Nessus!

Klasyfikacja luk

**Host: 192.168.64.1**

**Wykryte Luki:**

|  |  |
| --- | --- |
| **1** | **SSL Certificate Cannot Be Trusted** |
| **2** | **SSL Self-Signed Certificate** |
| **3** | **DNS Server Cache Snooping Remote Information Disclosure** |

**Host: 192.168.64.2**

**Wykryte Luki:**

|  |  |
| --- | --- |
| **1** | **SSL Certificate Cannot Be Trusted** |
| **2** | **SSL Self-Signed Certificate** |
| **3** | **SSL Certificate Signed Using Weak Hashing Algorithm** |
| **4** | **SSL Medium Strength Cipher Suites Supported (SWEET32)** |
| **5** | **SSL Weak Cipher Suites Supported** |
| **6** | **SSL RC4 Cipher Suites Supported (Bar Mitzvah)** |

**Host: 192.168.64.3**

**Wykryte Luki:**



**Host: 192.168.64.4**

**Wykryte Luki:**

|  |  |
| --- | --- |
| **1** | **SSL Certificate Cannot Be Trusted** |
| **2** | **SMB Signing not required** |
| **3** | **SSL Certificate Signed Using Weak Hashing Algorithm** |
| **4** | **SSL Certificate with Wrong Hostname** |
| **5** | **SSL Medium Strength Cipher Suites Supported (SWEET32)** |
| **6** | **SSL Certificate Chain Contains RSA Keys Less Than 2048 bits** |

**Host: 192.168.64.5**

**Wykryte Luki:**



**Host: 192.168.64.6**

**Wykryte Luki:**



**Host: 192.168.64.7**

**Wykryte Luki:**



**Host: 192.168.64.8**

**Wykryte Luki:**

|  |  |
| --- | --- |
| **1** | **SNMP Agent Default Community Name (public)** |
| **2** | **Unencrypted Telnet Server** |
| **3** | **SNMP 'GETBULK' Reflection DDoS** |
| **4** | **SSH Server CBC Mode Ciphers Enabled** |
| **5** | **SSH Weak MAC Algorithms Enabled** |

**Host: 192.168.64.11**

**Wykryte Luki:**

|  |  |
| --- | --- |
| **1** | **SNMP Agent Default Community Name (public)** |
| **2** | **Unencrypted Telnet Server** |
| **3** | **SNMP 'GETBULK' Reflection DDoS** |

**Host: 192.168.64.19**

**Wykryte Luki:**

|  |  |
| --- | --- |
| **1** | **NFS Exported Share Information Disclosure** |
| **2** | **SSL Certificate Cannot Be Trusted** |
| **3** | **SSL Self-Signed Certificate** |
| **4** | **SMB Signing not required** |
| **5** | **SSL Certificate Signed Using Weak Hashing Algorithm** |
| **6** | **SSL Certificate with Wrong Hostname** |
| **7** | **SSL Medium Strength Cipher Suites Supported (SWEET32)** |
| **8** | **SSL RC4 Cipher Suites Supported (Bar Mitzvah)** |
| **9** | **SSL Certificate Chain Contains RSA Keys Less Than 2048 bits** |

**Host: 192.168.64.20**

**Wykryte Luki:**



**Host: 192.168.64.21**

**Wykryte Luki:**

|  |  |
| --- | --- |
| **1** | **SNMP Agent Default Community Name (public)** |
| **2** | **rlogin Service Detection** |
| **3** | **Unencrypted Telnet Server** |
| **4** | **SNMP 'GETBULK' Reflection DDoS** |

**Host: 192.168.64.22**

**Wykryte Luki:**

|  |  |
| --- | --- |
| **1** | **SNMP Agent Default Community Name (public)** |
| **2** | **rlogin Service Detection** |
| **3** | **Unencrypted Telnet Server** |
| **4** | **SNMP 'GETBULK' Reflection DDoS** |

