1. ASSET DETAILS

Host Name

UBUNTU-1404-ESM

IP Address: 192.168.1.30

OS: Ubuntu Linux 14.04

MAC Address: 08:00:27:FD:02:BC

Asset Discovery Date: February 14, 2022 (43 days ago)

Vulnerabilities Assessed: February 14, 2022 (43 days ago)

2. SUMMARY

44	13	653
Total vulnerabilities	Running Services	Installed Software

3. SOLUTIONS

Risk Score	Fix	Vulnerability Names

2.55k	**Configure SMB signing for Samba**
	Configure Samba to enable or require SMB signing as appropriate. To enable SMB signing, put the following in the Samba configuration file, typically smb.conf, in the global section:
	`server signing = auto`
	To require SMB signing, put the following in the Samba configuration file, typically smb.conf, in the global section:
	`server signing = mandatory`
		SMB signing not required
		SMB signing disabled
		SMBv2 signing not required

2.04k	**Disable insecure TLS/SSL protocol support** Configure the server to require clients to use TLS version 1.2 using Authenticated Encryption with Associated Data (AEAD) capable ciphers.	TLS/SSL Server is enabling the POODLE attack TLS Server Supports TLS version 1.0 TLS Server Supports TLS version 1.1 TLS/SSL Server Supports SSLv3
868	**Upgrade Ubuntu** Upgrade to a supported version of Ubuntu Linux	Obsolete Version of Ubuntu
831	**Fix the subject's Common Name (CN) field in the certificate** The subject's common name (CN) field in the X.509 certificate should be fixed to reflect the name of the entity presenting the certificate (e.g., the hostname). This is done by generating a new certificate usually signed by a Certification Authority (CA) trusted by both the client and server.	X.509 Certificate Subject CN Does Not Match the Entity Name

Risk Score	Fix	Vulnerability Names

753	**Enable GRUB password**
	Set a password in the GRUB configuration file. This is often located in one of several locations, but can really be anywhere:
	`/etc/grub.conf /boot/grub/grub.conf /boot/grub/grub.cfg /boot/grub/menu.lst`
	For all files mentioned above ensure that a password is set or that the files do not exist.
	To set a plain-text password, edit your GRUB configuration file and add the following line before the first uncommented line:
	`password <password>`
	To set an encrypted password, run grub-md5-crypt and use its output when adding the following line before the first uncommented line:
	`password --md5 <encryptedpassword>`
	For either approach, choose an appropriately strong password.
		No password for Grub

752	**Restrict invalid guest logins** In the 'Local Security Settings' feature of the Windows Control Panel, modify the following settings: • Set the 'Local Policies->User Rights Assignment->Deny access to this computer from the network' to include the guest account • Set the 'Local Policies->Security Options->Accounts: Guest account status' to 'Disabled'.	Invalid CIFS Logins Permitted

744	**Disable ICMP redirect support**
	Issue the following commands as root:
	`sysctl -w net.ipv4.conf.all.accept_redirects=0`
	`sysctl -w net.ipv4.conf.default.accept_redirects=0`
	`sysctl -w net.ipv4.conf.all.secure_redirects=0`
	`sysctl -w net.ipv4.conf.default.secure_redirects=0`
	These settings can be added to /etc/sysctl.conf to make them permanent.
		ICMP redirection enabled

742	**Fix Apache Tomcat v4.x Example Scripts Information Leakage** Delete these scripts entirely. Example scripts should never be installed on production servers.	Apache Tomcat Example Scripts Information Leakage

