| etc./shadow | Terms | legacy protocols B5:128 |
|--|-------------------------|---------------------------------------|
| AADSTS-50055 B5.131 access control conditional B5.147 perms B5.166-72 emittiles B5.70 contributor B5.167 ACE B5.71 covener B5.167 ADDS B5.117 covener B5.167 ADDS B5.117 covener B5.167 ADDS B5.117 covener B5.167 ADDS B5.117 covener B5.167 bypasses B5.22 control B5.159 amsi B45.6-60 data B5.159 bypasses B4.58-60 data B5.159 amsi B4.5-6-60 data B5.159 amsi B4.5-60 amsi B4 | /ota/shadow R3-68 | * - |
| | • | <u> </u> |
| conditional B5:147 | | |
| entities B5.70 contributor B5.167 ACE B5.46 1AM document B5.168 ADCS B5.46 inheritance B5.169 ADDS B5.117 owner B5.169 ADDS B5.117 owner B5.167 admin hunting B1.63 plane ace B5.129 control B5.159 amsi B4.56.60 data B5.159 amsi B4.58.60 recon B5.159 amsi B4.58.60 recon B5.120 amsiscanBuffer B4.57 refresh token B5.159 amsiscanBuffer B4.57 refresh token B5.162 ASNs B1.67 roles B5.167 ASNs B1.67 scope B5.161 ASNs B1.17 scope B5.114 assumed breach B2.68 smart lockout B5.168 attack phases B1.17 synchronization B5.162 covering tracks B1.17 | | - |
| ACE B5.76 IAM document B5.16s ADCS B5.46 inheritance B5.16s ADDS B5.117 owner B5.167 ADFS Extranet Lockout B5.137 reader B5.167 Admin hunting B1.63 plane B5.167 aces B.522 control B5.159 amsi B4.56-60 data B5.159 bypasses B4.56-60 recon B5.120-29 AmsiScanBuffer B4.57 refresh token B5.152-29 AmsiScanBuffer B4.71 roles B5.162-29 application control B4.71 roles B5.162-29 ASNs B1.17 scope B5.116 assumed breach B2.68 smart lockout B5.168 astatack phases B1.17 scope B5.116 ceveloitation B1.17 spocesses admin B5.168 exploitation B1.17 post-exploitation B1.17 recovering tracks B1.17 < | | |
| ADCS B5:169 Inheritance B5:169 ADDS B5:117 owner B5:169 ADFS Extranct Lockout B5:137 reader B5:167 admin hunting B1:63 plane acs B5:22 control B5:159 amsi B4:56-60 data B5:159 bypasses B4:58-60 recon B5:129-29 amsiCanlbuffer B4:57 refresh token B5:152-4 annual reports B1:68 request throttle B5:162-4 aspiplication control B4:71 roles acree throttle B5:162-4 assumed breach B2:68 smart lockout B5:116-8 astek phases synchronization B5:116-8 covering tracks B1:17 synchronization B5:136-166 exploitation B1:17 user access admin B5:166-166 exploitation B1:17 post-exploitation B1:17 user access admin B5:166-166 exploitation B1:17 recon B1:17 recon <td></td> <td></td> | | |
| ADDS | | |
| ADPS Extranet Lockout B5:137 admin hunting reader B5:167 admin hunting acs B5:22 control B5:159 amsi amsi B4:56-60 data B5:159 amsi bypasses B4:56-60 recon B5:102-29 refresh token B5:122-29 refresh token AmsiScanBuffer B4:57 refresh token B5:122-29 refresh token B5:122-29 refresh token AmsiScanBuffer B4:71 roles B5:167 refresh token B5:122-29 refresh token ASNs B1:75 scope B5:167 request throttle B5:167 request throttle ASNs B1:75 scope B5:168 request throttle B5:168 request throttle assumed breach B2:68 smart lockout B5:168 scope B5:166 scope asteck phases B1:17 scope B5:108 smart lockout B5:136 stope attack phases B1:17 scope B5:136 smart lockout B5:136 smart lockout <td></td> <td></td> | | |
| admin hunting B1:63 as plane amsi B4:56-60 data B5:159 AmsiScanBuffer B4:56-60 data B5:159 AmsiScanBuffer B4:57 refresh token B5:152-4 annual reports B1:68 request throttle B5:125-4 amual reports B1:68 request throttle B5:125-4 application control B4:71 roles B5:166 asrep roast B5:104 shell B5:166 asrep roast B5:104 shell B5:108 assumed breach B5:118 assumed breach B5:128 assumed breach B5:149 | | |
| acs B5:22 ams control B5:159 data amsi B4:56-60 bypasses B4:56-60 data B5:159 data bypasses B4:56-60 recon B5:120-29 refresh token B5:120-29 refresh token AmsiScanBuffer B4:57 refresh token B5:120-29 refresh token B5:120-29 refresh token AmsiScanBuffer B4:57 refresh token B5:120-29 refresh token B5:120-29 refresh token ASNs B1:75 scope B5:167 request throttle B5:125 request throttle B5:125 request throttle ASNs B1:75 scope B5:166 request throttle B5:125 request throttle B5:126 request throttle B5:126 request throttle B5:126 request throttle B5:145 request throttle <t< td=""><td></td><td></td></t<> | | |
| amsi B4:56-60 data B5:159 bypasses B4:58-60 recon B5:129-2 AmisScanBuffer B4:57 refresh token B5:152-2 annual reports B1:68 request throttle B5:152-2 application control B4:71 roles B5:167 ASNs B1:75 scope B5:116 assumed breach B2:68 smart lockout B5:136 attack phases B1:17 user access admin B5:136 covering tracks B1:17 user access admin B5:168 exploitation B1:17 user access admin B5:168 exploitation B1:17 backup servers B5:338 post-exploitation B1:17 browser B5:438 post-exploitation B1:17 browser B5:438 attack phases B1:17 browser B5:438 attact phase B1:17 browser B2:49 competitive phase B2:39 2 C:/Windows/Panther B3:15-6 | | |
| Day by a sasses | | |
| AmsiScanBuffer B4.57 refresh token B5:152-4 annual reports B1:68 request throttle B5:125 application control B4:71 roles B5:116 ASNs B1:75 scope B5:116 ASNs B1:17 scope B5:116 assumed breach B2:68 smart lockout B5:136 attack phases B1:17 smart lockout B5:136 covering tracks B1:17 user access admin B5:160 exploitation B1:17 user access admin B5:160 post-exploitation B1:17 user access admin B5:160 post-exploitation B1:17 user enumeration B5:162 post-exploitation B1:17 user enumeration B5:162 asaming B1:17 browser B2:89 covering B1:17 browser B2:49 authenticated proxy B2:89 c2 C:/Windows/Panther B3:15-6 central B5:144 authority B5:46 </td <td></td> <td></td> | | |