**Host: 192.168.64.23**

**Wykryte Luki:**



**Host: 192.168.64.24**

**Wykryte Luki:**

|  |  |
| --- | --- |
| **1** | **SNMP Agent Default Community Name (public)** |
| **2** | **rlogin Service Detection** |
| **3** | **Unencrypted Telnet Server** |
| **4** | **SNMP 'GETBULK' Reflection DDoS** |

**Host: 192.168.64.25**

**Wykryte Luki:**

|  |  |
| --- | --- |
| **1** | **Web Server Generic Cookie Injection** |

**Host: 192.168.64.30**

**Wykryte Luki:**

|  |  |
| --- | --- |
| **1** | **SSL Version 2 and 3 Protocol Detection** |
| **2** | **SSL Certificate Cannot Be Trusted** |
| **3** | **SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection** |
| **4** | **Unencrypted Telnet Server** |
| **5** | **SSL Certificate Expiry** |
| **6** | **SSL Medium Strength Cipher Suites Supported (SWEET32)** |
| **7** | **SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)** |
| **8** | **SSL Weak Cipher Suites Supported** |
| **9** | **SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)** |
| **10** | **SSL RC4 Cipher Suites Supported (Bar Mitzvah)** |
| **11** | **SSL Certificate Chain Contains RSA Keys Less Than 2048 bits** |

**Host: 192.168.64.31**

**Wykryte Luki:**

|  |  |
| --- | --- |
| **1** | **Web Server Directory Traversal Arbitrary File Access** |
| **2** | **Unencrypted Telnet Server** |

**Host: 192.168.64.32**

**Wykryte Luki:**

|  |  |
| --- | --- |
| **1** | **Unencrypted Telnet Server** |

**Host: 192.168.64.35**

**Wykryte Luki:**

|  |  |
| --- | --- |
| **1** | **MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)** |
| **2** | **Microsoft Windows SMBv1 Multiple Vulnerabilities** |
| **3** | **MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)** |
| **4** | **SMB Signing not required** |

**Host: 192.168.64.37**

**Wykryte Luki:**

|  |  |
| --- | --- |
| **1** | **MS05-027: Vulnerability in SMB Could Allow Remote Code Execution (896422) (uncredentialed check)** |
| **2** | **MS05-046: Vulnerability in the Client Service for NetWare Could Allow Remote Code Execution (899589) (uncredentialed check)** |
| **3** | **MS06-040: Vulnerability in Server Service Could Allow Remote Code Execution (921883) (uncredentialed check)** |
| **4** | **MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644) (ECLIPSEDWING) (uncredentialed check)** |
| **5** | **MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687) (uncredentialed check)** |
| **6** | **MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)** |
| **7** | **Microsoft IIS 6.0 Unsupported Version Detection** |
| **8** | **Microsoft Windows XP Unsupported Installation Detection** |
| **9** | **Unsupported Windows OS (remote)** |
| **10** | **MS06-035: Vulnerability in Server Service Could Allow Remote Code Execution (917159) (uncredentialed check)** |
| **11** | **SNMP Agent Default Community Name (public)** |
| **12** | **Unsupported Web Server Detection** |
| **13** | **SSL Version 2 and 3 Protocol Detection** |
| **14** | **SSL Certificate Cannot Be Trusted** |
| **15** | **SSL Self-Signed Certificate** |
| **16** | **Unencrypted Telnet Server** |
| **17** | **HTTP TRACE / TRACK Methods Allowed** |
| **18** | **MS10-024: Vulnerabilities in Microsoft Exchange and Windows SMTP Service Could Allow Denial of Service (981832) (uncredentialed check)** |
| **19** | **Microsoft Windows SMB NULL Session Authentication** |
| **20** | **SMB Signing not required** |
| **21** | **SSL Certificate Signed Using Weak Hashing Algorithm** |
| **22** | **SSL Certificate with Wrong Hostname** |
| **23** | **SSL Medium Strength Cipher Suites Supported (SWEET32)** |
| **24** | **SSL Weak Cipher Suites Supported** |
| **25** | **SSL/TLS EXPORT\_RSA &lt;= 512-bit Cipher Suites Supported (FREAK)** |
| **26** | **SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)** |
| **27** | **TLS Padding Oracle Information Disclosure Vulnerability (TLS POODLE)** |
| **28** | **SSL RC4 Cipher Suites Supported (Bar Mitzvah)** |
| **29** | **SSL Certificate Chain Contains RSA Keys Less Than 2048 bits** |