Risk Score	Fix	Vulnerability Names
739	**Edit '/etc/securetty' entries** Remove all the entries in /etc/securetty except console, tty[0-9]* and vc\[0-9]* Note: ssh does not use /etc/securetty. To disable root login through ssh, use the "PermitRootLogin" setting in /etc/ssh/sshd_config and restart the ssh daemon.	Anonymous root login is allowed
736	**Reset umask value** To ensure complete access control over newly created files, set the umask value to 077 for root and other user accounts for both interactive and non-interactive processes. The umask value for interactive processes is typically set via PAM. See 'man 8 pam_umask'. For non-interactive processes, /etc/login.defs is a common location for controlling umask on Linux systems. In both cases, you may need to consult your operating system's documentation for the correct file(s) and settings. For Red Hat Enterprise Linux and derivative distributions the umask value is set in /etc/profile and /etc/bashrc shell configuration files. See the Red Hat manual for more details.	User umask value is unsafe
697	**Obtain a new certificate from your CA and ensure the server configuration is correct** Ensure the common name (CN) reflects the name of the entity presenting the certificate (e.g., the hostname). If the certificate(s) or any of the chain certificate(s) have expired or been revoked, obtain a new certificate from your Certificate Authority (CA) by following their documentation. If a self-signed certificate is being used, consider obtaining a signed certificate from a CA. References: Mozilla: Connection Untrusted ErrorSSLShopper: SSL Certificate Not Trusted ErrorWindows/IIS certificate chain configApache SSL configNginx SSL configCertificateChain.io	Untrusted TLS/SSL server X.509 certificate
600	**Restrict Query Access on Caching Nameservers** Restrict the processing of DNS queries to only systems that should be allowed to use this nameserver.	DNS server allows cache snooping
593	**Change the default page, or stop and disable the Tomcat server completely** If this server is required to provide necessary functionality, then the default page should be replaced with relevant content. Otherwise, this server should be removed from the network, following the security principle of minimum complexity.	Apache Tomcat default installation/welcome page installed
583	**Restrict User's home directory mode** Restrict the user home directory mode to at most 750 using the command: `chmod 750 userDir`	User home directory mode unsafe
581	**Partition Mounting Weakness** The specific way to modify the partition mount options varies from system to system. Consult your operating system's manual or mount man page.	Partition Mounting Weakness
579	**Disable HTTP OPTIONS method** Disable HTTP OPTIONS method on your web server. Refer to your web server's instruction manual on how to do this.	HTTP OPTIONS Method Enabled

Risk Score	Fix	Vulnerability Names
578	**Disable any MD5 or 96-bit HMAC algorithms within the SSH configuration** Consult the product documentation for instructions to disable any insecure MD5 or 96-bit HMAC algorithms within the SSH configuration.	SSH Weak Message Authentication Code Algorithms
573	**Remove/disable SMB1** For Samba systems on Linux, disabling SMB1 is quite straightforward: How to configure Samba to use SMBv2 and disable SMBv1 on Linux or Unix	SMB: Service supports deprecated SMBv1 protocol
546	**Disable SSLv2, SSLv3, and TLS 1.0. The best solution is to only have TLS 1.2 enabled** There is no server-side mitigation available against the BEAST attack. The only option is to disable the affected protocols (SSLv3 and TLS 1.0). The only fully safe configuration is to use Authenticated Encryption with Associated Data (AEAD), e.g. AES-GCM, AES-CCM in TLS 1.2.	TLS/SSL Server is enabling the BEAST attack
538	**Disable TLS/SSL support for 3DES cipher suite** Configure the server to disable support for 3DES suite. For Microsoft IIS web servers, see Microsoft Knowledgebase article 245030 for instructions on disabling 3DES cipher suite. The following recommended configuration provides a higher level of security. This configuration is compatible with Firefox 27, Chrome 22, IE 11, Opera 14 and Safari 7. SSLv2, SSLv3, and TLSv1 protocols are not recommended in this configuration. Instead, use TLSv1.1 and TLSv1.2 protocols. Refer to your server vendor documentation to apply the recommended cipher configuration: ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-DSS-AES128-GCM-SHA256:kEDH+AESGCM:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA:DHE-DSS-AES128-SHA256:DHE-RSA-AES256-SHA256:DHE-DSS-AES256-SHA:DHE-RSA-AES256-SHA:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!3DES:!MD5:!PSK	TLS/SSL Server Supports 3DES Cipher Suite TLS/SSL Birthday attacks on 64-bit block ciphers (SWEET32)
527	**Disable SSH support for RC4 ciphers** Remove arcfour, arcfour128, and arcfour256 from the Ciphers list specified in sshd_config.	SSH Server Supports RC4 Cipher Algorithms

