# Références des risques

## Les références PingCastle

|  |  |
| --- | --- |
| Index | Nom |
| 1 | T-SIDFiltering |
| 2 | A-AuditDC |
| 3 | A-CertEnrollHttp |
| 4 | A-CertTempCustomSubject |
| 5 | A-DCLdapsChannelBinding |
| 6 | A-DCLdapSign |
| 7 | A-DnsZoneAUCreateChild |
| 8 | A-DnsZoneTransfert |
| 9 | A-DsHeuristicsLDAPSecurity |
| 10 | A-Krbtgt |
| 11 | A-LAPS-Joined-Computers |
| 12 | A-NoNetSessionHardening |
| 13 | A-NoServicePolicy |
| 14 | A-PreWin2000AuthenticatedUsers |
| 15 | A-PreWin2000Other |
| 16 | A-SHA1RootCert |
| 17 | A-UnixPwd |
| 18 | A-WeakRSARootCert2 |
| 19 | P-AdminPwdTooOld |
| 20 | P-ControlPathIndirectMany |
| 21 | P-Delegated |
| 22 | P-DelegationGPOData |
| 23 | P-DNSAdmin |
| 24 | P-Kerberoasting |
| 25 | P-LogonDenied |
| 26 | P-OperatorsEmpty |
| 27 | P-ProtectedUsers |
| 28 | P-ServiceDomainAdmin |
| 29 | P-UnconstrainedDelegation |
| 30 | P-UnkownDelegation |
| 31 | S-ADRegistration |
| 32 | S-ADRegistrationSchema |
| 33 | S-DesEnabled |
| 34 | S-OS-2003 |
| 35 | S-OS-2008 |
| 36 | S-OS-Win7 |
| 37 | S-OS-XP |
| 38 | S-PwdLastSet-90 |
| 39 | S-PwdLastSet-DC |
| 40 | S-PwdNeverExpires |
| 41 | S-PwdNotRequired |
| 42 | S-Reversible |
| 43 | S-SIDHistory |
| 44 | S-SMB-v1 |
| 45 | S-WSUS-HTTP |
| 46 | T-AlgsAES |
| 47 | T-Inactive |
| 48 | T-SIDHistoryUnknownDomain |

## Les corrélations PingCastle

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| PingCastle | METSYS | PurpleKnight | ANSSI | MITRE ATT&CK |
| 1 | 1 | 1 | 10 | 1, 13 |
| 2 | 36 |  |  | 5 |
| 3 | 32 |  |  | 19 |
| 4 | 6 | 5, 16 | 11 | 21 |
| 5 | 37 |  |  | 19 |
| 6 | 38 |  |  | 19 |
| 7 | 27 |  |  | 19 |
| 8 | 29 |  |  |  |
| 9 | 51 |  | 22 | 14 |
| 10 | 3 | 14 | 16 | 22 |
| 11 | 35 | 6 |  | 2, 18 |
| 12 | 50 |  |  | 10 |
| 13 | 9 |  |  | 15 |
| 14 | 39 | 7 | 21 | 12, 16 |
| 15 | 39 | 7 | 21 | 12, 16 |
| 16 | 7 |  | 20 | 26 |
| 17 | 52 |  | 24 | 17 |
| 18 | 7 |  | 20 | 26 |
| 19 | 11 | 3, 4, 10, 34, 35 | 5, 14, 17 | 1, 4 |
| 20 | 30 |  |  | 4, 9 |
| 21 | 10 |  |  | 1, 25 |
| 22 | 14 |  |  | 1 |
| 23 | 28 |  |  | 4, 8 |
| 24 | 24 | 21, 24, 36 | 8 | 23 |
| 25 | 34 |  |  |  |
| 26 | 53 | 20 |  | 4 |
| 27 | 33 | 25 | 23 | 3, 4 |
| 28 | 16 | 22 | 3 | 7 |
| 29 | 40 | 8 | 13 | 1 |
| 30 | 17 |  |  | 1, 14 |
| 31 | 35 | 6 |  | 2, 18 |
| 32 | 13 |  | 19 | 2 |
| 33 | 4 | 32 | 15 | 24 |
| 34 | 12 | 9 |  | 6 |
| 35 | 12 | 9 |  | 6 |
| 36 | 12 | 9 |  | 6 |
| 37 | 12 | 9 |  | 6 |
| 38 | 11 | 3, 4, 10, 34, 35 | 5, 14, 17 | 1, 4 |
| 39 |  |  | 4 | 1 |
| 40 |  | 3, 4, 10, 34, 35 | 5, 14, 17 | 1, 4 |
| 41 |  |  |  | 1 |
| 42 |  | 31 | 24 | 11 |
| 43 |  |  | 25 | 13 |
| 44 |  |  |  | 20 |
| 45 |  |  |  | 6 |
| 46 |  |  |  | 6 |
| 47 |  | 27 | 18 | 19 |
| 48 |  |  | 25 | 13 |

