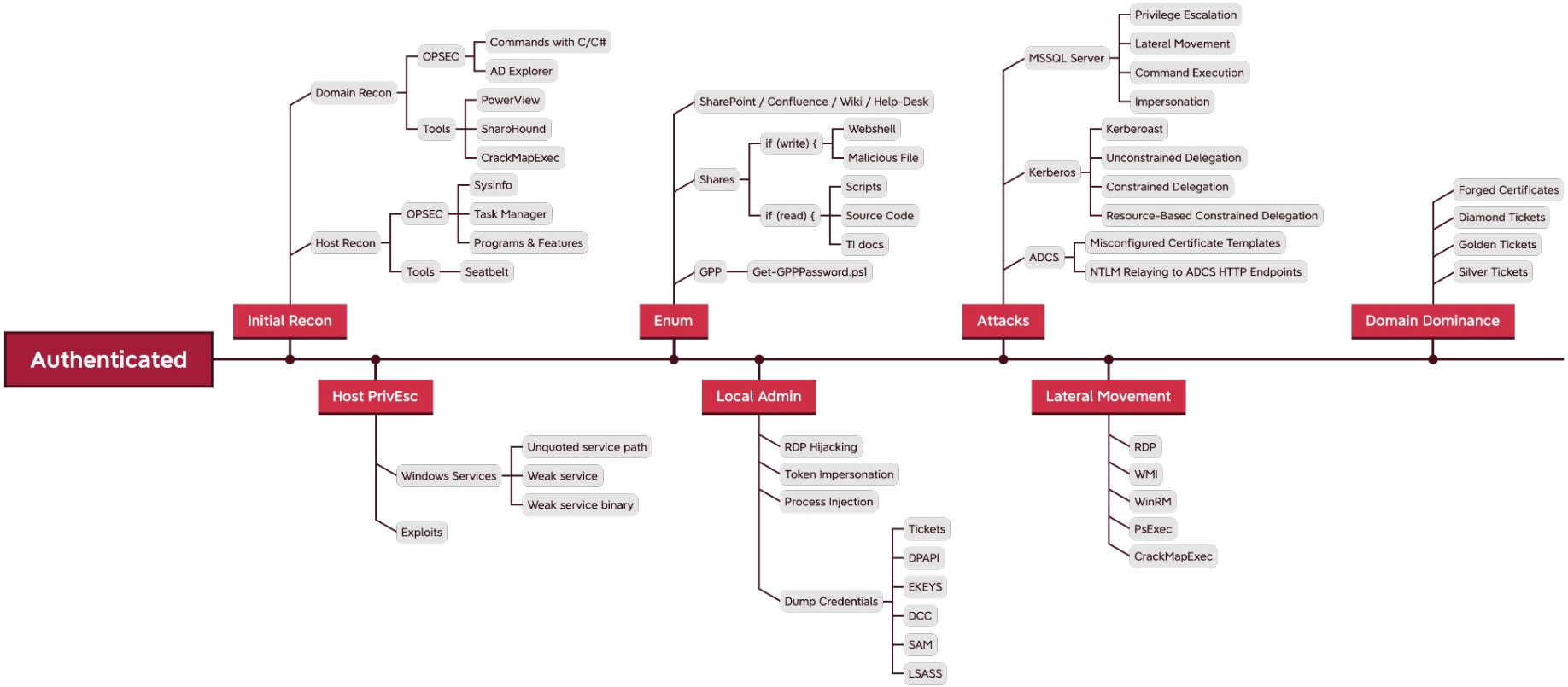
Execution

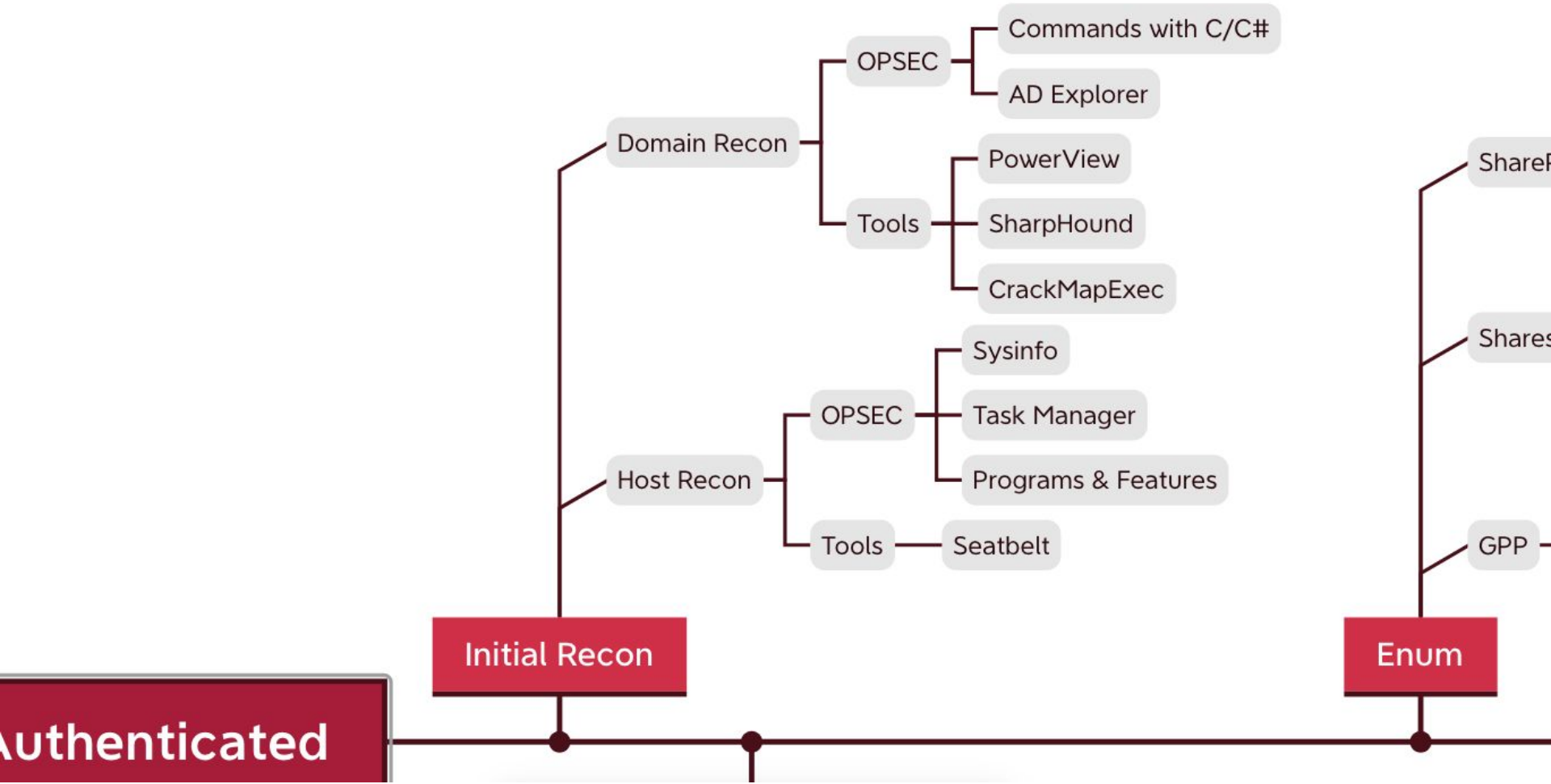


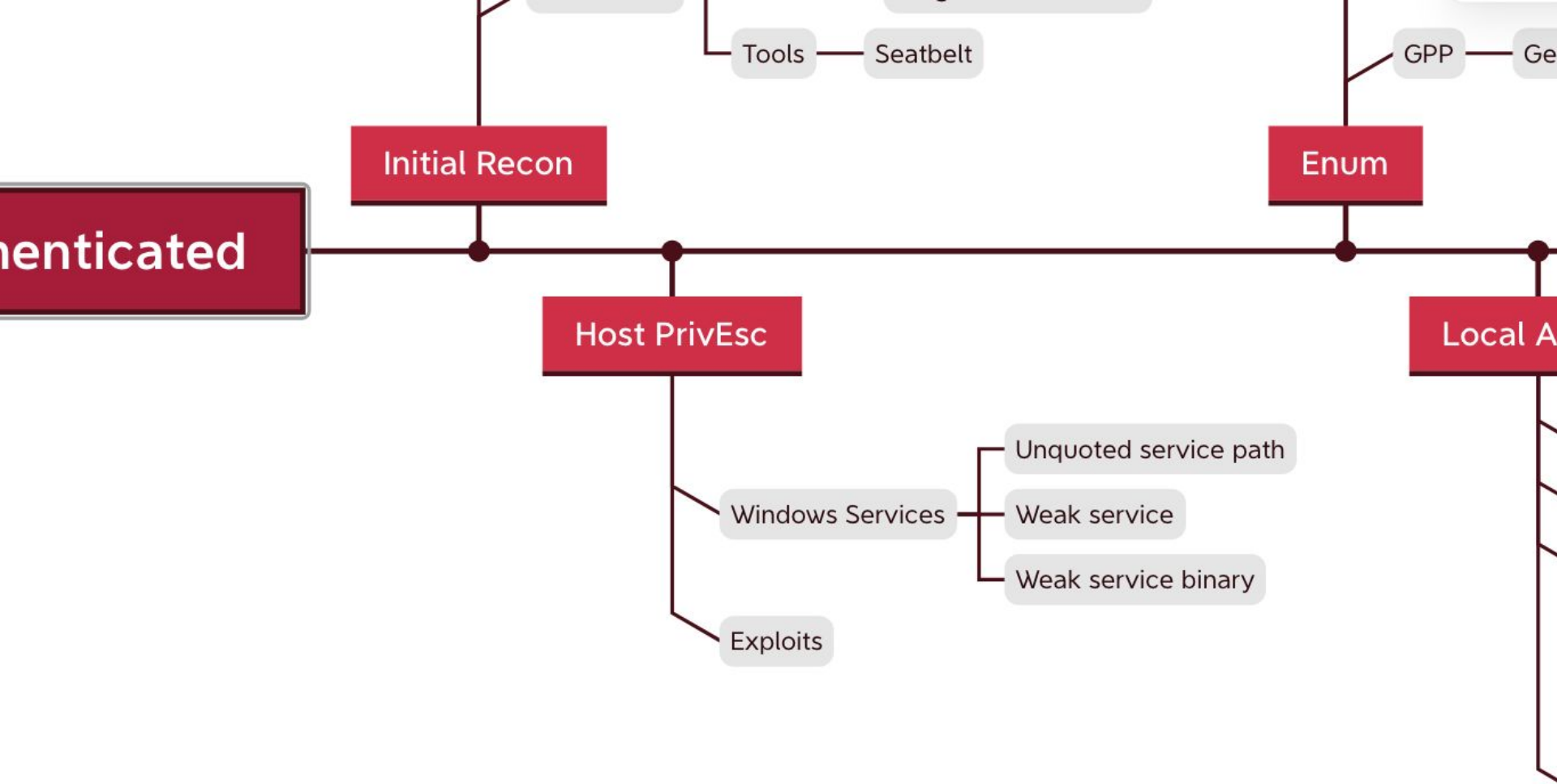

Sniffing / Poisoning / Spoofing
Sniffing and clone MAC
Printer, VOIP, IP Cam
NAC / 802.1x
Initial Attacks
thenticated
Enum
Other
Domain
ping domain_name
nslookup
Network
PortScan
53,389,3389,80,443,21,22,23,25,135,137,445,139,2222,8080,8000,8443,1433,1434,5432,1521, 1830,3306
CrackMapExec
Enum Users
Kerbrute
CrackMapExec