Risk Score	Fix	Vulnerability Names
527	**Disable TLS/SSL support for RC4 ciphers** Configure the server to disable support for RC4 ciphers. For Microsoft IIS web servers, see Microsoft Knowledgebase article 245030 for instructions on disabling rc4 ciphers. The following recommended configuration provides a higher level of security. This configuration is compatible with Firefox 27, Chrome 22, IE 11, Opera 14 and Safari 7. SSLv2, SSLv3, and TLSv1 protocols are not recommended in this configuration. Instead, use TLSv1.1 and TLSv1.2 protocols. Refer to your server vendor documentation to apply the recommended cipher configuration: ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-DSS-AES128-GCM-SHA256:kEDH+AESGCM:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA:DHE-DSS-AES128-SHA256:DHE-RSA-AES256-SHA256:DHE-DSS-AES256-SHA:DHE-RSA-AES256-SHA:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!3DES:!MD5:!PSK	TLS/SSL Server Supports RC4 Cipher Algorithms (CVE-2013-2566)
512	**Disable SSH support for CBC cipher suite** SSH can be done using Counter (CTR) mode encryption. This mode generates the keystream by encrypting successive values of a "counter" function. In order to mitigate this vulnerabilty SSH can be setup to use CTR mode rather CBC mode.	SSH CBC vulnerability
471	**Disable TLS/SSL support for static key cipher suites** Configure the server to disable support for static key cipher suites. For Microsoft IIS web servers, see Microsoft Knowledgebase article 245030 for instructions on disabling static key cipher suites. The following recommended configuration provides a higher level of security. This configuration is compatible with Firefox 27, Chrome 22, IE 11, Opera 14 and Safari 7. SSLv2, SSLv3, and TLSv1 protocols are not recommended in this configuration. Instead, use TLSv1.1 and TLSv1.2 protocols. Refer to your server vendor documentation to apply the recommended cipher configuration: ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-DSS-AES128-GCM-SHA256:kEDH+AESGCM:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA:DHE-DSS-AES128-SHA256:DHE-RSA-AES256-SHA256:DHE-DSS-AES256-SHA:DHE-RSA-AES256-SHA:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!3DES:!MD5:!PSK	TLS/SSL Server Supports The Use of Static Key Ciphers
462	**Upgrade to the latest version of Apache HTTPD** Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.4.51.tar.gz	Apache HTTPD: HTTP request smuggling attack against chunked request parser (CVE-2015-3183) Apache HTTPD: HTTP Trailers processing bypass (CVE-2013-5704)
433	**Disable weak Key Exchange Algorithms**	SSH Server Supports Weak Key Exchange Algorithms

Risk Score	Fix	Vulnerability Names
393	**Disable HTTP DELETE method** Disable HTTP DELETE method on your web server. Refer to your web server's instruction manual on how to do this.	HTTP DELETE Method Enabled
249	**Replace TLS/SSL self-signed certificate** Obtain a new TLS/SSL server certificate that is NOT self-signed and install it on the server. The exact instructions for obtaining a new certificate depend on your organization's requirements. Generally, you will need to generate a certificate request and save the request as a file. This file is then sent to a Certificate Authority (CA) for processing. Your organization may have its own internal Certificate Authority. If not, you may have to pay for a certificate from a trusted external Certificate Authority, such as Thawte or Verisign.	Self-signed TLS/SSL certificate
200	**Restrict Processing of Recursive Queries** Restrict the processing of recursive queries to only systems that should be allowed to use this nameserver.	Nameserver Processes Recursive Queries
193	**Use a Stronger Diffie-Hellman Group** Please refer to this guide to deploying Diffie-Hellman for TLS for instructions on how to configure the server to use 2048-bit or stronger Diffie-Hellman groups with safe primes.	Diffie-Hellman group smaller than 2048 bits
0	**Adjust the share permissions to be more secure** Adjust the share permissions to restrict access to only those members of the organization who need the data. It is considered bad practice to grant the "Everyone", "Guest", or "Authenticated Users" groups read or write access to a share.	CIFS Share Readable By Everyone CIFS Share Writeable By Everyone
0	**Disable SSH support for 3DES cipher suite** Remove all 3DES ciphers from the cipher list specified in sshd_config.	SSH Server Supports 3DES Cipher Suite
0	**Restrict access to DNS**	DNS Traffic Amplification
0	**Restrict access to NetBIOS**	NetBIOS NBSTAT Traffic Amplification