| annual reports B1:68 request throttle B5:125 application control B4:71 roles B5:167 ASNs B1:75 scope B5:168 assumed breach B2:68 smart lockout B5:108 astack phases synchronization B5:136 covering tracks B1:17 user access admin B5:166 exploitation B1:17 backup servers B5:33 post-exploitation B1:17 backup servers B5:132 post-exploitation B1:17 backup servers B5:132 post-exploitation B1:17 backup servers B5:138 scanning B1:17 backup servers B5:142 scanning B1:17 browsers B2:33 authenticated proxy B2:89 c2 B2:72 cuthentication C:/Windows/Panther B3:154 central B5:144 central auth server B5:144 FIDO2 B5:144 authoriticate central auth server B5:144 < | v - | |
| application control B4:71 roles B5:167 ASNs B1:75 scope B5:1167 asrep roast B5:104 shell B5:108 assumed breach B2:68 smart lockout B5:136 attack phases B1:17 user access admin B5:136 covering tracks B1:17 user enumeration B5:122-27 maintaining access B1:17 backup servers B5:36 recon B1:17 browser B2:46 scanning B1:17 browsers B2:46 scanning B1:17 browsers B2:46 scanning B1:17 browsers B2:46 scanning B1:17 browsers B2:46 central B5:144 central auth server B3:144 LDAPS B5:144 central auth server B5:144 MFA B5:144 authority B5:68 api gateway B5:18 service B5:68 api gateway B5:19 encollment <td></td> <td></td> | | |
| ASNs B1:75 scope B5:116 assumed breach B2:68 smart lockout B5:136 attack phases B1:17 user access admin B5:138 covering tracks B1:17 user access admin B5:136 exploitation B1:17 user access admin B5:122-27 maintaining access B1:17 backup servers B5:33 post-exploitation B1:17 backup servers B5:33 post-exploitation B1:17 backup servers B5:33 access conning B1:17 browser B2:46 scanning B1:17 browser B2:43 authenticated proxy B2:89 c2 B2:72 authentication C./Windows/Panther B3:15-6 central B5:144 central auth server B5:144 EDAPS B5:144 authority B5:46 authentication B5:13 authority B5:61 api gateway B5:13 service B5:46 auzue acc | | - |
| asrep roast B5:104 shell B5:108 assumed breach B2:68 smart lockout B5:138 attack phases synchronization B5:148 covering tracks B1:17 user access admin B5:168 exploitation B1:17 user enumeration B5:162-227 maintaining access B1:17 backup servers B5:138 recon B1:17 browser B2:49 saming B1:17 browsers B2:46 scanning B1:17 browsers B2:43 authenticated prox B2:89 c2 B2:72 authentication C:/Windows/Panther B3:15-6 central B5:144 central auth server B5:144 LDAPS B5:144 certificate AWS B5:144 certificate autonomous systems numbers B1:75 ernollment B5:46 azure access control B5:111, 117 access control B5:61 AD B5:111, 117 access control | | |
| assumed breach attack phases B2:68 smart lockout B5:136 covering tracks B1:17 user access admin B5:136 exploitation B1:17 user access admin B5:162-227 maintaining access B1:17 backup servers B5:33 post-exploitation B1:17 browser B2:46 scanning B1:17 browser B2:46 scanning B1:17 browser B2:46 scanning B1:17 browser B2:46 scanning B1:17 browser B2:46 browser B2:46 browsers B2:46 browser B2:46 browsers B2:46 central B5:144 certificate certificate LDAPS B5:144 certificate certificate AWS B5:144 internal B5:46 authonity B5:63 service B5:64 azure B5:109, 116 service B5:64 authentication B5:111, 117 < | | |
| Strick phases Synchronization Sich | | |
| covering tracks B1:17 exploitation user access admin user enumeration B5:166 user enumeration B5:166 user enumeration B5:122-27 user enumeration B5:122-27 user enumeration B5:133 user enumeration B5:134 user enumeration B5:135 user enumeration B5:138 user enumeration B5:144 user enumeration B5:155 user entificate B5:161 user enumeration B5:161 user enumeration B5:161 user | | |
| exploitation B1:17 maintaining access B1:17 beckup servers B5:133 post-exploitation B1:17 recon B1:17 browser B1:78 browser B2:48 browsers B2:33 browsers B2:33 browsers B2:33 browsers B2:33 browsers B2:33 browsers B2:33 browsers B2:32 browsers B2:33 browsers B2:33 browsers B2:33 browsers B2:33 browsers B2:33 browsers B2:32 browsers B2:33 browsers B2:32 browsers B2:72 browsers </td <td></td> <td>· ·</td> | | · · |
| maintaining access B1:17 post-exploitation B1:17 BGP B1:78 BCP B1:78 BCP B2:44 BCP B2:44 BCP B2:44 BCP B2:44 BCP B2:45 BCP B2:44 BCP B2:45 BCP B2:45 BCP B2:46 BCP B2:47 BCP B2:47 BCP B2:47 BCP B2:47 BCP B2:47 BCP B2:47 BCP B2:48 BCP B2:144 BCP B2:144 BCP B3:15-64 BCP B3:15-64 BCP B3:15-64 BCP B3:15-64 BCP B3:15-64 BCP B3:144 BCP B3:15-64 BCP B3:144 BCP B3:15-64 BCP B3:145 BCP B3:144 BCP B3:144 BCP B3:144 BCP B3:144 BCP | | |
| post-exploitation B1:17 recon B1:17 browser B2:46 browser B2:46 browser B2:46 browser B2:46 browser B2:46 browser B2:33 authenticated proxy B2:33 authentication C2 M5 B2:33 cc B2:34 cc Cc/Windows/Panther B3:15-6 cettificate Cc Central auth server B5:144 ccertificate Central auth server B5:144 certificate Central auth server B5:144 certificate Central auth server B5 | = | |