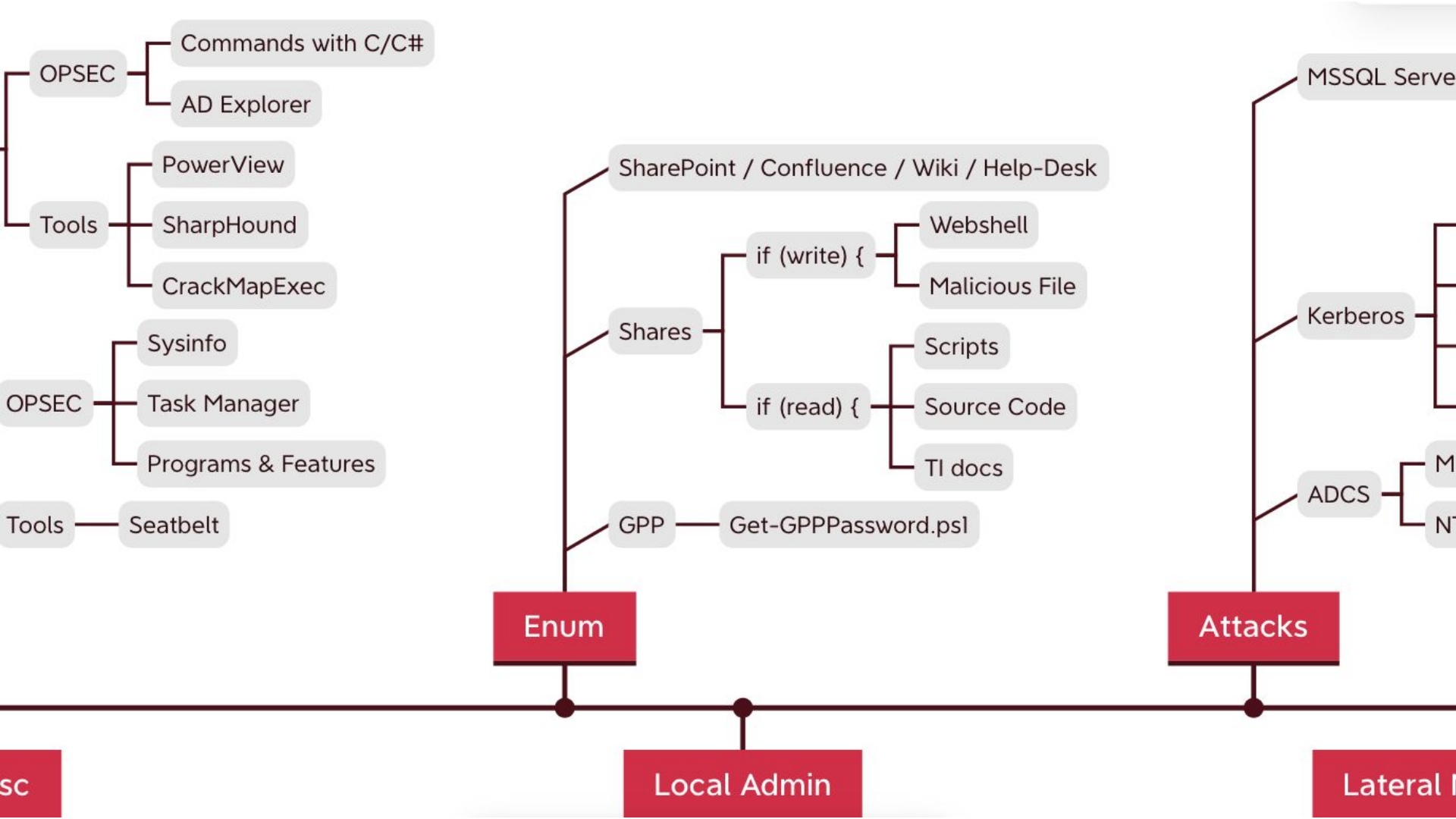

Services Default Creds
Tomcat, Glassfish, DBs, PHPMyAdmin, Console Admin Printers and VOIP, etc
Open Shares
CrackMapExec
Responder
Inveigh
Sniffing / Poisoning / Spoofing
if (!SMB signing) {
Relay Attacks
if (NetNTLMv1) {
NetNTLMtoSilverTicket
Printer, VOIP, IP Cam
Initial Attacks
Others Attacks
ping domain_name
nslookup
MailSniper.ps1
Password Spray
CrackMapExec