## Les références PurpleKnight

|  |  |
| --- | --- |
| Index | Nom |
| 1 | Outbound forest trust with SID History enabled |
| 2 | AD Certificate Authority with Web Enrollment - PetitPotam and ESC8 |
| 3 | Admins with old passwords |
| 4 | Built-in domain Administrator account with old password (180 days) |
| 5 | Certificate templates with three or more insecure configurations |
| 6 | Changes to MS LAPS read permissions |
| 7 | Changes to PreWindows 2000 Compatible Access Group membership |
| 8 | Computer or user accounts with unconstrained delegation |
| 9 | Computers with older OS versions |
| 10 | Computers with password last set over 90 days ago |
| 11 | Dangerous control paths expose certificate templates |
| 12 | Domain trust to a third-party domain without quarantine |
| 13 | gMSA objects with old passwords |
| 14 | Kerberos krbtgt account with old password |
| 15 | LDAP signing is not required on Domain Controllers |
| 16 | Modèles de certificats qui permettent aux demandeurs de spécifier un subjectAltName |
| 17 | Non-default principals with DC Sync rights on the domain |
| 18 | Non-privileged users with access to gMSA passwords |
| 19 | Objects with constrained delegation configured |
| 20 | Operator Groups that are not empty |
| 21 | Primary users with SPN not supporting AES encryption on Kerberos |
| 22 | Privileged accounts with a password that never expires |
| 23 | Privileged users that are disabled |
| 24 | Privileged users with ServicePrincipalNames defined |
| 25 | Protected Users group not in use |
| 26 | RC4 or DES encryption type are supported by Domain Controllers |
| 27 | Trust accounts with old passwords |
| 28 | Unprivileged principals as DNS Admins |
| 29 | Unprivileged users can add computer accounts to domain |
| 30 | Unprotected accounts with adminCount=1 |
| 31 | User accounts that store passwords with reversible encryption |
| 32 | User accounts that use DES encryption |
| 33 | User accounts with password not required |
| 34 | Users with old passwords |
| 35 | Users with Password Never Expires flag set |
| 36 | Users with ServicePrincipalName defined |