| recon B1:17 scanning B1:17 browser B2:46 browsers B2:46 browsers B2:46 browsers B2:46 browsers B2:33 browsers B2:34 browsers B2:33 browsers B2:46 browsers B2:33 browsers B2:33 browsers B2:33 browsers B2:33 browsers B2:46 browsers B2:33 browsers B2:34 browsers B3:15-6 central auth server B3:15-4 central auth server B3:144 certificate B3:144 certificate B3:144 certificate Central auth server B3:144 certificate B3:144 certificate Certificate B3:46 central auth server B3:144 certificate B3:144 certificate Certificate B3:46 central auth server B3:46 central auth server B3:144 certificate Certificate B3:46 central auth server B3: | | |
| scanning B1:17 authenticated proxy B2:89 c2 B2:33 authentication authentication C:/Windows/Panther B3:15-6 central B5:144 central auth server B5:144 certificate LDAPS B5:144 dinternal B5:145 authonity B5:46 authority B5:57 access control B5:57 access control B5:57 access control B5:70 access control B5:71 access control B5:70 access control B5:71 access cont | | |
| authenticated proxy B2:89 c2 B2:72 authentication C:/Windows/Panther B3:15-6 central B5:144 central auth server B5:144 FIDO2 B5:144 certificate authority B5:46 LDAPS B5:144 authority B5:49 autonomous systems numbers B1:75 enrollment B5:49 AWS pfx B5:61 api gateway B5:138 service B5:61 azure signing request B5:64 azure signing request B5:46 azure signing request B5:46 azure signing request B5:66 access control B5:111, 117 access control B5:50-70 auth library B5:162 ESC1 B5:50-70 auth library B5:162 ESC4 B5:71-81 automation B5:163 ESC8 B5:82-3 automation B5:167 ESC8 B5:82-3 blobs B5:157 Exi | | |
| authentication C:/Windows/Panther B3:15-6 central B5:144 central auth server B5:144 FIDO2 B5:144 certificate certificate LDAPS B5:144 authority B5:49 MFA B5:144 internal B5:49 autonomous systems numbers B1:75 enrollment B5:49 AWS pfx B5:61 api gateway B5:138 service B5:61 azure signing request B5:61 access control B5:109, 116 template B5:50 AD B5:111, 117 access control B5:50 auth library B5:162 ESC1 B5:70 auth library B5:162 ESC4 B5:71 automation B5:163 ESC8 B5:82-3 automation B5:163 certificate transparency B1:79 chaining certificate transparency B1:79 chaining B2:80 chaining B3:63 ex | ~ | |
| central B5:144 central auth server B5:144 FIDO2 B5:144 certificate LDAPS B5:144 authority B5:46 MFA B5:144 authority B5:49 autonomous systems numbers B1:75 enrollment B5:49 AWS pfx B5:149 api gateway B5:138 service B5:46 azure signing request B5:46 access control B5:111, 117 access control B5:50 AD B5:111, 117 access control B5:50 AD B5:157 ESC1 B5:50-70 auth library B5:162 ESC4 B5:71-81 authentication B5:118 ESC8 B5:82-3 automation B5:163 certificate transparency B1:79 backup B5:157 chaining B2:0 blobs B5:157 Kerberos B3:99 devops B5:157 LANMAN B3:63 external recon B5:11 | - · · | |
| FIDO2 | | • |
| LDAPS | | |
| MFA B5:144 autonomous systems numbers B1:75 B1:75 B1:75 B1:75 B1:75 B2:82 internal B5:49 B5:49 B5:82 B1:82 AWS pfx B5:61 B5:61 B5:61 B5:66 B5:46 B5:50 B5:46 B5:50 B5:46 B5:50 B5:46 B5:50 B5:46 B5:47 B5:50 B5:46 B5:50 B5:46 B5:47 B5:46 B5:47 B5:46 B5:47 B5:47 B5:46 B5:47 B5:48 B5:47 B5:47 B5:48 B5:47 B5:47 B5:48 B5:47 B5:48 B5:47 B5:48 B5:44 | | |
| autonomous systems numbers B1:75 enrollment B5:82 AWS pfx B5:61 api gateway B5:138 service B5:46 azure signing request B5:46 access control B5:109, 116 template B5:50 AD B5:111, 117 access control B5:70 api manage B5:157 ESC1 B5:50-70 auth library B5:162 ESC4 B5:71-81 authentication B5:111-8 ESC8 B5:82-3 automation B5:163 certificate transparency B1:79 backup B5:157 chaining B2:80 blobs B5:157 Kerberos B3:99 devops B5:157 Kerberos B3:63 extensions B5:163 NTLMv1 B3:63 external recon B5:118 CIDR B1:78 global admin B5:166 cloud shell B5:108 groups cmd.exe autorun B3:40 management | | |
| AWS | | |
| api gateway B5:138 service B5:46 azure signing request B5:46 access control B5:109, 116 template B5:50 AD B5:111, 117 access control B5:70 api manage B5:157 ESC1 B5:50-70 auth library B5:162 ESC4 B5:71-81 authentication B5:111-8 ESC8 B5:82-3 automation B5:163 certificate transparency B1:79 backup B5:157 chaining B2:80 blobs B5:157 challenge-response compute B5:157 Kerberos B3:99 devops B5:157 LANMAN B3:63 extensions B5:163 NTLMv1 B3:63 external recon B5:121 NTLMv2 B3:65-6, 100-01 federation B5:118 CIDR B1:78 global admin B5:166 cloud shell B5:108 management B5:158 common subdomains B1:72 | · · | |
| azure signing request B5:46 access control B5:109, 116 template B5:50 AD B5:111, 117 access control B5:70 api manage B5:157 ESC1 B5:50-70 auth library B5:162 ESC4 B5:71-81 authentication B5:111-8 ESC8 B5:82-3 automation B5:163 certificate transparency B1:79 backup B5:157 chaining B2:80 blobs B5:157 chaining B2:80 blobs B5:157 challenge-response compute B5:157 Kerberos B3:99 devops B5:157 LANMAN B3:63 extensions B5:163 NTLMv1 B3:65-6, 100-01 federation B5:118 CIDR B1:78 global admin B5:166 cloud shell B5:108 groups cmd.exe autorun B3:40 management B5:158 common subdomains B1:72 resource <td></td> <td>-</td> | | - |
| access control B5:109, 116 template B5:50 AD B5:111, 117 access control B5:70 api manage B5:157 ESC1 B5:50-70 auth library B5:162 ESC4 B5:71-81 authentication B5:111-8 ESC8 B5:82-3 automation B5:163 certificate transparency B1:79 backup B5:157 chaining B2:80 blobs B5:157 chailenge-response compute B5:157 Kerberos B3:99 devops B5:157 LANMAN B3:63 external recon B5:163 NTLMv1 B3:63 external recon B5:121 NTLMv2 B3:65-6, 100-01 federation B5:18 CIDR B1:78 global admin B5:166 cloud shell B5:108 groups cmd.exe autorum B3:40 management B5:158 competitive intel B1:68 IAM B5:109 conditional access policies B5:147 <td></td> <td></td> | | |
