

Gytpol Validator | Audit konfigurační bezpečnosti

Jak si v oblasti konfiguračního hardeningu stojí vaše infrastruktura?

Gytpol umožňuje nezávazné otestování, proveditelné **v řádu jednotek hodin** včetně všech nezbytných příprav. Testování je možné ve variantách cloud i on-premise a umožní získat **komplexní přehled o vašem stavu konfigurační bezpečnosti**.

Gytpolem odhalené zranitelnosti jsou neviditelné pro technologie jako Vulnerability Management, EDR a antiviry, vzhledem k náročnosti manuální detekce jsou i penetračními testy nalezeny jen ve velmi omezené míře. Jejich výskyt na rovině koncových bodů je však snadno identifikovatelný útočníky a jejich zneužívání je běžnou praxí. Dle Microsoft Cyber Signals (8/2022) lze zneužití chybných konfigurací přisoudit až 80 % úspěšných ransomware útoků.

Výstupem testování je ucelená analýza konfigurační bezpečnosti pokrývající:

- Soulad AD a GPO politik s benchmarky CIS, NIST
- Detekce rizikových nastavení v rozporu s best practices
- Zranitelné konfigurace řadičů domény, serverů i desktopů
- Výskyty nevyužívaných účtů, privilegované účty s dlouhodobě neměnnými hesly
- Nesoulady konfigurací AD vs. koncový bod, konfliktní politiky
- Riziková defaultní nastavení
- Cleartextová hesla
- Nežádoucí lokální konfigurace

Nálezy jsou k dispozici bezprostředně po zprovoznění, Gytpol je pro usnadnění:

- Seřadí dle rizikovosti
- Opatří podrobným popisem problematiky
- Doplní ověřený nápravný postup
- Setřídí do kategorií, například:
 - Nálezy umožňující lateral movement
 - Nálezy umožňující eskalaci oprávnění
 - Nálezy související se SMB a sdílením
 - Nálezy spojené s možným zneužitím přihlašovacích údajů

Privilege Escalation				Credentials			
Sev.	Comput...	Topic	Subject	Sev.	Computers	Topic	Subject
H	16	Print Spooler Log ...	Print Spooler Log	H	1	Credential Manager	User credentials are stored
H	16	Print Spooler	Print Spooler service status	H	4	Service Account	Service using unsafe account
H	16	Batch Privilege	Dangerous privilege granted: Log on as a Batch	H	4	UAC	User Access Control status
H	11	Service Privilege	Dangerous privilege granted: Log on as a Service	L	1	IIS Anonymous	IIS open to anonymous login
M	12	Log on Locally Priv...	Dangerous privilege granted: Allow log on Locally	H	1	Windows LAPS	LAPS Installation
M	4	Local Users Logon...	Local users logon date	M	5	Device Guard	Windows Defender Credential Guard
M	4	Local Users	Local user activity	H	1	IIS Credentials	IIS web service using unprotected credentials