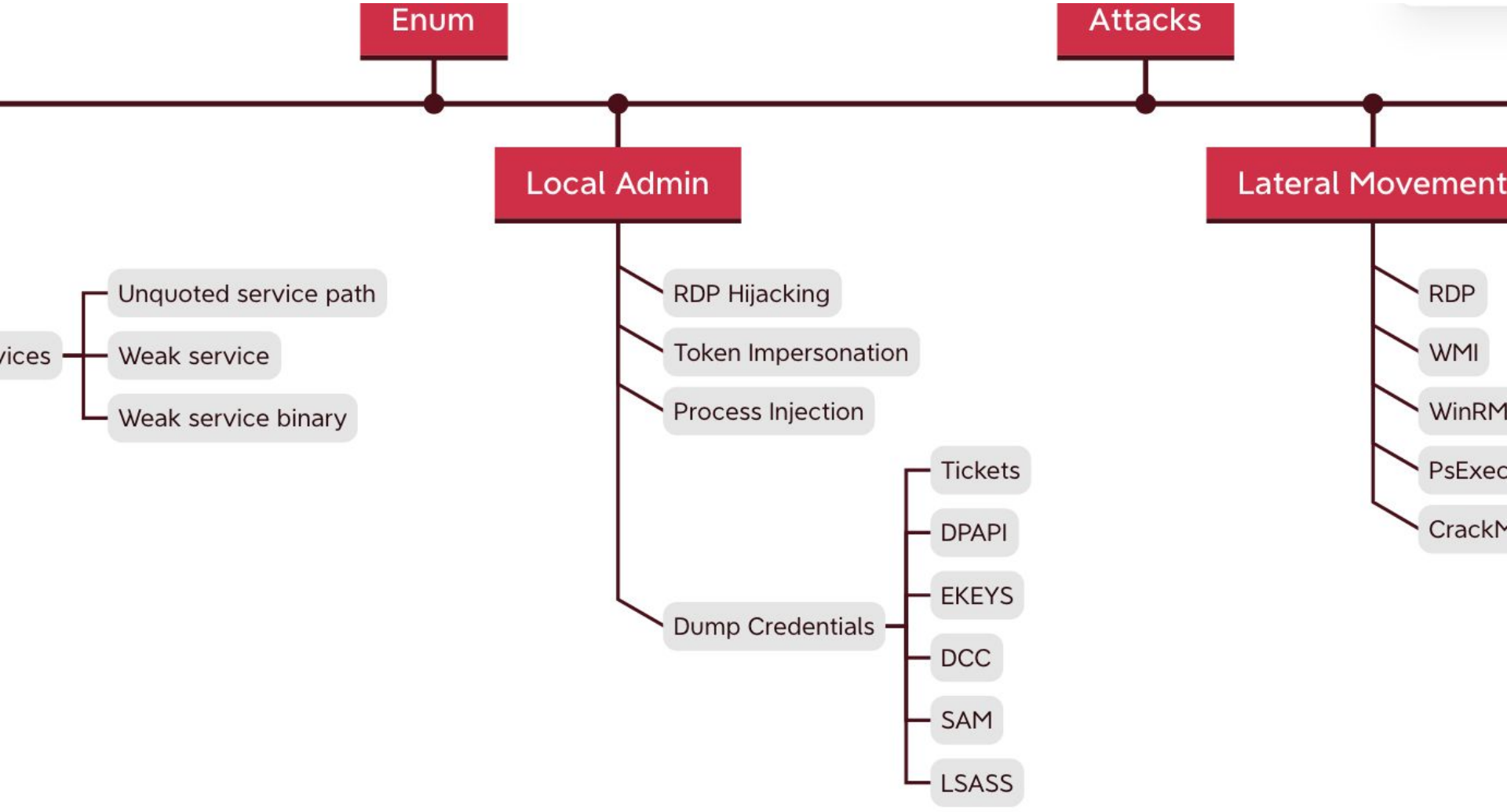

Initial Attacks
Others Attacks
main_name
p
an
53,389,3389,80,443,21,22,23,25,135,137,445,139,2222,8080,8000,8443,1433,1434,5432,1521, 1830,3306
MapExec
brute
ckMapExec
Password Spray
MailSniper.ps1
CrackMapExec
brutespray.py
Kerberos
ASREPRoast
Exploits
APP Hacking
SQL Injection
RCE
LFI, RFI
SSRF
Brute-Force