| AD B5:111, 117 access control B5:70 api manage B5:157 ESC1 B5:50-70 auth library B5:162 ESC4 B5:71-81 authentication B5:111-8 ESC8 B5:82-3 automation B5:163 certificate transparency B1:79 backup B5:157 chaining B2:80 blobs B5:157 chailenge-response compute B5:157 Kerberos B3:99 devops B5:157 LANMAN B3:63 extensions B5:163 NTLMv1 B3:63 external recon B5:121 NTLMv2 B3:65-6, 100-01 federation B5:18 CIDR B1:78 global admin B5:166 cloud shell B5:108 groups cmd.exe autorum B3:40 management B5:158 competitive intel B1:72 resource B5:158 conditional access policies B5:147 identities B5:171 credential guard B3:15-6< | | |
| api manage B5:157 ESC1 B5:50-70 auth library B5:162 ESC4 B5:71-81 authentication B5:111-8 ESC8 B5:82-3 automation B5:163 certificate transparency B1:79 backup B5:157 chaining B2:80 blobs B5:157 challenge-response compute B5:157 Kerberos B3:99 devops B5:157 LANMAN B3:63 extensions B5:163 NTLMv1 B3:63 external recon B5:121 NTLMv2 B3:65-6, 100-01 federation B5:118 CIDR B1:78 global admin B5:166 cloud shell B5:108 groups cmd.exe autorun B3:40 management B5:158 common subdomains B1:72 resource B5:158 competitive intel B1:68 IAM B5:109 conditional access policies B5:147 identities B5:171 credential guard B4:44 <td></td> <td></td> | | |
| auth library B5:162 ESC4 B5:71-81 authentication B5:111-8 ESC8 B5:82-3 automation B5:163 certificate transparency B1:79 backup B5:157 chaining B2:80 blobs B5:157 chaillenge-response compute B5:157 Kerberos B3:99 devops B5:157 LANMAN B3:63 extensions B5:163 NTLMv1 B3:63 external recon B5:121 NTLMv2 B3:65-6, 100-01 federation B5:118 CIDR B1:78 global admin B5:166 cloud shell B5:108 groups cmd.exe autorum B3:40 management B5:158 common subdomains B1:72 resource B5:158 competitive intel B1:68 IAM B5:109 conditional access policies B5:147 identity token B5:171 credential guard B4:44 | · | |
| authentication B5:111-8 ESC8 B5:82-3 automation B5:163 certificate transparency B1:79 backup B5:157 chaining B2:80 blobs B5:157 chaillenge-response compute B5:157 Kerberos B3:99 devops B5:157 LANMAN B3:63 extensions B5:163 NTLMv1 B3:63 external recon B5:121 NTLMv2 B3:65-6, 100-01 federation B5:118 CIDR B1:78 global admin B5:166 cloud shell B5:108 groups cmd.exe autorum B3:40 management B5:158 common subdomains B1:72 resource B5:158 competitive intel B1:68 IAM B5:109 conditional access policies B5:147 identities B5:171 credential guard B4:44 | | |
| automation B5:163 certificate transparency B1:79 backup B5:157 chaining B2:80 blobs B5:157 challenge-response compute B5:157 Kerberos B3:99 devops B5:157 LANMAN B3:63 extensions B5:163 NTLMv1 B3:63 external recon B5:121 NTLMv2 B3:65-6, 100-01 federation B5:118 CIDR B1:78 global admin B5:166 cloud shell B5:108 groups cmd.exe autorun B3:40 management B5:158 common subdomains B1:72 resource B5:158 competitive intel B1:68 IAM B5:109 conditional access policies B5:147 identities B5:171 credential guard B4:44 | | |
| backup B5:157 chaining B2:80 blobs B5:157 challenge-response compute B5:157 Kerberos B3:99 devops B5:157 LANMAN B3:63 extensions B5:163 NTLMv1 B3:63 external recon B5:121 NTLMv2 B3:65-6, 100-01 federation B5:118 CIDR B1:78 global admin B5:166 cloud shell B5:108 groups cmd.exe autorum B3:40 management B5:158 competitive intel B1:68 IAM B5:109 conditional access policies B5:147 identities B5:171 cpassword B3:15-6 identity token B5:171 credential guard B4:44 | | |
| blobs B5:157 challenge-response compute B5:157 Kerberos B3:99 devops B5:157 LANMAN B3:63 extensions B5:163 NTLMv1 B3:63 external recon B5:121 NTLMv2 B3:65-6, 100-01 federation B5:118 CIDR B1:78 global admin B5:166 cloud shell B5:108 groups cmd.exe autorun B3:40 management B5:158 common subdomains B1:72 resource B5:158 competitive intel B1:68 IAM B5:109 conditional access policies B5:147 identities B5:171 cpassword B3:15-6 identity token B5:171 credential guard B4:44 | | - v |
| compute B5:157 Kerberos B3:99 devops B5:157 LANMAN B3:63 extensions B5:163 NTLMv1 B3:63 external recon B5:121 NTLMv2 B3:65-6, 100-01 federation B5:118 CIDR B1:78 global admin B5:166 cloud shell B5:108 groups cmd.exe autorun B3:40 management B5:158 common subdomains B1:72 resource B5:158 competitive intel B1:68 IAM B5:109 conditional access policies B5:147 identities B5:171 cpassword B3:15-6 identity token B5:171 credential guard B4:44 | | O Company |
| devops B5:157 LANMAN B3:63 extensions B5:163 NTLMv1 B3:63 external recon B5:121 NTLMv2 B3:65-6, 100-01 federation B5:118 CIDR B1:78 global admin B5:166 cloud shell B5:108 groups cmd.exe autorun B3:40 management B5:158 common subdomains B1:72 resource B5:158 competitive intel B1:68 IAM B5:109 conditional access policies B5:147 identities B5:171 cpassword B3:15-6 identity token B5:171 credential guard B4:44 | | © 1 |
| extensions B5:163 NTLMv1 B3:63 external recon B5:121 NTLMv2 B3:65-6, 100-01 federation B5:118 CIDR B1:78 global admin B5:166 cloud shell B5:108 groups cmd.exe autorun B3:40 management B5:158 common subdomains B1:72 resource B5:158 competitive intel B1:68 IAM B5:109 conditional access policies B5:147 identities B5:171 cpassword B3:15-6 identity token B5:171 credential guard B4:44 | | |