## Les corrélations PurpleKnight

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| PurpleKnight | METSYS | PingCastle | ANSSI | MITRE ATT&CK |
| 1 | 1 | 1 | 9, 10 | 1, 13 |
| 2 | 5 |  |  |  |
| 3 | 11 | 19, 38, 40 | 5, 14, 17 | 1, 4 |
| 4 | 11 | 19, 38, 40 | 5, 14, 17 | 1, 4 |
| 5 | 6 | 4 | 11 | 21 |
| 6 | 35 | 11, 31 |  | 2, 18 |
| 7 | 39 | 14, 15 | 21 | 12, 16 |
| 8 | 40 | 29 | 13 | 1 |
| 9 | 12 | 34, 35, 36, 37 |  | 6 |
| 10 | 11 | 19, 38, 40 | 5, 14, 17 | 1, 4 |
| 11 | 19 |  | 1 |  |
| 12 | 1 | 1 | 9, 10 | 1, 13 |
| 13 | 21 |  |  |  |
| 14 | 3 | 10 | 16 | 22 |
| 15 | 23 |  |  |  |
| 16 | 6 | 4 | 11 | 21 |
| 17 | 8 |  | 7 |  |
| 18 | 22 |  |  |  |
| 19 | 45 |  |  |  |
| 20 | 53 | 26 |  | 4 |
| 21 | 24 | 24 | 8 | 23 |
| 22 | 16 | 28 | 3 | 7 |
| 23 | 46 |  |  |  |
| 24 | 24 | 24 | 8 | 23 |
| 25 | 33 | 27 | 23 | 3, 4 |
| 26 | 25 |  |  |  |
| 27 | 15 | 47 | 18 | 19 |
| 28 | 26 |  | 2, 6 |  |
| 29 | 47 |  |  |  |
| 30 | 48 |  |  |  |
| 31 | 42 | 42 | 24 | 11 |
| 32 | 4 | 33 | 15 | 24 |
| 33 | 49 |  |  |  |
| 34 | 11 | 19, 38, 40 | 5, 14, 17 | 1, 4 |
| 35 | 11 | 19, 38, 40 | 5, 14, 17 | 1, 4 |
| 36 | 24 | 24 | 8 | 23 |

## Les références ANSSI

|  |  |
| --- | --- |
| Index | Nom |
| 1 | vuln1\_adcs\_template\_ control |
| 2 | vuln1\_dnsadmins |
| 3 | vuln1\_dont\_expire\_priv |
| 4 | vuln1\_password\_change\_dc\_no\_change |
| 5 | vuln1\_password\_change\_priv |
| 6 | vuln1\_permissions\_msdn |
| 7 | vuln1\_permissions\_naming\_context |
| 8 | vuln1\_spn\_priv |
| 9 | vuln1\_trusts\_domain\_notfiltered |
| 10 | vuln1\_trusts\_forest\_sidhistory |
| 11 | vuln1\_vuln\_adcs\_template\_auth\_enroll\_with\_name |
| 12 | vuln1\_vuln\_display\_specifier |
| 13 | vuln2\_delegation\_t4d |
| 14 | vuln2\_dont\_expire |
| 15 | vuln2\_kerberos\_properties\_deskey |
| 16 | vuln2\_krbtgt |
| 17 | vuln2\_password\_change\_server\_no\_change\_90 |
| 18 | vuln2\_trusts\_accounts |
| 19 | vuln2\_warning\_schema\_posssuperiors |
| 20 | vuln3\_certificates\_vuln |
| 21 | vuln3\_compatible\_2000\_not\_default |
| 22 | vuln3\_dsheuristics\_bad |
| 23 | vuln3\_protected\_users |
| 24 | vuln3\_reversible\_password |
| 25 | vuln3\_sidhistory\_present |
| 26 | vuln4\_dnsadmins |