**Host: 192.168.64.38**

**Wykryte Luki:**

|  |  |
| --- | --- |
| **1** | **MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644) (ECLIPSEDWING) (uncredentialed check)** |
| **2** | **MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687) (uncredentialed check)** |
| **3** | **MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)** |
| **4** | **Microsoft IIS 6.0 Unsupported Version Detection** |
| **5** | **Microsoft Windows XP Unsupported Installation Detection** |
| **6** | **Unsupported Windows OS (remote)** |
| **7** | **MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check)** |
| **8** | **SNMP Agent Default Community Name (public)** |
| **9** | **Unsupported Web Server Detection** |
| **10** | **Unencrypted Telnet Server** |
| **11** | **Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness** |
| **12** | **HTTP TRACE / TRACK Methods Allowed** |
| **13** | **MS10-024: Vulnerabilities in Microsoft Exchange and Windows SMTP Service Could Allow Denial of Service (981832) (uncredentialed check)** |
| **14** | **Microsoft Windows SMB NULL Session Authentication** |
| **15** | **Terminal Services Encryption Level is Medium or Low** |
| **16** | **Terminal Services Encryption Level is not FIPS-140 Compliant** |

**Host: 192.168.64.39**

**Wykryte Luki:**

|  |  |
| --- | --- |
| **1** | **SMB Signing not required** |

**Host: 192.168.64.41**

**Wykryte Luki:**

|  |  |
| --- | --- |
| **1** | **Multiple Ethernet Driver Frame Padding Information Disclosure (Etherleak)** |

**Host: 192.168.64.42**

**Wykryte Luki:**

|  |  |
| --- | --- |
| **1** | **Multiple Ethernet Driver Frame Padding Information Disclosure (Etherleak)** |

**Host: 192.168.64.43**

**Wykryte Luki:**

|  |  |
| --- | --- |
| **1** | **Multiple Ethernet Driver Frame Padding Information Disclosure (Etherleak)** |

**Host: 192.168.64.44**

**Wykryte Luki:**

|  |  |
| --- | --- |
| **1** | **Multiple Ethernet Driver Frame Padding Information Disclosure (Etherleak)** |

**Host: 192.168.64.45**

**Wykryte Luki:**

|  |  |
| --- | --- |
| **1** | **Unix Operating System Unsupported Version Detection** |
| **2** | **SSH Weak Algorithms Supported** |
| **3** | **SSH Server CBC Mode Ciphers Enabled** |
| **4** | **SSH Weak MAC Algorithms Enabled** |

**Host: 192.168.64.46**

**Wykryte Luki:**

|  |  |
| --- | --- |
| **1** | **MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)** |
| **2** | **MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)** |
| **3** | **SSL Version 2 and 3 Protocol Detection** |
| **4** | **MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)** |
| **5** | **SSL Certificate Cannot Be Trusted** |
| **6** | **SSL Self-Signed Certificate** |
| **7** | **SMB Signing not required** |
| **8** | **SSL Certificate Signed Using Weak Hashing Algorithm** |
| **9** | **SSL Certificate with Wrong Hostname** |
| **10** | **SSL Medium Strength Cipher Suites Supported (SWEET32)** |
| **11** | **SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)** |
| **12** | **TLS Padding Oracle Information Disclosure Vulnerability (TLS POODLE)** |
| **13** | **SSL RC4 Cipher Suites Supported (Bar Mitzvah)** |
| **14** | **SSL Certificate Chain Contains RSA Keys Less Than 2048 bits** |