| external recon B5:121 NTLMv2 B3:65-6, 100-01 federation B5:118 CIDR B1:78 global admin B5:166 cloud shell B5:108 groups cmd.exe autorun B3:40 management B5:158 common subdomains B1:72 resource B5:158 competitive intel B1:68 IAM B5:109 conditional access policies B5:147 identities B5:171 cpassword B3:15-6 identity token B5:171 credential guard B4:44 | | |
| federation B5:118 CIDR B1:78 global admin B5:166 cloud shell B5:108 groups cmd.exe autorun B3:40 management B5:158 common subdomains B1:72 resource B5:158 competitive intel B1:68 IAM B5:109 conditional access policies B5:147 identities B5:171 cpassword B3:15-6 identity token B5:171 credential guard B4:44 | | |
| global admin B5:166 cloud shell B5:108 groups cmd.exe autorun B3:40 management B5:158 common subdomains B1:72 resource B5:158 competitive intel B1:68 IAM B5:109 conditional access policies B5:147 identities B5:171 cpassword B3:15-6 identity token B5:171 credential guard B4:44 | | · · · · · · · · · · · · · · · · · · · |
| $\begin{array}{cccccccccccccccccccccccccccccccccccc$ | | |
| management B5:158 common subdomains B1:72 resource B5:158 competitive intel B1:68 IAM B5:109 conditional access policies B5:147 identities B5:171 cpassword B3:15-6 identity token B5:171 credential guard B4:44 | ~ | |
| resource B5:158 competitive intel B1:68 IAM B5:109 conditional access policies B5:147 identities B5:171 cpassword B3:15-6 identity token B5:171 credential guard B4:44 | | |
| IAM B5:109 conditional access policies B5:147 identities B5:171 cpassword B3:15-6 identity token B5:171 credential guard B4:44 | | |
| identities B5:171 cpassword B3:15-6 identity token B5:171 credential guard B4:44 | | - |
| identity token B5:171 credential guard B4:44 | | |
| 01000011000 00000 00000 00000 00000 00000 00000 0000 | | - |
| minustracture Bo.191 b | infrastructure B5:177-9 | стеченыя диаги В4:44 |

Lischke 1 08/2024

| credential reuse B4:6 | types B2:30 |
|--|----------------------------------|
| credential stuffing B2:9-10 | windows B2:45, 49-51 |
| crypt3 B3:58-66 | extended key usage B5:48 |
| daisy-chaining B2:80 | Extranet Lockout B5:137 |
| data breaches B1:85 | file |
| data dump forums B1:85 | install files B3:15-6 |
| DCShadow B5:40 | iso B2:101 |
| DCSync B5:38 | lnk-shortcuts B2:103 |
| dedicated systems B1:36 | permissions B3:10 |
| dhcpclient B2:131 | pilfering B2:115-6, 132 |
| directory replication service remote B5:39 | searching |
| dirty cow B3:8 | world-writeable B3:10 |
| document-reading apps B2:33 | zip B2:102 |
| documented permission B1:20, 23 | file-transfer B2:109-12 |
| domain | file/print sharing B4:42 |
| admin B5:30, 35, B2:129 | firewall B2:31, B2:131 |
| administration B2:126 | first-class citizen B5:144 |
| cleanup B2:130 | full-knowledge B1:26 |
| controllers plural B5:36 | GetCredentialType B5:123-5 |
| DCShadow B5:40 | global admin B5:166 |
| DCSync B5:38 | golden ticket B5:94-7 |
| groups B2:129 | Google search |
| ntds file B5:33 | grant B5:155 |
| persistence B5:32 | group policy |
| privesc B5:101-4 | objects B3:17 |
| replication B5:38 | preferences |
| skeleton key B5:36 | guardrails B2:35, 80 |
| users B2:127 | hash |
| DRSR B5:39 | formats |
| dynamic code generation B2:77 | LANMAN B3:60, 63 |
| dynamic data exchange B2:100 | MD5 B3:69 |
| env variable B2:124 | NT B3:61 |
| ephemeral shell B1:47 | rounds |
| ESC | HKCU B3:40 |
| 1 B5:50-69 | html application B1:68 |
| 4 B5:71-81 | hybrid auth B5:111 |
| 8 B5:82-3 | identity token B5:171 |
| etypes | IdsLocked B5:136 |
| evasion | imds B5:170 |
| amsi B4:56-60 | impacket |
| application control B4:72-80 | kerberos B4:33 |
| signature detection B4:64 | remote exec B4:35-7 |
| static analysis B4:61 | secretsdump B4:34 |
| tactics B4:52-69 | syntax B4:35 |
| windows defender B4:65 | implant chaining B2:80 |
| event logs | infrastructure recon B1:71-81 |
| DCShadow B5:40 | ingestors B3:30 |
| ID-5137-5141 B5:40 | inheritance B5:169 |
| execution plan B5:134 | initial access B2:6 |
| exploit B1:11 | install from media B5:34 |
| unquoted paths B3:20 | instance metadata service B5:170 |
| exploitation B2:26-8 | intrusion prevention B2:31 |
| client-side | ipsec B2:131 |
| framework B2:41 | jitter B2:72 |
| local privesc B2:38 | job reqs B1:85 |
| payload delivery B2:36 | JSON web token B5:115 |
| server-side B2:31 | junior testers B1:61 |
| social engineering B2:34 | JWT B5:115 |
| | |

Lischke 2 08/2024

| kerberoasting B5:21 | reliability B2:47 |
|--------------------------------|--------------------------------------|
| computer accounts B5:22 | stagers B2:48-50 |
| etypes B5:22 | stages B2:51 |
| service accounts B5:22 | user interfaces B2:43 |
| targets | meterpreter B2:53-60 |
| kerberos B3:99 | modules B2:60 |
| asrep roast B5:104 | microsoft |
| asreq/asrep B5:8 | ADDS B5:117 |
| auth B5:6 | authentication B5:116 |
| golden ticket94-7 | MSAL B5:162 |
| impacket B4:33 | msbuild B4:74-80 |
| kdc B5:5-7 | MSOL B5:146 |
| kerberoasting B5:11 | NBT-NS |
| krbtgt account B5:30, 87-8, 94 | network sweep |
| long-term keys B5:8, 88 | ntds file |
| overpass-the-hash B5:29 | ntds.dit |
