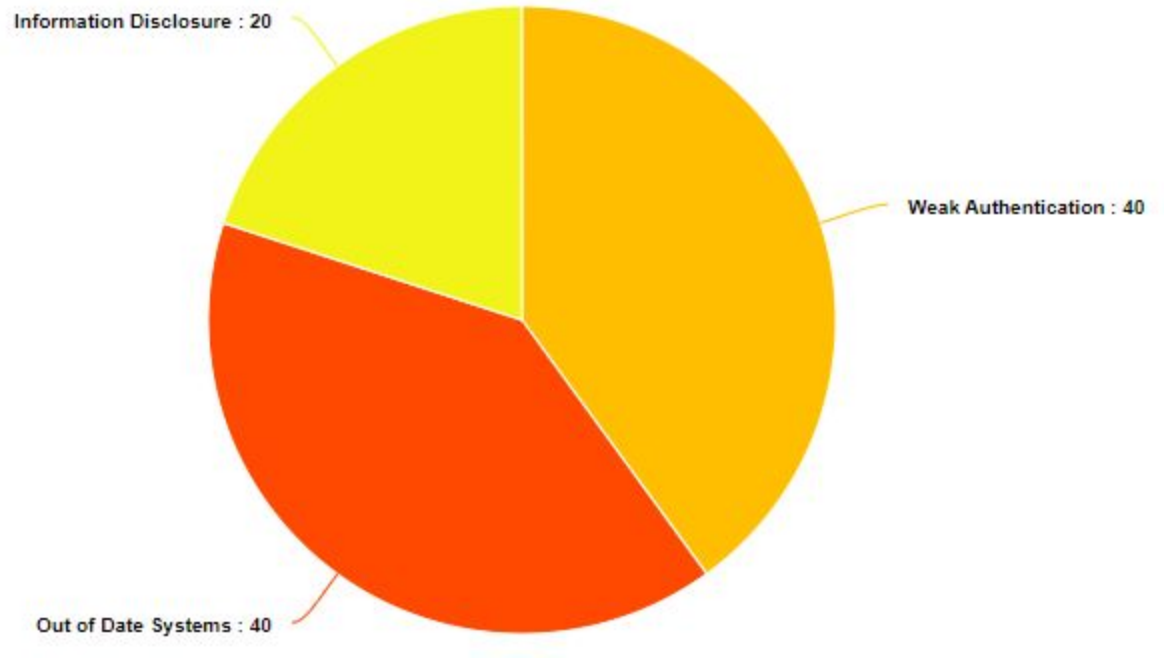
Penetration Test
Summary of Findings

Andrey Rainchik
4/22/2018

Summary of Findings

- **Weak Authentication:** users on the host have weak passwords and SSH keys that allow an attacker to gain administrative access
- **Out of Date Systems:** the operating system as well as software on the host are out of date by several versions and are missing critical patches
- **Information Disclosure:** Attackers can easily find information about the PHP version on the web server, allowing them to find specific vulnerabilities in the system



Weak Passwords - Rating: HIGH

Threat Agent Factors					Vulnerability Factors			
Skill Level	Motive	Opportunity	Size		Ease of Discovery	Ease of Exploit	Awareness	Intrusion Detection
7	4	8	9		7	9	8	3
Overall Likelihood = 6.9 (HIGH)								

Technical Impact					Business Impact			
Loss of Confidentiality	Loss of Integrity	Loss of Availability	Loss of Accountability		Financial Damage	Reputation Damage	Non-compliance	Privacy Violation
9	7	4	9		3	7	7	4
Overall Technical Impact = 7.3 (HIGH)					Overall Business Impact = 5.3 (MEDIUM)			

Weak SSH Keys - Rating: HIGH

Threat Agent Factors					Vulnerability Factors			
Skill Level	Motive	Opportunity	Size		Ease of Discovery	Ease of Exploit	Awareness	Intrusion Detection
5	4	7	7		7	7	8	8
Overall Likelihood = 6.6 (HIGH)								

Technical Impact					Business Impact			
Loss of Confidentiality	Loss of Integrity	Loss of Availability	Loss of Accountability		Financial Damage	Reputation Damage	Non-compliance	Privacy Violation
9	7	4	9		3	5	6	4
Overall Technical Impact = 7.3 (HIGH)					Overall Business Impact = 4.5 (MEDIUM)			

End of Life Operating System - Rating: HIGH

Threat Agent Factors					Vulnerability Factors			
Skill Level	Motive	Opportunity	Size		Ease of Discovery	Ease of Exploit	Awareness	Intrusion Detection
6	5	8	8		6	7	6	3
Overall Likelihood = 6.1 (HIGH)								