## Les corrélations ANSSI

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ANSSI | METSYS | PingCastle | PurpleKnight | MITRE ATT&CK |
| 1 |  |  |  |  |
| 2 |  |  |  |  |
| 3 | 16 | 28 | 22 | 7 |
| 4 | 41 | 39 |  | 1 |
| 5 | 11 | 19 | 3, 4, 10, 34, 35 | 1, 4 |
| 6 |  |  |  |  |
| 7 |  |  |  |  |
| 8 | 24 | 24 | 21, 24, 36 | 23 |
| 9 | 1 | 1 | 1 | 1, 13 |
| 10 | 1 | 1 | 1 | 1, 13 |
| 11 | 6 | 4 | 5, 16 | 21 |
| 12 |  |  |  |  |
| 13 | 40 | 29 | 8 | 1 |
| 14 | 11 | 19 | 3, 4, 10, 34, 35 | 1, 4 |
| 15 | 4 | 33 | 32 | 24 |
| 16 | 3 | 10 | 14 | 22 |
| 17 | 11 | 19 | 3, 4, 10, 34, 35 | 1, 4 |
| 18 | 15 | 47 | 27 | 19 |
| 19 | 13 | 32 |  | 2 |
| 20 | 7 | 16, 18 |  | 26 |
| 21 | 39 | 14, 15 | 7 | 12, 16 |
| 22 | 51 | 9 |  | 14 |
| 23 | 33 | 27 | 25 | 3, 4 |
| 24 | 42, 52 | 17, 42 | 31 | 11, 17 |
| 25 | 2 | 43, 48 |  | 13 |
| 26 | 28 | 23 |  | 4, 8 |

## Les références MITRE ATT&CK

|  |  |
| --- | --- |
| Index | Nom |
| 1 | M1015 |
| 2 | M1018 |
| 3 | M1025 |
| 4 | M1026 |
| 5 | M1047 |
| 6 | M1051 |
| 7 | T1003.004 |
| 8 | T1018 |
| 9 | T1069.002 |
| 10 | T1087.001 |
| 11 | T1110.002 |
| 12 | T1110.003 |
| 13 | T1134.005 |
| 14 | T1187 |
| 15 | T1201 |
| 16 | T1210 |
| 17 | T1552 |
| 18 | T1555.005 |
| 19 | T1557 |
| 20 | T1557.001 |
| 21 | T1558 |
| 22 | T1558.001 |
| 23 | T1558.003 |
| 24 | T1558.004 |
| 25 | T1569 |
| 26 | T1600.001 |

## Les corrélations MITRE ATT&CK

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| MITRE ATT&CK | METSYS | PingCastle | PurpleKnight | ANSSI |
| 1 | 1, 10, 11, 14, 17, 18, 40 | 1, 19, 21, 22, 29,  30, 32, 38, 39, 40, 41 | 1, 3, 4, 8, 10, 34, 35 | 4, 5, 10, 13, 14, 17 |
| 2 | 13, 35 | 11, 31, 32 | 6 | 19 |
| 3 | 33 | 27 | 25 | 23 |
| 4 | 11, 28, 30, 33, 53 | 19, 20, 23, 26, 27, 38, 40 | 3, 4, 10, 20, 25, 34, 35 | 5, 14, 17, 23 |
| 5 | 36 | 2 |  |  |
| 6 | 12, 43, 44 | 34, 35, 36, 37, 45, 46 | 9 |  |
| 7 | 16 | 28 | 22 | 3 |
| 8 | 28 | 23 |  |  |
| 9 | 30 | 20 |  |  |
| 10 | 50 | 12 |  |  |
| 11 | 42 | 42 | 31 | 24 |
| 12 | 39 | 14, 15 | 7 | 21 |
| 13 | 1, 2 | 1, 43, 48 | 1 | 10, 25 |
| 14 | 17, 51 | 9, 30 |  | 22 |
| 15 | 9 | 13 |  |  |
| 16 | 39 | 14, 15 | 7 | 21 |
| 17 | 52 | 17 |  | 24 |
| 18 | 35 | 11, 31 | 6 |  |
| 19 | 15, 27, 32, 37, 38 | 3, 5, 6, 7, 47 | 27 | 18 |
| 20 | 31 | 44 |  |  |
| 21 | 6 | 4 | 5, 16 | 11 |
| 22 | 3 | 10 | 14 | 16 |
| 23 | 24 | 24 | 21, 24, 36 | 8 |
| 24 | 4 | 33 | 32 | 15 |
| 25 | 10 | 21 |  |  |
| 26 | 7 | 16, 18 |  | 20 |