**Host: 192.168.64.48**

**Wykryte Luki:**

|  |  |
| --- | --- |
| **1** | **MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687) (uncredentialed check)** |
| **2** | **MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)** |
| **3** | **Microsoft Windows XP Unsupported Installation Detection** |
| **4** | **Unsupported Windows OS (remote)** |
| **5** | **MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check)** |
| **6** | **Unencrypted Telnet Server** |
| **7** | **Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness** |
| **8** | **Microsoft Windows SMB NULL Session Authentication** |
| **9** | **SMB Signing not required** |
| **10** | **Terminal Services Encryption Level is Medium or Low** |
| **11** | **Terminal Services Encryption Level is not FIPS-140 Compliant** |

**Host: 192.168.64.49**

**Wykryte Luki:**

|  |  |
| --- | --- |
| **1** | **MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687) (uncredentialed check)** |
| **2** | **MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)** |
| **3** | **Microsoft Windows XP Unsupported Installation Detection** |
| **4** | **Unsupported Windows OS (remote)** |
| **5** | **MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check)** |
| **6** | **Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness** |
| **7** | **Microsoft Windows SMB NULL Session Authentication** |
| **8** | **SMB Signing not required** |
| **9** | **Terminal Services Encryption Level is Medium or Low** |
| **10** | **Terminal Services Encryption Level is not FIPS-140 Compliant** |

**Host: 192.168.64.50**

**Wykryte Luki:**

|  |  |
| --- | --- |
| **1** | **Samba 'AndX' Request Heap-Based Buffer Overflow** |
| **2** | **Samba Badlock Vulnerability** |
| **3** | **NTP ntpd Mode 7 Error Response Packet Loop Remote DoS** |
| **4** | **SSL Certificate Cannot Be Trusted** |
| **5** | **SSL Self-Signed Certificate** |
| **6** | **IP Forwarding Enabled** |
| **7** | **DNS Server Cache Snooping Remote Information Disclosure** |
| **8** | **Network Time Protocol (NTP) Mode 6 Scanner** |
| **9** | **Network Time Protocol Daemon (ntpd) monlist Command Enabled DoS** |
| **10** | **SMB Signing not required** |
| **11** | **SSL Certificate Expiry** |
| **12** | **SSL Certificate Signed Using Weak Hashing Algorithm** |
| **13** | **SSL Certificate with Wrong Hostname** |
| **14** | **SSL Medium Strength Cipher Suites Supported (SWEET32)** |
| **15** | **SSL Weak Cipher Suites Supported** |
| **16** | **SSL/TLS EXPORT\_RSA &lt;= 512-bit Cipher Suites Supported (FREAK)** |
| **17** | **SSL RC4 Cipher Suites Supported (Bar Mitzvah)** |
| **18** | **SSL/TLS Diffie-Hellman Modulus &lt;= 1024 Bits (Logjam)** |
| **19** | **SSL/TLS EXPORT\_DHE &lt;= 512-bit Export Cipher Suites Supported (Logjam)** |

**Host: 192.168.64.55**

**Wykryte Luki:**



**Host: 192.168.64.57**

**Wykryte Luki:**



**Host: 192.168.64.61**

**Wykryte Luki:**



**Host: 192.168.64.62**

**Wykryte Luki:**



**Host: 192.168.64.64**

**Wykryte Luki:**



**Host: 192.168.64.73**

**Wykryte Luki:**



**Host: 192.168.64.75**

**Wykryte Luki:**



**Host: 192.168.64.76**

**Wykryte Luki:**



**Host: 192.168.64.77**

**Wykryte Luki:**



**Host: 192.168.64.78**

**Wykryte Luki:**



**Host: 192.168.64.81**

**Wykryte Luki:**



**Host: 192.168.64.82**

**Wykryte Luki:**



**Host: 192.168.64.83**

**Wykryte Luki:**



**Host: 192.168.64.85**

**Wykryte Luki:**



**Host: 192.168.64.96**

**Wykryte Luki:**



**Host: 192.168.64.97**

**Wykryte Luki:**