* Write a brief description of a vulnerability found in the scan, including the operating system on which it was found, its risk factor, and its CVSS scores. Mozilla Firefox is an open source web browser. One Vulnerability that CentOS 6/7 Firefox (CESA-20107) the risk was high, CVSS base score is 9.3, the CVSS Temporal Score is at 6.9, CVSS Vector. CVSS2#AV: N/AC: Au: N/C:C/I:C/A:C. Multiple flaws were found in the processing of malformed web content. A web page containing malicious content could cause Firefox to crash or, potentially, execute arbitrary code with the privileges of the user running FireFox.
* Are the results of default scans different than the credentialed scan? Why might that be? Yes, because default scans will identify only a small number of patches and credentialed scan can identify a large number of patches. What types of vulnerabilities might an attacker without any credentials be able to identify and exploit? There are five common types of website vulnerabilities that attacker without any credentials be able to identify and exploit. First, SQL Injection Vulnerabilities (SQLi) This vulnerability refers to areas in website code where direct user input is passed to a database. This allows the attacker to access the website through various ways such as putting malicious and spam posts into a site, stealing customer information, and Bypassing authentication to gain full control of the website. It is frequently used to gain access to open source content management system applications like Joomla, Word Press. Second, Cross-Site Scripting (XSS) This happens when attacker puts scripts through unclean user input or other fields on a website to execute code on the site. This use to target website visitors. Browsers are unable to determine if the script is intended to be a part of the website will result in malicious actions like session hijacking and stealing session data. This vulnerability was found in gaming giant steam’s system that potentially exposed login credentials to attackers Third, Command Injection Vulnerability occurs when user input that is passed to the server that is not properly validated. This allows attackers to include shell commands with the user information. These attacks are critical because they can allow bad actors to initiate hijacking an entire site, hosting server, and utilize the hijacked server in botnet attacks. The most dangerous and command injection vulnerabilities was the shellshock vulnerability that impacted most Linux distributions. Fourth, File Inclusion (LFI/RFI) Remote file inclusion attacks use the include functions in server side-web application languages to execute code from remotely stored file. Attackers host malicious files and take advantage improperly cleaned user input to modify an include function to victim site’s PHP Code. This includes taking control of a website admin panel or host server and include malicious shell files on publicly available websites. This vulnerability occurs can occur when user input is able to modify the full or absolute path to included files. Attackers can then use this vector to gain, read or write access to sensitive local files. These types of vulnerabilities are frequently used to launch other attacks, such as DDoS and cross-site scripting attacks. They have also been used to expose and steal sensitive financial information, such as when [Starbucks fell victim to an inclusion attack](https://www.techworm.net/2015/09/critical-vulnerabilities-in-starbucks-allows-hackers-to-steal-credit-card-details.html) leading to a compromise of customer credit card data. Last, **Cross-Site Request Forgery (CSRF)** – [Cross-site request forgery](https://sitelock.com/blog/2016/08/what-is-cross-site-request-forgery-csrf/) CSRF attacks trick site users or administrators to unknowingly perform malicious actions for the attacker. Examples of this vulnerability is Transfer funds from one account to another and Change user passwords to hijack accounts. These types of attacks are particularly vexing for ecommerce and banking sites where attackers can gain access to sensitive financial information
* This was a simple three computer LAN. How much more complicated would this process be for 100 computers? What about an enterprise with 10,000 computers than on their LAN/WAN? First, configuring windows firewall, creating firewall profiles like domain, private, and public, filtering incoming traffic, filtering outbound traffic. An enterprise with 10,000 computers on their LAN the software files will be shared among all users all can have access to the latest files. Wan covers large geographical areas. Business offices situated at longer distance can communicate. Contains devices like gaming consoles, mobile phones, laptops, and computers. A disadvantage to maintain WAN network you will need technicians, and network administrators. Wan requires more time to resolve issues because of the involvement of multiple wired and wireless technologies.

Consider a cloud-hosted Infrastructure as a Service (IaaS) environment with many new, internet-accessible systems regularly being built and brought online. What advantages or challenges might there be with regards to vulnerability management in the cloud? What challenges might there be with regards to vulnerability management in the cloud. The challenges that might occur are the following: shared security responsibility. An organization moves applications and data to the cloud the organization will shift the responsibility to the cloud provider. Most cloud providers are responsible for securing the cloud infrastructure. The cloud user is responsible for the applications and data used in the cloud platform. It is very important to how the responsibility is shared. Dynamic Environments can occur when organizations can create large numbers of circumstances, increased the number of servers to monitor and manage. More players and different skillsets are individuals and teams outside the IT department can deploy and manage IT department. Some individuals will not have the expertise to set up cloud environment securely. There are no guarantees that there will not be a negative or positive effect.

References

[www.tenable.com](http://www.tenable.com)

[https://www.sitelock.com](https://www.sitelock.com/)