Risk Score	Fix	Vulnerability Names

0	**Disable ICMP timestamp responses on Linux**
	Linux offers neither a sysctl nor a /proc/sys/net/ipv4 interface to disable ICMP timestamp responses. Therefore, you should block ICMP on the affected host using iptables, and/or block it at the firewall. For example:
	`ipchains -A input -p icmp --icmp-type timestamp-request -j DROP`
	`ipchains -A output -p icmp --icmp-type timestamp-reply -j DROP`
	The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).
		ICMP timestamp response

0	**Disable TCP timestamp responses on Linux**
	Set the value of net.ipv4.tcp_timestamps to 0 by running the following command:
	`sysctl -w net.ipv4.tcp_timestamps=0`
	Additionally, put the following value in the default sysctl configuration file, generally sysctl.conf:
	`net.ipv4.tcp_timestamps=0`
		TCP timestamp response

4. VULNERABILITIES (44)

Vulnerability Name	CVSS Score	Risk Score	Published On	Found	Severity	Solution
Anonymous root login is allowed	6.5	739	Tue, Nov 30, 2004	Tue, Nov 30, 2004	Severe	Solution
Apache HTTPD: HTTP request smuggling attack against chunked request parser (CVE-2015-3183)	5	229	Mon, Jul 20, 2015	Mon, Jul 20, 2015	Severe	Solution
Apache HTTPD: HTTP Trailers processing bypass (CVE-2013-5704)	5	234	Tue, Apr 15, 2014	Thu, Sep 4, 2014	Severe	Solution
Apache Tomcat default installation/welcome page installed	5	593	Wed, Jul 20, 2005	Wed, Jul 20, 2005	Severe	Solution
Apache Tomcat Example Scripts Information Leakage	7.8	742	Mon, Nov 1, 2004	Mon, Nov 1, 2004	Critical	Solution
CIFS Share Readable By Everyone	0	0.0	Fri, Jan 1, 1999	Thu, Jan 19, 2017	Moderate	Solution
CIFS Share Writeable By Everyone	0	0.0	Fri, Jan 1, 1999	Thu, Jan 19, 2017	Moderate	Solution
Diffie-Hellman group smaller than 2048 bits	2.6	193	Wed, May 20, 2015	Thu, Nov 12, 2015	Moderate	Solution
DNS server allows cache snooping	5	600	Mon, Jan 1, 1990	Fri, Apr 1, 2011	Severe	Solution
DNS Traffic Amplification	0	0.0	Fri, Mar 29, 2013	Wed, Dec 10, 2014	Moderate	Solution
HTTP DELETE Method Enabled	6.5	393	Mon, Aug 20, 2007	Mon, Aug 20, 2007	Severe	Solution
HTTP OPTIONS Method Enabled	2.6	579	Fri, Oct 7, 2005	Tue, Aug 28, 2018	Moderate	Solution
ICMP redirection enabled	6.8	744	Wed, Dec 31, 2003	Tue, Nov 30, 2004	Severe	Solution
ICMP timestamp response	0	0.0	Fri, Aug 1, 1997	Mon, Nov 1, 2004	Moderate	Solution
Invalid CIFS Logins Permitted	7.5	752	Tue, Jan 25, 2005	Tue, Jan 25, 2005	Critical	Solution

