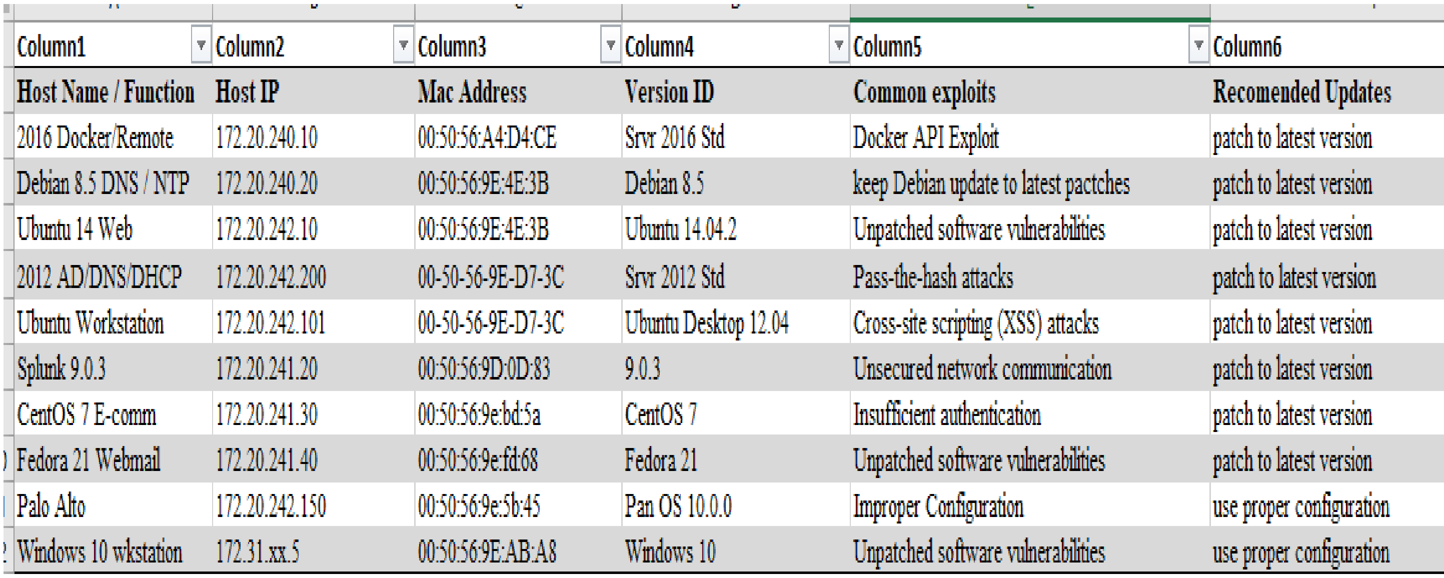
Team-9a

Inject: EVAL11A

Internal Services Evaluation

This Table is an Inventory Audits of all our host devices, with associated physical and internet address, as well as device version.

We have also have common typical exploits of each device, we always recommend updating to the latest patch as soon as possible for security reason.



Column1	Column2	Column3	Column4	Column5	Column6
Host Name / Function	**Host IP**	**Mac Address**	**Version ID**	**Common exploits**	**Recomended Updates**
2016 Docker/Remote	172.20.240.10	00:50:56:A4:D4:CE	Srvr 2016 Std	Docker API Exploit	patch to latest version
Debian 8.5 DNS / NTP	172.20.240.20	00:50:56:9E:4E:3B	Debian 8.5	keep Debian update to latest pactches	patch to latest version
Ubuntu 14 Web	172.20.242.10	00:50:56:9E:4E:3B	Ubuntu 14.04.2	Unpatched software vulnerabilities	patch to latest version
2012 AD/DNS/DHCP	172.20.242.200	00-50-56-9E-D7-3C	Srvr 2012 Std	Pass-the-hash attacks	patch to latest version
Ubuntu Workstation	172.20.242.101	00-50-56-9E-D7-3C	Ubuntu Desktop 12.04	Cross-site scripting (XSS) attacks	patch to latest version
Splunk 9.0.3	172.20.241.20	00:50:56:9D:0D:83	9.0.3	Unsecured network communication	patch to latest version
CentOS 7 E-comm	172.20.241.30	00:50:56:9e:bd:5a	CentOS 7	Insufficient authentication	patch to latest version
Fedora 21 Webmail	172.20.241.40	00:50:56:9e:fd:68	Fedora 21	Unpatched software vulnerabilities	patch to latest version
Palo Alto	172.20.242.150	00:50:56:9e:5b:45	Pan OS 10.0.0	Improper Configuration	use proper configuration
Windows 10 wkstation	172.31.xx.5	00:50:56:9E:AB:A8	Windows 10	Unpatched software vulnerabilities	use proper configuration

.