| pass-the-ticket | ntlm |
| priv attribute cert B5:10 | relay |
| service ticket B5:11, 13-6 | NTLMv1 B3:64 |
| silver ticket | NTLMv2 B3:65-6, 100 |
| spn B5:12, 18 | attacks |
| stateless | defense |
| tgsreq/tgsrep B5:11 | NtProtectVirtualMemory |
| 0 1 0 1 | OAuth Token B5:131 |
| ticket reuse | Oauth2 |
| ticket-granting ticket B5:10 | |
| kernel B3:8 | access token |
| kernel attacks | claims B5:150 |
| keyrings B2:122 | code flow B5:144-54 |
| LDAP | flow types B5:155 |
| legacy authen B5:128 | JWT B5:149 |
| linux | refresh token B5:152-4 |
| connections B1:51 | OAuthToken B5:126-7 |
| filesystem | obfuscation |
| permissions B1:50 | office |
| suid | dde B2:100 |
| LLMNR B3:106 | macros |
| load balancing B5:138 | OIDC B5:107 |
| local groups B2:128 | OpenID |
| lockout B2:15 | access token B5:149, 152 |
| duration | claims |
| observation window B2:16 | Connect B5:144, 166 |
| threshold B2:16 | JWT B5:149 |
| login.microsoftonline B5:146 | refresh token B5:152-4 |
| logon script B2:127 | opsec B2:89 |
| LSASS B4:41, 77, B5:103 | organizational recon B1:67-9 |
| managed identity | os fingerprinting B1:94 |
| system assigned B5:171 | nmap B1:129 |
| user assigned B5:171 | PAC B5:10, 13, 88 |
| mangling B3:51 | parallel scans B1:121 |
| mDNS B3:106 | parent process spoofing B2:80 |
| memory dumps B5:103 | pass-the-hash B4:41-9, B3:54 |
| mergers & acquisitions B1:67 | mitigations B4:44 |
| metasploit | pass-through auth B5:118 |
| exploits | password |
| meterpreter | guessing B2:11-22 |
| modules B2:44 | spraying B2:18 |
| payloads | password attacks B4:47 |
| psexec B4:46 | password hash synchronization B5:118 |
| | |

Lischke 3 08/2024

| passwords | local B2:38 |
|--------------------------------|------------------------------------|
| cloud hardware B3:53 | motivations B3:5 |
| dictionaries B3:50 | windows |
| in linux B3:58-66 | alwaysinstallelevated B3:14 |
| in windows B3:58-66 | dll hijacking B3:14 |
| keystroke B3:54 | group policy preferences B3:17-8 |
| mangling B3:51 | unattended install files B3:15-6 |
| reporting B3:56 | unquoted paths B3:20 |
| salt B3:61 | writable service executables B3:14 |
| sniffing B3:54, 100-01 | privileged process B2:39 |
| synced B3:49 | process dumps B5:103 |
| payload delivery B2:36 | proof key code exchange B5:155 |
| payloads B2:97 | proxies |
| PCI B1:61 | http B5:140 |
| penetration test | ssh B5:139 |
| definition B1:15 | psexec B2:45 |
| types B1:16 | purple team B1:13 |
| permissions B1:50 | race conditions B2:39 |
| persistence | rc4 B5:22, 36 |
| cmd.exe autorun B3:40 | recon |
| domain/AD B5:32 | ethics B1:64 |
| HKCU B3:40 | infrastructure B1:71-81 |
| scheduled task B3:42 | internal PCI B1:61 |
| services B3:43 | light-touch B1:62 |
| startup folder B3:41 | organizational B1:67-9 |
| WMI events B3:43 | user B1:82-9 |
| pfx B5:61 | zero-touch B1:62 |
| pgp B2:122 | red team B1:13 |
| phishing | refresh token B5:152-4 |
| device code flow B5:162 | regional internet registries B1:78 |
| pivoting | registry B2:133 |
| linux | registry keys B3:40 |
| ssh B4:87-8 | reporting B4:94-119 |
| windows B4:9-28 | format B4:96 |
| PKCE B5:155 | representative sample B2:37 |
| PKI B5:46 | rid 512 B5:30 |
| plugins B1:149 | RIRs B1:78 |
| polling interval B2:72 | risk B1:12 |
| port forwarding B4:5 | rules of engagement B1:24 |
| port scan B1:94 | runtime env B2:33 |
| post-exploitation B2:108 | SAM database B4:41, B3:58, 75 |
| powershell | sam database |
| obfuscation | scada B2:46 |
| pre-engagement | ScanContent B4:57 |
| goals B1:22 | scans |
| rules | asynchronous B1:96 |
| scope B1:23 | efficiency B1:96 |
| press releases B1:68 | parallel B1:121 |
| primary refresh token B5:152-4 | stateless B1:122 |
| priv attribute cert B5:10 | tcp B1:103-4, 115-6, 122 |
| privacy regulations B1:27 | types B1:94 |
| privesc | udp B1:106-7, 117 |
| domain B5:101-4 | ultrafast B1:122 |
| linux | vulnerability B1:145-51 |
| files B3:10 | SCCM B5:163 |
| kernel B3:8 | scf file |
| service B3:9 | scheduled tasks B3:42 |
| suid B3:11 | scope B1:23 |
| | |

| security audit B1:14 |
|--|
| security identifiers B4:44 |
| sensitive data |
| services |
| |
| controller B4:14 |
| name B4:16 |
| shared object B3:9 |
| shells |
| ephemeral B1:47 |
| prompts B1:55 |
| silver ticket B5:89-90 |
| singles |
| 8 44 |
| situational awareness |
| linux B2:118-22 |
| skeleton key B5:36 |
| smart cards B3:67 |
| smb B4:13, B2:46 |
| named pipes B2:80 |
| smb relaying B3:111 |
| smb signing B3:113 |
| source anchor B5:118 |
| |
| SPN B5:12, 18 |
| SPNs B3:99 |
| ssh |
| key theft B4:6 |
| port forwarding B4:87-8 |
| stagers B2:48 |
| stages B2:48 |
| startup folder B3:41 |
| |
| 91.59 |
| sudo |
| suid B3:11, B2:39, B1:51, 120 |
| $\begin{array}{llllllllllllllllllllllllllllllllllll$ |
| suid B3:11, B2:39, B1:51, 120 SYSTEM registry B5:33 sysvol B2:127 |
| suid B3:11, B2:39, B1:51, 120 SYSTEM registry B5:33 sysvol B2:127 tactics B2:108 |
| suid B3:11, B2:39, B1:51, 120 SYSTEM registry B5:33 sysvol B2:127 |
| suid B3:11, B2:39, B1:51, 120 SYSTEM registry B5:33 sysvol B2:127 tactics B2:108 |
| suid B3:11, B2:39, B1:51, 120 SYSTEM registry B5:33 sysvol B2:127 tactics B2:108 tcp B1:99-102 pivots B2:80 |