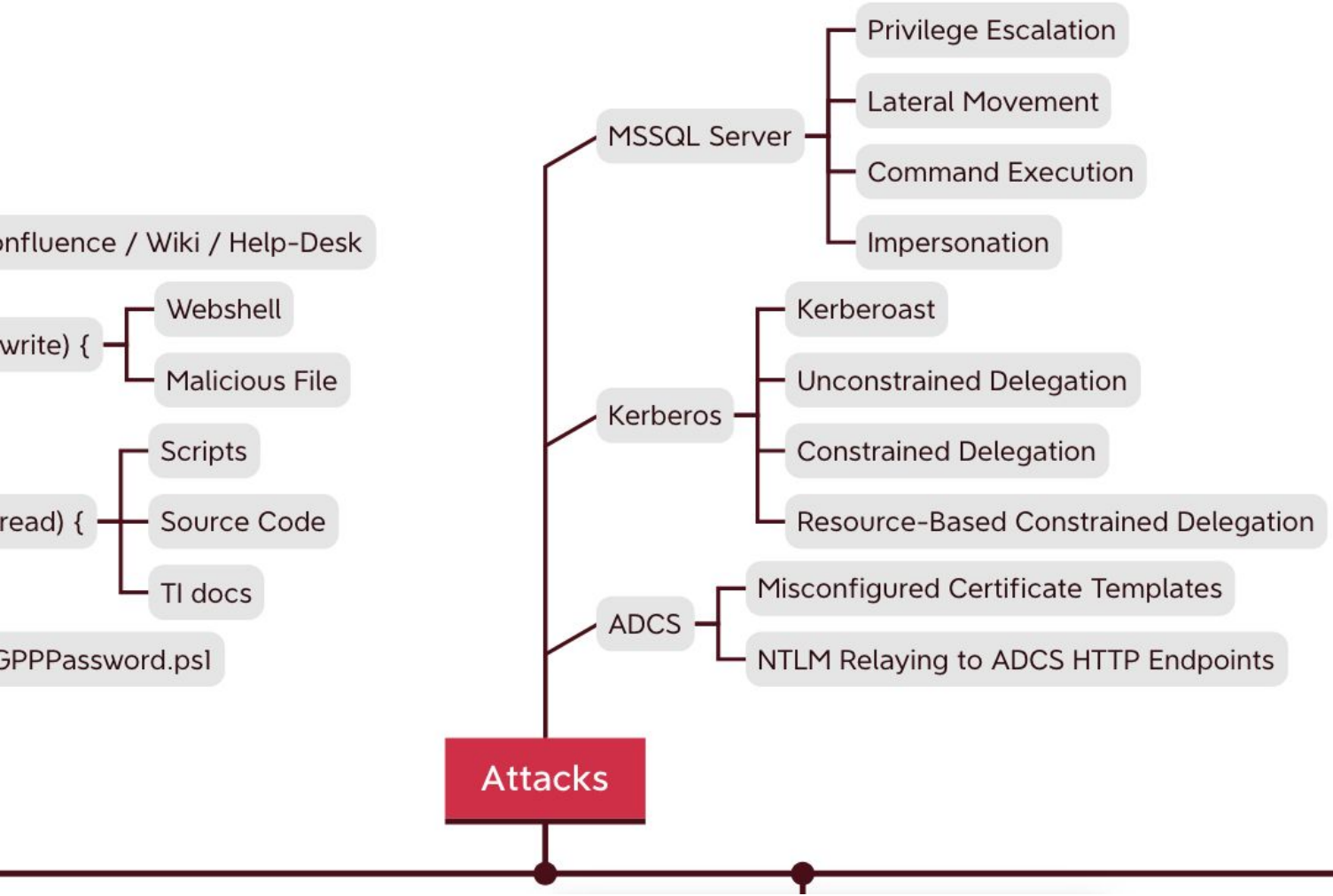


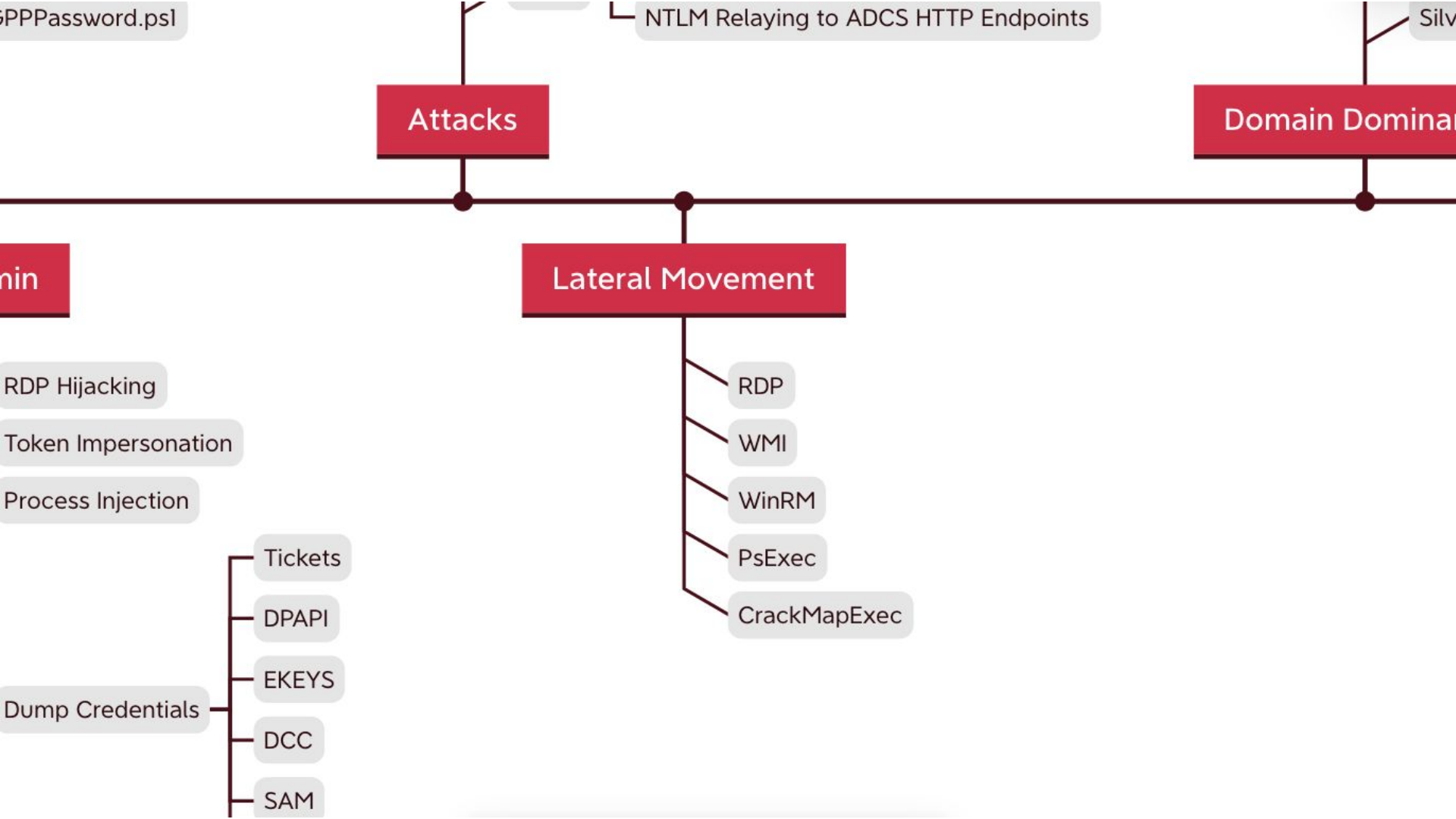

Commands with C/C#
OPSEC
AD Explorer
Domain Recon
PowerView
Tools
SharpHound
CrackMapExec
Sysinfo
OPSEC
Task Manager
Host Recon
Programs & Features
Tools
Seatbelt
Initial Recon
Enum
GPP
uthenticated