Vulnerability Name	CVSS Score	Risk Score	Published On	Found	Severity	Solution
Nameserver Processes Recursive Queries	5	200	Mon, Jan 1, 1990	Fri, Feb 26, 2010	Severe	Solution
NetBIOS NBSTAT Traffic Amplification	0	0.0	Sun, Feb 9, 2014	Wed, Dec 10, 2014	Moderate	Solution
No password for Grub	4.6	753	Fri, Jan 1, 1999	Tue, Nov 30, 2004	Severe	Solution
Obsolete Version of Ubuntu	10	868	Mon, May 6, 2013	Mon, May 6, 2013	Critical	Solution
Partition Mounting Weakness	1.9	581	Sat, Jan 15, 2005	Sat, Jan 15, 2005	Moderate	Solution
Self-signed TLS/SSL certificate	4.3	249	Sun, Jan 1, 1995	Thu, Jul 16, 2009	Severe	Solution
SMB signing disabled	7.3	851	Mon, Nov 1, 2004	Fri, Apr 1, 2011	Severe	Solution
SMB signing not required	6.2	848	Mon, Nov 1, 2004	Fri, Apr 1, 2011	Severe	Solution
SMB: Service supports deprecated SMBv1 protocol	4.8	573	Tue, Apr 21, 2015	Thu, Apr 11, 2019	Severe	Solution
SMBv2 signing not required	6.2	848	Mon, Nov 1, 2004	Wed, Feb 21, 2018	Severe	Solution
SSH CBC vulnerability	2.6	512	Fri, Feb 8, 2013	Tue, Mar 31, 2020	Moderate	Solution
SSH Server Supports 3DES Cipher Suite	0	0.0	Sun, Feb 1, 2009	Tue, Mar 31, 2020	Moderate	Solution
SSH Server Supports RC4 Cipher Algorithms	4.3	527	Tue, Mar 12, 2013	Tue, Mar 31, 2020	Severe	Solution
SSH Server Supports Weak Key Exchange Algorithms	4.3	433	Thu, Jul 13, 2017	Tue, Mar 31, 2020	Severe	Solution
SSH Weak Message Authentication Code Algorithms	4	578	Mon, Jan 6, 2014	Tue, Mar 31, 2020	Severe	Solution
TCP timestamp response	0	0.0	Fri, Aug 1, 1997	Fri, Apr 1, 2011	Moderate	Solution
TLS Server Supports TLS version 1.0	4.3	501	Tue, Oct 14, 2014	Thu, Nov 12, 2015	Severe	Solution
TLS Server Supports TLS version 1.1	2.6	478	Tue, Oct 14, 2014	Thu, Nov 12, 2015	Moderate	Solution
TLS/SSL Birthday attacks on 64-bit block ciphers (SWEET32)	7.5	538	Wed, Aug 24, 2016	Wed, Aug 24, 2016	Severe	Solution
TLS/SSL Server is enabling the BEAST attack	4.3	546	Tue, Sep 6, 2011	Thu, Feb 18, 2016	Severe	Solution
TLS/SSL Server is enabling the POODLE attack	3.4	532	Tue, Oct 14, 2014	Tue, Feb 23, 2016	Severe	Solution
TLS/SSL Server Supports 3DES Cipher Suite	0	0.0	Sun, Feb 1, 2009	Wed, Sep 30, 2015	Moderate	Solution
TLS/SSL Server Supports RC4 Cipher Algorithms (CVE-2013-2566)	5.9	527	Tue, Mar 12, 2013	Thu, Sep 18, 2014	Severe	Solution
TLS/SSL Server Supports SSLv3	3.4	532	Tue, Oct 14, 2014	Tue, Oct 14, 2014	Severe	Solution
TLS/SSL Server Supports The Use of Static Key Ciphers	2.6	471	Sun, Feb 1, 2015	Wed, Sep 30, 2015	Moderate	Solution
Untrusted TLS/SSL server X.509 certificate	5.8	697	Sun, Jan 1, 1995	Mon, Oct 19, 2009	Severe	Solution
User home directory mode unsafe	2.1	583	Sat, Jan 15, 2005	Sat, Jan 15, 2005	Moderate	Solution
User umask value is unsafe	4.4	736	Sat, Jan 15, 2005	Sat, Jan 15, 2005	Severe	Solution

Vulnerability Name	CVSS Score	Risk Score	Published On	Found	Severity	Solution
X.509 Certificate Subject CN Does Not Match the Entity Name	7.1	831	Fri, Aug 3, 2007	Fri, Aug 3, 2007	Severe	Solution