| suid B3:11, B2:39, B1:51, 120 SYSTEM registry B5:33 sysvol B2:127 tactics B2:108 tcp B1:99-102 pivots B2:80 RST B1:122 |
| suid B3:11, B2:39, B1:51, 120 SYSTEM registry B5:33 sysvol B2:127 tactics B2:108 tcp B1:99-102 pivots B2:80 RST B1:122 terraform automation B5:155 |
| suid B3:11, B2:39, B1:51, 120 SYSTEM registry B5:33 sysvol B2:127 tactics B2:108 tcp B1:99-102 pivots B2:80 RST B1:122 terraform automation B5:155 test types |
| suid B3:11, B2:39, B1:51, 120 SYSTEM registry B5:33 sysvol B2:127 tactics B2:108 tcp B1:99-102 pivots B2:80 RST B1:122 terraform automation B5:155 test types B1:26 full-knowledge B1:26 |
| suid B3:11, B2:39, B1:51, 120 SYSTEM registry B5:33 sysvol B2:127 tactics B2:108 tcp B1:99-102 pivots B2:80 RST B1:122 terraform automation B5:155 test types B1:26 unannounced B1:25 |
| suid B3:11, B2:39, B1:51, 120 SYSTEM registry B5:33 sysvol B2:127 tactics B2:108 tcp B1:99-102 pivots B2:80 RST B1:122 terraform automation B5:155 test types Full-knowledge B1:26 unannounced B1:25 zero-knowledge B1:26 |
| suid B3:11, B2:39, B1:51, 120 SYSTEM registry B5:33 sysvol B2:127 tactics B2:108 tcp B1:99-102 pivots B2:80 RST B1:122 terraform automation B5:155 test types Full-knowledge B1:26 unannounced B1:25 zero-knowledge B1:26 threat B1:12 |
| suid B3:11, B2:39, B1:51, 120 SYSTEM registry B5:33 sysvol B2:127 tactics B2:108 tcp B1:99-102 pivots B2:80 RST B1:122 terraform automation B5:155 test types B1:26 unannounced B1:25 zero-knowledge B1:26 threat B1:12 TLS B1:79 |
| suid B3:11, B2:39, B1:51, 120 SYSTEM registry B5:33 sysvol B2:127 tactics B2:108 tcp B1:99-102 pivots B2:80 RST B1:122 terraform automation B5:155 test types Full-knowledge B1:26 unannounced B1:25 zero-knowledge B1:26 threat B1:12 |
| suid B3:11, B2:39, B1:51, 120 SYSTEM registry B5:33 sysvol B2:127 tactics B2:108 tcp B1:99-102 pivots B2:80 RST B1:122 terraform automation B5:155 test types B1:26 unannounced B1:25 zero-knowledge B1:26 threat B1:12 TLS B1:79 |
| suid B3:11, B2:39, B1:51, 120 SYSTEM registry B5:33 sysvol B2:127 tactics B2:108 tcp B1:99-102 pivots B2:80 RST B1:122 terraform automation B5:155 test types B1:26 unannounced B1:25 zero-knowledge B1:26 threat B1:12 TLS B1:79 torrents B1:85 tunnels B5:176 |
| suid B3:11, B2:39, B1:51, 120 SYSTEM registry B5:33 sysvol B2:127 tactics B2:108 tcp B1:99-102 pivots B2:80 RST B1:122 terraform automation B5:155 test types B1:26 unannounced B1:25 zero-knowledge B1:26 threat B1:12 TLS B1:79 torrents B1:85 tunnels B5:176 UAC B4:44 |
| suid B3:11, B2:39, B1:51, 120 SYSTEM registry B5:33 sysvol B2:127 tactics B2:108 tcp B1:99-102 pivots B2:80 RST B1:122 terraform automation B5:155 test types full-knowledge B1:26 unannounced B1:25 zero-knowledge B1:26 threat B1:12 TLS B1:79 torrents B1:85 tunnels B5:176 UAC B4:44 udp B1:105 |
| suid B3:11, B2:39, B1:51, 120 SYSTEM registry B5:33 sysvol B2:127 tactics B2:108 tcp B1:99-102 pivots B2:80 RST B1:122 terraform automation B5:155 test types B1:26 unannounced B1:25 zero-knowledge B1:26 threat B1:12 TLS B1:79 torrents B1:85 tunnels B5:176 UAC B4:44 udp B1:105 unannounced test B1:25 |
| suid B3:11, B2:39, B1:51, 120 SYSTEM registry B5:33 sysvol B2:127 tactics B2:108 tcp B1:99-102 pivots B2:80 RST B1:122 terraform automation B5:155 test types B1:26 unannounced B1:25 zero-knowledge B1:26 threat B1:12 TLS B1:79 torrents B1:85 tunnels B5:176 UAC B4:44 udp B1:105 unannounced test B1:25 unattend.xml B3:15-6 |
| suid B3:11, B2:39, B1:51, 120 SYSTEM registry B5:33 sysvol B2:127 tactics B2:108 tcp B1:99-102 pivots B2:80 RST B1:122 terraform automation B5:155 test types B1:26 unannounced B1:25 zero-knowledge B1:26 threat B1:12 TLS B1:79 torrents B1:85 tunnels B5:176 UAC B4:44 udp B1:105 unannounced test B1:25 unattend.xml B3:15-6 unquoted paths B3:20 |
| suid B3:11, B2:39, B1:51, 120 SYSTEM registry B5:33 sysvol B2:127 tactics B2:108 tcp B1:99-102 pivots B2:80 RST B1:122 terraform automation B5:155 test types B1:26 unannounced B1:25 zero-knowledge B1:26 threat B1:12 TLS B1:79 torrents B1:85 tunnels B5:176 UAC B4:44 udp B1:105 unannounced test B1:25 unattend.xml B3:15-6 unquoted paths B3:20 UPN B5:114 |
| suid B3:11, B2:39, B1:51, 120 SYSTEM registry B5:33 sysvol B2:127 tactics B2:108 tcp B1:99-102 pivots B2:80 RST B1:122 terraform automation B5:155 test types full-knowledge full-knowledge B1:26 unannounced B1:25 zero-knowledge B1:26 threat B1:25 torrents B1:79 torrents B1:85 tunnels B5:176 UAC B4:44 udp B1:105 unannounced test B1:25 unattend.xml B3:15-6 unquoted paths B3:20 UPN B5:114 user access admin B5:166 |
| suid B3:11, B2:39, B1:51, 120 SYSTEM registry B5:33 sysvol B2:127 tactics B2:108 tcp B1:99-102 pivots B2:80 RST B1:122 terraform automation B5:155 test types full-knowledge full-knowledge B1:26 unannounced B1:25 zero-knowledge B1:26 threat B1:12 TLS B1:79 torrents B1:85 tunnels B5:176 UAC B4:44 udp B1:105 unannounced test B1:25 unattend.xml B3:15-6 unquoted paths B3:20 UPN B5:114 user access admin B5:166 user account control B3:21-2 |
| suid B3:11, B2:39, B1:51, 120 SYSTEM registry B5:33 sysvol B2:127 tactics B2:108 tcp B1:99-102 pivots B2:80 RST B1:122 terraform automation B5:155 test types full-knowledge B1:26 unannounced B1:25 zero-knowledge B1:26 threat B1:12 TLS B1:79 torrents B1:85 tunnels B5:176 UAC B4:44 udp B1:105 unannounced test B1:25 unattend.xml B3:15-6 unquoted paths B3:20 UPN B5:114 user access admin B5:166 user account control B3:21-2 bypass B3:23 |