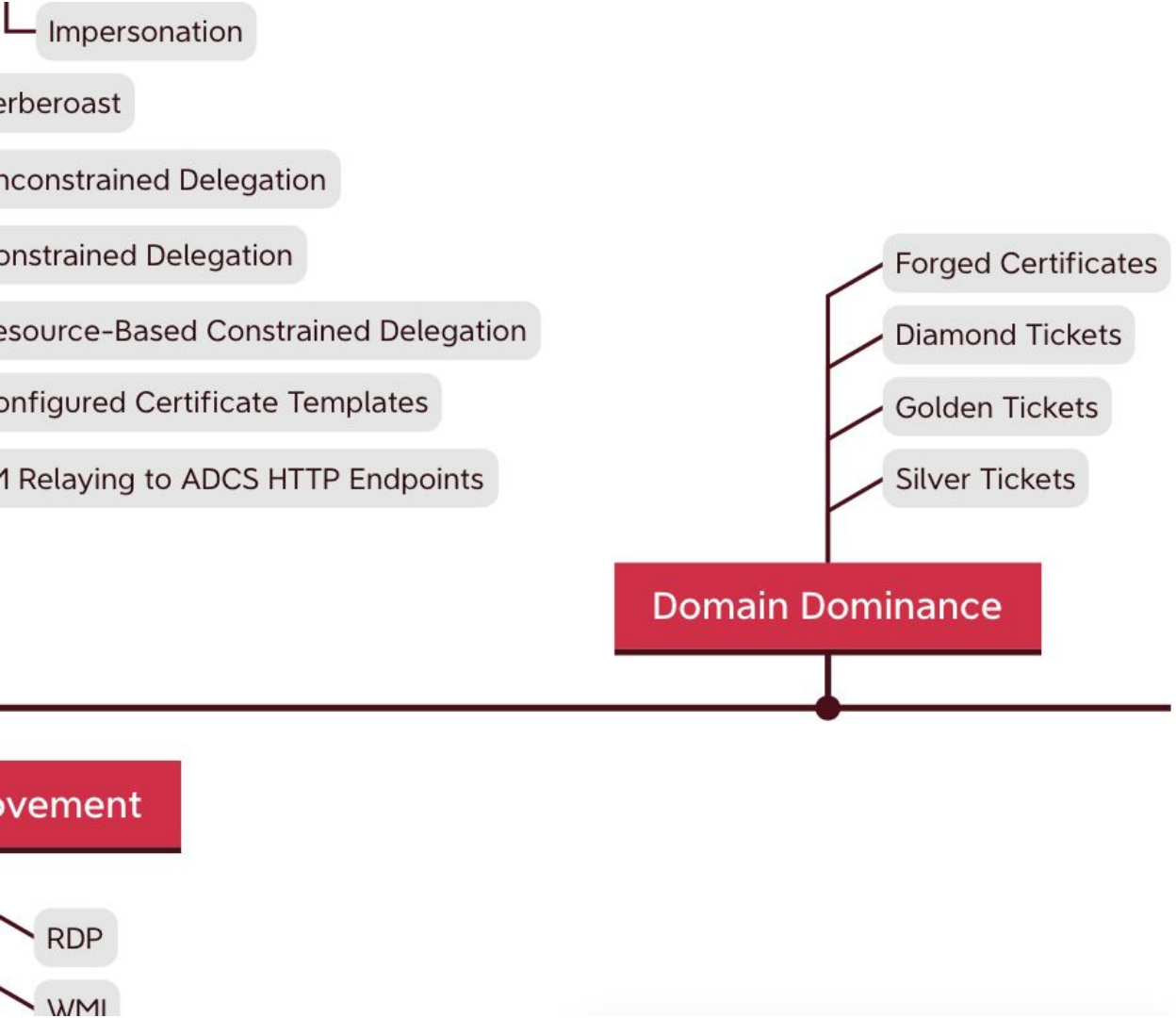

Tools
Seatbelt
GPP
Ge
Initial Recon
Enum
henticated
Host PrivEsc
Local A
Unquoted service path
Windows Services
Weak service
Weak service binary
Exploits


OPSEC
Commands with C/C#
AD Explorer
Tools
PowerView
SharpHound
CrackMapExec
OPSEC
Sysinfo
Task Manager
Programs & Features
Tools
Seatbelt
SharePoint / Confluence / Wiki / Help-Desk
Shares
if (write) {
Webshell
Malicious File
if (read) {
Scripts
Source Code
TI docs
GPP
Get-GPPPassword.ps1
MSSQL Serve
Kerberos
ADCS
Enum
Attacks
Local Admin
sc
Lateral


Enum
Attacks
Local Admin
Lateral Movement
vices
Unquoted service path
Weak service
Weak service binary
RDP Hijacking
Token Impersonation
Process Injection
Dump Credentials
Tickets
DPAPI
EKEYS
DCC
SAM
LSASS
RDP
WMI
WinRM
PsExec
CrackM


Privilege Escalation
Lateral Movement
MSSQL Server
Command Execution
Impersonation
onfluence / Wiki / Help-Desk
Webshell
write) {
Malicious File
Kerberoast
Kerberos
Unconstrained Delegation
Scripts
Constrained Delegation
read) {
Source Code
Resource-Based Constrained Delegation
TI docs
Misconfigured Certificate Templates
ADCS
GPPPassword.ps1
NTLM Relaying to ADCS HTTP Endpoints
Attacks
For
Dia
Gol
Silv
Domain Domina


GPPPassword.psl
NTLM Relaying to ADCS HTTP Endpoints
Attacks
Domain Domina
nin
Lateral Movement
RDP Hijacking
Token Impersonation
Process Injection
RDP
WMI
WinRM
PsExec
CrackMapExec
Tickets
DPAPI
EKEYS
Dump Credentials
DCC
SAM


Impersonation
erberoast
nconstrained Delegation
onstrained Delegation
esource-Based Constrained Delegation
onfigured Certificate Templates
M Relaying to ADCS HTTP Endpoints
Forged Certificates
Diamond Tickets
Golden Tickets
Silver Tickets
Domain Dominance
ovement
RDP
WMI


CONNECTION TERMINATED