

Penetration Testing Execution Standard (PTES)

✓ = Geen kwetsbaarheid aangetroffen, X = Kwetsbaarheid gevonden, N/A = Niet van toepassing

PTES-ID	Intelligence Gathering	Status	ID
INTEL-01	OSINT	[Kies]	
INTEL-02	External footprinting	[Kies]	
INTEL-03	Internal footprinting	[Kies]	

PTES-ID	Vulnerability Analysis	Status	ID
ANALYZE-01	Active	[Kies]	
ANALYZE-02	Passive	[Kies]	
ANALYZE-03	Validation	[Kies]	
ANALYZE-04	Research	[Kies]	

PTES-ID	Exploitation	Status	ID
EXPLOIT-01	Countermeasures	[Kies]	
EXPLOIT-02	Precision Strike	[Kies]	
EXPLOIT-03	Customized Exploitation – Attacking the user	[Kies]	
EXPLOIT-04	Customized Exploitation – Directory services	[Kies]	
EXPLOIT-05	Customized Exploitation – Network	[Kies]	
EXPLOIT-06	Customized Exploitation – Webservices	[Kies]	
EXPLOIT-07	Customized Exploitation – WiFi	[Kies]	

PTES-ID	Post Exploitation	Status	ID
POST-01	Pillaging – Backup	[Kies]	
POST-02	Pillaging – Certificates (CA)	[Kies]	
POST-03	Pillaging – Cloud	[Kies]	
POST-04	Pillaging – Databases	[Kies]	
POST-05	Pillaging – Deployment	[Kies]	
POST-06	Pillaging – Directory services	[Kies]	
POST-07	Pillaging – Fileshares	[Kies]	
POST-08	Pillaging – Installed software	[Kies]	
POST-09	Pillaging – Monitoring and management	[Kies]	
POST-10	Pillaging – Source code management	[Kies]	
POST-11	Pillaging – User data	[Kies]	
POST-12	Pillaging – Video	[Kies]	
POST-13	Pillaging – Virtualization	[Kies]	
POST-14	Pillaging – WiFi	[Kies]	
POST-15	Windows Post-Exploitation	[Kies]	
POST-16	Linux/Unix Post-Exploitation	[Kies]	
POST-17	Data exfiltration	[Kies]	
POST-18	High value files	[Kies]	
POST-19	Persistence	[Kies]	