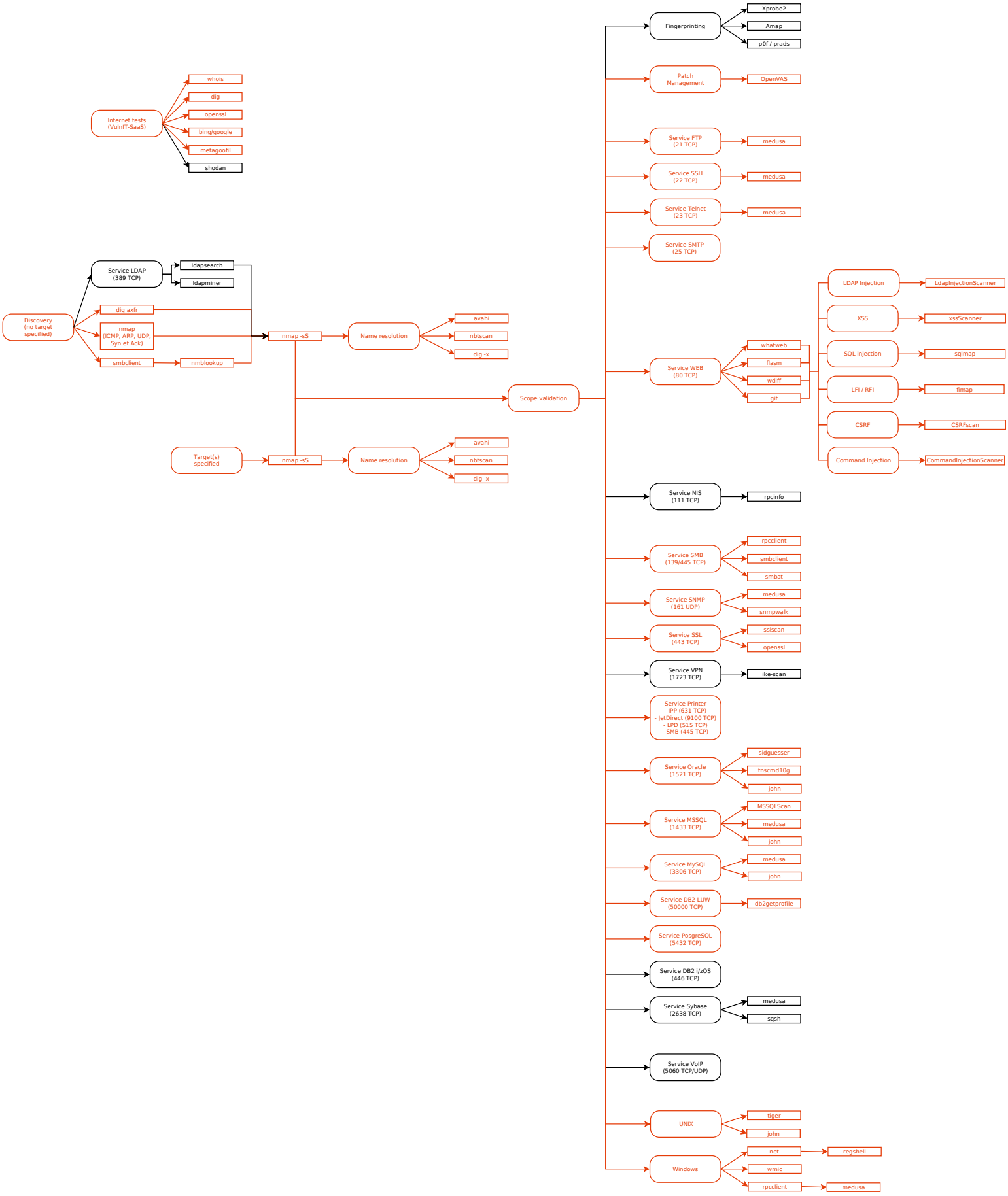
Internet tests (VulnIT-SaaS)
whois
dig
openssl
bing/google
metagoofil
shodan
Discovery (no target specified)
Service LDAP (389 TCP)
ldapsearch
ldapminer
dig axfr
nmap (ICMP, ARP, UDP, Syn et Ack)
smbclient
nmblookup
nmap -sS
Name resolution
avahi
nbtscan
dig -x
Scope validation
Target(s) specified
nmap -sS
Name resolution
avahi
nbtscan
dig -x
Fingerprinting
Xprobe2
Amap
p0f / prads
Patch Management
OpenVAS
Service FTP (21 TCP)
medusa
Service SSH (22 TCP)
medusa
Service Telnet (23 TCP)
medusa
Service SMTP (25 TCP)
Service WEB (80 TCP)
whatweb
flasm
wdiff
git
LDAP Injection
LdapInjectionScanner
XSS
xssScanner
SQL injection
sqlmap
LFI / RFI
fimap
CSRF
CSRFscan
Command Injection
CommandInjectionScanner
Service NIS (111 TCP)
rpcinfo
Service SMB (139/445 TCP)
rpcclient
smbclient
smbat
Service SNMP (161 UDP)
medusa
snmpwalk
Service SSL (443 TCP)
sslscan
openssl
Service VPN (1723 TCP)
ike-scan
Service Printer - IPP (631 TCP) - JetDirect (9100 TCP) - LPD (515 TCP) - SMB (445 TCP)
Service Oracle (1521 TCP)
sidguesser
tnscmd10g
john
Service MSSQL (1433 TCP)
MSSQLScan
medusa
john
Service MySQL (3306 TCP)
medusa
john
Service DB2 LUW (50000 TCP)
db2getprofile
Service PosgreSQL (5432 TCP)
Service DB2 i/zOS (446 TCP)
Service Sybase (2638 TCP)
medusa
sqsh
Service VoIP (5060 TCP/UDP)
UNIX
tiger
john
Windows
net
regshell
wmic
rpcclient
medusa