Penetration Test Report

for the Behemoth Network

Kevin Haroldsen

March 9, 2017

BYU | CYBERSECURITY RESEARCH LAB

Contents

1 Risk Analysis

I've determined the overall risk to the Behemoth Network as being **High** from this penetration test. With a targeted attack, a malicious agent could gain full access with domain administrator credentials and retrieve proprietary data.

I also individually rate the discovered vulnerabilities based on their likelihood and impact to determine risk.

1.1 RDP Remote Code Execution Vulnerabilities

Overall Risk: **High**
Hosts Affected: `192.168.207.42`
Description: The host is missing a critical security update to Windows Remote Desktop.
Impact: The Remote Desktop in Windows has a vulnerability which could allow execution of code in the context of the logged-on user, or cause a denial of service attack.
Recommendation: Update Windows to install the hotfix described in Microsoft Bulletin MS12-020.

1.2 SMB Server NTLM Multiple Vulnerabilities

Overall Risk: **High**
Hosts Affected: `192.168.207.42`
Description: The host is missing a critical security update to the Windows SMB service stack.
Impact: Remote attackers may be able to execute abritrary code, cause a denial or service, or bypass authentication with a brute-force method.
Recommendation: Update Windows to install the hotfix described in Microsoft Bulletin MS10-012.

1.3 PHP `com_print_typeinfo()` Remote Code Execution

Overall Risk: **High**
Hosts Affected: `192.168.207.101`
Description: The host is out of date and installed with PHP.
Impact: Remote code execution can be performed in the context of the web server.
Recommendation: Update to a new version of PHP and Windows.

1.4 SMBv1 Remote Code Execution (Shadow Brokers)

Overall Risk: **High**
Hosts Affected: `192.168.207.42,192.168.207.101,192.168.207.121,192.168.208.20`
Description: The host is prone to a remote code execution vulnerability in the SMBv1 protocol.
Impact: Arbitrary code can possibly be executed in a system context.
Recommendation: Disable SMBv1, and/or block all versions of SMB with the firewall or otherwise.

1.5 Multiple PHP Vulnerabilities

Overall Risk: **High**
Hosts Affected: `192.168.207.101`
Description: The host is installed with an old version of PHP that has reach end-of-life and is vulnerable to many known attacks.
Impact: Successfully exploiting any of the issues can cause a denial of service, ability to read and write abritrary files, execute arbitrary code, and perform buffer overflow attacks.
Recommendation: Upgrade to PHP version 5.6.10 or later.

1.6 WordPress `wp-admin` Multiple Vulnerabilities

Overall Risk: **High**
Hosts Affected: `192.168.207.119`
Description: The host is running a version of WordPress that is prone to multiple vulnerabilities.
Impact: Remote Code Execution and gaining access to the administrative page of WordPress are both possible for an attacker.
Recommendation: Upgrade WordPress to at least version 2.8.3.

1.7 Poor Password Policies

Overall Risk: **High**
Hosts Affected: `192.168.207.101,192.168.207.121,192.168.207.122`
Description: The hosts used passwords that were easy to guess, and/or shared the passwords with operating system accounts.
Impact: Access to system administrator accounts became possible with password brute force attempts or simple social engineering.
Recommendation: Enforce stronger password policies, and separate system and service accounts.

1.8 SQL Injection Vulnerability can reveal accounts

Overall Risk: **High**
Hosts Affected: `192.168.207.101`
Description: The custom Wheatley Labs page is vulnerable to a SQL Injection attack on its username/password database. In addition, passwords are also stored in plaintext that are shared with system accounts.
Impact: A remote attacker can retrieve usernames and passwords for local accounts on the system, gaining full access.
Recommendation: Do not store passwords in plaintext, separate system and service accounts, and escape SQL input.

1.9 HTTP.sys Remote Code Execution Vulnerability

Overall Risk: **High**
Hosts Affected: `192.168.207.121,192.168.208.20`
Description: The host is missing an important security update to its HTTP parsing mechanisms.
Impact: Remote attackers can run arbitrary code in the context of the current user and perform actions in the security context of the current user.
Recommendation: Update Windows to install the hotfix described in Microsoft Bulletin MS15-034.

1.10 Damn Vulnerable Web App

Overall Risk: **High**
Hosts Affected: `192.168.207.119`
Description: The system has an extremely vulnerable web application with many, many vulnerabilities.
Impact: Remote code execution, XSS, SQL Injection, and a large variety of vulnerabilities allow a remote attacker to gain complete control of a device.
Recommendation: Do not use this web application.

2 Conclusion

Overall, the Behemoth Networkhas many vulnerabilities which may be exploited. The risks listed above were deemed the most important to disclose and fix, although others do exist. I highly suggest following the recommendations provided with each listed vulnerability.