Technical Impact					Business Impact			
Loss of Confidentiality	Loss of Integrity	Loss of Availability	Loss of Accountability		Financial Damage	Reputation Damage	Non-compliance	Privacy Violation
9	7	4	9		3	6	9	4
Overall Technical Impact = 7.3 (HIGH)					Overall Business Impact = 5.5 (MEDIUM)			

Vulnerable Java Server - Rating: MEDIUM

Threat Agent Factors					Vulnerability Factors			
Skill Level	Motive	Opportunity	Size		Ease of Discovery	Ease of Exploit	Awareness	Intrusion Detection
6	4	8	8		7	9	7	3
Overall Likelihood = 6.5 (HIGH)								

Technical Impact					Business Impact			
Loss of Confidentiality	Loss of Integrity	Loss of Availability	Loss of Accountability		Financial Damage	Reputation Damage	Non-compliance	Privacy Violation
9	7	4	9		3	4	3	4
Overall Technical Impact = 7.3 (HIGH)					Overall Business Impact = 3.5 (MEDIUM)			

PHP Information Disclosure - Rating: MEDIUM

Threat Agent Factors					Vulnerability Factors			
Skill Level	Motive	Opportunity	Size		Ease of Discovery	Ease of Exploit	Awareness	Intrusion Detection
7	4	8	9		7	3	5	4
Overall Likelihood = 5.9 (MEDIUM)								

Technical Impact					Business Impact			
Loss of Confidentiality	Loss of Integrity	Loss of Availability	Loss of Accountability		Financial Damage	Reputation Damage	Non-compliance	Privacy Violation
5	6	4	8		3	4	3	4
Overall Technical Impact = 5.8 (MEDIUM)					Overall Business Impact = 3.5 (MEDIUM)			

Findings Matrix

#	Category	Finding	Impact	Severity/ Difficulty of Exploit	Recommendation
1	Weak Authentication	Multiple users on the system had passwords that were the same as their username.	One of the affected users had administrative access to the machine, meaning that it would be trivial for an attacker to guess the password and have unlimited admin access.	Severity: HIGH Difficulty: LOW Status: OPEN	Establish strong password policies, refer to NIST guidelines for passwords to model the password policies
2	Weak Authentication	SSH keys generated on the machine were created with a weak encryption, allowing an attacker to more easily brute-force access to the machine.	The root user had a private SSH key that was vulnerable, allowing an attacker to brute-force the key and log in with full administrative access	Severity: HIGH Difficulty: LOW Status: OPEN	Update the version of OpenSSH and OpenSSH to the most recent versions. Monitor for patches and establish a patching cycle.
3	Out of Date Systems	The operating system running on the machine, Ubuntu 8.04, has reached its end of life and has not received security patches since 2013.	Multiple vulnerabilities exist on this operating system and will not be patched due to the operating system reaching its end of support. Some vulnerabilities allow for an attacker to gain administrative access on the machine.	Severity: HIGH Difficulty: MEDIUM Status: OPEN	Update the operating system on the machine to the most recent Ubuntu release. Install security patches as they come out and move on to more recent operating systems when end of life occurs.
4	Out of Date Systems	The default configuration of the Java runtime environment associated with the Java RMI server on the host is vulnerable to remote code execution.	An attacker can send a carefully crafted JAR file to the server to gain administrative access to the machine.	Severity: HIGH Difficulty: LOW Status: OPEN	Update the version of the JRE, JDK, and/or Jrockit installed on the machine to the most recent version. Monitor for patches and establish a patching cycle.

5	Information Disclosure	The webserver on the host includes a page with information about the specific PHP version being used on the server.	Using the information found on the page, an attacker can search for exploits associated with the PHP version found.	Severity: MEDIUM Difficulty: LOW Status: OPEN	Limit access to the PHP information page or remove it from webhosting entirely.

Analysis

According to my professional determination, this security environment rates weak. Multiple vulnerabilities were found that gave an attacker root access, and the operating system and software on the machine are out of date by several years. A majority of the vulnerabilities found were low-difficulty to exploit and would cause a high-severity impact if they were exploited. My recommendation is for this system to be taken offline until appropriate patches and updates can be applied, if not completely wiped and reinstalled due to the presence of several backdoors, indicating that this host is being actively exploited. This security environment rates below average, and this is reflected in the comparative rating and ratings matrix summary.

Ratings Matrix Summary		Difficulty		
		Low	Medium	High
Severity	High	3	1	
	Medium	1		
	Low