1. ASSET DETAILS

Host Name

UBUNTU_1604_ESM

IP Address: 192.168.1.27

OS: Ubuntu Linux 16.04

MAC Address: 08:00:27:DB:E3:00

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

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

2. SUMMARY

23	9	576
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`
		SMBv2 signing not required
		SMB signing not required
		SMB signing disabled

868	**Upgrade Ubuntu** Upgrade to a supported version of Ubuntu Linux	Obsolete Version of Ubuntu

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

Risk Score	Fix	Vulnerability Names
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

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
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
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

Risk Score	Fix	Vulnerability Names
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
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
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
154	**Upgrade ISC BIND to latest version** More information about upgrading your version of ISC BIND is available on the ISC website.	ISC BIND: A query name which is too long can cause a segmentation fault in lwresd (CVE-2016-2775)
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	**Restrict access to DNS**	DNS Traffic Amplification

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	**Restrict access to NetBIOS**	NetBIOS NBSTAT Traffic Amplification

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 (23)

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
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
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 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
ISC BIND: A query name which is too long can cause a segmentation fault in lwresd (CVE-2016-2775)	5.9	154	Tue, Jul 19, 2016	Tue, Aug 2, 2016	Severe	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
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 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
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