| suid B3:11, B2:39, B1:51, 120 SYSTEM registry B5:33 sysvol B2:127 tactics B2:108 tcp B1:99-102 pivots B2:80 RST B1:122 terraform automation B5:155 test types full-knowledge full-knowledge B1:26 unannounced B1:25 zero-knowledge B1:26 threat B1:12 TLS B1:79 torrents B1:85 tunnels B5:176 UAC B4:44 udp B1:105 unannounced test B1:25 unattend.xml B3:15-6 unquoted paths B3:20 UPN B5:114 user access admin B5:166 user account control B3:21-2 |
| suid B3:11, B2:39, B1:51, 120 SYSTEM registry B5:33 sysvol B2:127 tactics B2:108 tcp B1:99-102 pivots B2:80 RST B1:122 terraform automation B5:155 test types full-knowledge B1:26 unannounced B1:25 zero-knowledge B1:26 threat B1:12 TLS B1:79 torrents B1:85 tunnels B5:176 UAC B4:44 udp B1:105 unannounced test B1:25 unattend.xml B3:15-6 unquoted paths B3:20 UPN B5:114 user access admin B5:166 user account control B3:21-2 bypass B3:23 |

| vba B2:98 |
|---|
| version scan B1:94 |
| VLANs B3:113 |
| Volume Shadow Copy Service B5:33, B3:74 |
| VSS B5:33, B3:74 |
| vuln scanning B1:145-5 |
| agent-based B1:148 |
| authenticated B1:148 |
| plugins B1:149 |
| unauthenticated B1:148 |
| vulnerability B1:11 |
| vulnerability assessment B1:14 |
| vulnerability scan B1:94 |
| web proxy auto discovery B3:108 |
| whois B1:78 |
| windows |
| exploit obfuscation B2:13 |
| file/print sharing B4:42 |
| files B2:132 |
| firewall B2:133 |
| passwords B3:58-66, 72-7 |
| registry B2:133 |
| WinInet InternetQueryOption B3:108 |
| WinRM B4:10-11 |
| wlan B2:133 |
| WMI |
| event subscription B3:44 |
| world-writeable B1:53 |
| WPAD B3:108 |
| X509 B5:117 |
| zero-knowledge B1:20 |

| ols/Commands | DeHashed B1:85 |
|-----------------------------------|--|
| Get-Credential B4:11 | DNSDumpster B1:75-7 |
| Test-WSMan B4:11 | DNSRecon B1:73-4 |
| arp | Dradis Reporting B1:40 |
| base64 | Empire B3:23, B2:88-92 |
| bitsadmin B3:26 | modules |
| cscript | Ews-Crack |
| dir B2:124 | ExploitDB B1:33 |
| findstr B2:124 | EyeWitness B1:140- |
| | GatherContacts |
| find B3:12, B2:132 | GetFFGP |
| ip | |
| lsof connections B1:53 | FineGrainedPassPolicy B2:18 GetUserSPN B5:20 |
| more | |
| msbuild.exe | GhostPack B2:137-9 |
| net.exe B4:13, B2:16 | GTFOBins |
| net/net1 B2:126-30 | Hashcat B5:22, B3:89-94 |
| netsh B2:131 | HaveIBeenPwned B1:85 |
| netstat connections B1:53, B2:116 | Hunter.io B1:85 |
| ntdsutil.exe B5:34, B3:76 | Hydra B2:20-2 |
| ps B3:9 | Immunity CANVAS B2:39 |
| reg B2:133 | Impacket B4:32-7 |
| schtasks B4:21, B3:42 | golden ticket B5:97 |
| sc B4:14, 23 | silver ticket B5:89-90 |
| services.msc B4:16 | smbexec/wmiexec B4:37 |
| setspn.exe B5:12, 19 | Invoke-Kerberoast B5:20 |
| set B2:124 | Iptables |
| ss B2:116 | JohnTheRipper B3:83-6 |
| type B2:132 | conf file B3:82 |
| uname B3:8 | potfile B3:83 |
| uniq B3:50 | unshadow B3:71 |
| unshadow B3:71 | jwt.ms |
| winrs B4:10 | L0phtCrack B3:59 |
| wmic B4:25-6 | LinPEAS B2:39 |
| AAD-Internals | LinuxExploitSuggester B2:39 |
| AD Explorer B2:135 | LockoutStatus.exe B2:15 |
| ADCSPwn B5:83 | LOLBAS B3:26 |
| ALockout.dll B2:15 | MailSniper B5:128 |
| AWS API Gateway B5:138-40 | Masscan B1:96, 123-5 |
| Azure CLI B5:162-4 | Metasploit B2:19, B3:23, 42-60 |
| Run-Command B5:164 | owalogin B5:128 |
| BeRoot B3:24 | pivoting B4:84 |
| BloodHound B3:30-5 | psexec B4:46 |
| Burp | Meterpreter B2:53-60 |
| IP Rotate B5:140 | credsall B3:77 |
| C2 Matrix | hashdump B3:75 |
| Cain B3:102 | load kiwi B3:7' |
| | pivoting |
| Certify ESC1 D5.57.61 | Mimikatz B5:27-8, B3:7' |
| ESC1 B5:57-61 | DCShadow B5.27-6, B5.7 DCShadow B5.41 |
| ESC4 B5:73-4 | |
| Certipy | DCSync B5:39 |
| ESC1 B5:65-9 | golden ticket B5:9' |
| ESC4 B5:75-81 | skeleton key B5:3' |
| CeWL B3:51 | MITRE ATTACK B1:38 |
| Chameleon B2:134 | MITRE CVE B1:3' |
| Cobalt Strike B2:39 | Monster.com |
| Core IMPACT B2:36 | MSBuild B4:72-9 |
| crt.sh B1:79 | MSOLSpray B5:131 |
| DefenderCheck B4:65 | NCrack B2:19 |

Lischke 6 08/2024

| Netcat B4:5, B1:133-8 | Rubeus B4:12, B5:27, 61 |
|-------------------------------|-------------------------------|
| ngrok B5:175-8 | ESC1 B5:62-4 |
| nmap B4:10, B1:109-21, 129-33 | ScanRand B1:96 |
| limitations B1:121, 151 | schtasksabuse B3:42 |
| os fingerprinting B1:129 | Seatbelt B2:137-9 |
| script.db B1:156 | secretsdump.py B5:33, B3:59 |
| scripting engine B1:153-6 | SharpBlock B4:63 |
| NPK B3:53 | Shodan B1:80-1 |
| NTDSUtil | SkullSecurity Passwords B3:50 |
| ntlmrelayx.py B5:83 | Sliver B2:76-83 |
| Patator | commands |
| Pcredz | payloads B2:79-80, 83 |
| phonebook.cz B1:84 | server-client B2:82 |
| Pipal B3:95 | Spray365 |
| Posh-SecMod | load balance |
| PowerBreach B2:90 | TrevorSpray B5:132 |
| PowerSploit B2:90, 134 | load balance139 |
| Out-MiniDump B5:103 | UACME B3:23 |
| Remove-Comment B4:62 | VeilEvasion B4:53, 69 |
| PowerStripper B4:62 | Verizon DBIR B2:69 |
| PowerUp B3:25, B2:90 | VirtualProtect |
| PowerView B2:90, 134 | VirusTotal |
| domain privesc B5:101-2 | VSSAdmin B4:34 |
| PsExec B4:18-20 | VSSOwn B3:74 |
| pw-inspector B2:13 | Watson |
| Responder B3:106-13 | WMIC |
| RIRs B1:78 | |

Lischke 7 08/2024