Scanning For Vulnerable Apache Servers

Enterprise Network Security

Dylan Bray and David Chun

ABSTRACT

Describe the overall area of contribution, the crux of the problem, and end with highlights of results. For the initial report, end with the proposed experiments and what you aim to find out.

1. INTRODUCTION

First paragraph on the technology/society trends that lead to the problem at hand.

Second para: describe the key problem that if solved would make an impact. Why the current approaches leave a gap?

Third: describe your approach. Key insight that enables your approach, and what is novel/interesting about the insight.

Fourth, fifth: Delve deeper into the approach and experimental setup. In the final report, describe key findings.

End with outline or what comes next and why.

2. MOTIVATION

In a paper by Li, Avellino, Janies, and Collins (2016) [3], they discuss a tool designed to improve vulnerability management via detection and monitoring called the Software Asset Analyzer (SAA). This scanner addresses a few key scenarios that could lead to vulnerable systems, namely unapproved software download, failure to upgrade, lack of knowledge of installed applications, and remediation verification. To detect the potential install of vulnerable CPEs and verify it has been properly dealt with, the SAA tool takes a blacklist and checks network hosts for unauthorized CPEs by analyzing their individual configurations. By first scanning the system, the SAA tool will mark it as safe if three distinct checks are passed: all required CPEs are present, no blacklisted CPE is present, and only one version of a CPE is installed at a time. Once marked as safe, this configuration is used for future comparison analysis, thus accounting for deviations between CPE configurations on different machines. While this particular tool concentrates on categorizing the CPEs, a next step mentioned in the paper is to "incorporate a scoring system such as CVE, NVD, and CVSS" [3] to assess overall vulnerability of network machines. We will take this emphasis on analyzing for CVEs and scan for such vulnerabilities, specifically concentrating on the BlueKeep vulnerability for the Windows operating system. Once we filter out and detect the vulnerable machines, we can then collect network addresses, site type, and similar holistic data to gather statistics for BlueKeep vulnerable environments in order to try to detect commonalities.

3. OUR ARCHITECTURE

Our tool will scan the network for vulnerable IPs by fingerprinting each OS, firstly by http header and secondly via methods including a TCP/IP/SYN method described by Han and Du (2010) [2]. We can then proceed to filter by open ports and finally by scanning the actual host for the BlueKeep vulnerability. This scan can consist of detecting the RDP is installed and then attempting a request/response comparison to check if the vulnerability has been patched or not. Once we have detected a BlueKeep vulnerable machine, we can then proceed to extract holistic data about our targets, including OS version, open ports, geographic location, among others. This data can then be used to aggregate common environment or network features which could give insight into the applicability, danger, and relevancy of BlueKeep.

4. EXPERIMENTAL RESULTS

For the chosen BlueKeep vulnerability, we expect to see a very wide range of vulnerable machines as the CVE is new and applicable only for older OS without a patch. At a count of almost 500k Windows systems still vulnerable as reported by Shodan, a number only half of the original release, we expect to find comparable ratios of vulnerable machines in our network scans. We also expect the detected machines to be running older websites, deprecated web stacks, and similar such dated software. Additionally, these machines should be more likely to have high numbers of other possible vulnerabilities due to update neglect indicated by the lack of a BlueKeep patch.

5. RELATED WORK

Since BlueKeep only targets Windows machines ranging from Windows Server 2008 to Windows 7, we need to properly fingerprint each IP's host machine to determine likely candidates for this vulnerability. However, the header fields in the http request/responses may not be accurate. To increase confidence and properly identify the host machine OS, we can use an approach described by Han and Du (2010) [2] which identifies OS by TCP/IP fingerprint. This paper uses a method in which a host can be fingerprinted via an open TCP port. The method described in this approach constructs a TCP packet, initiates a connection handshake protocol, and records the protocol fingerprints found in the TCP response header. Once recorded, the data gathered is used to compare the behavior with a database of OS fingerprints to accurately judge the host OS type and version.

Once the OS has been fingerprinted, the next step is to examine the system for the BlueKeep vulnerability. BlueKeep relies on RDP being installed on the host machine however, there are a few key indicators of vulnerability. The packet handling of RDP communications requires several modules, among them termdd.sys, a driver used to send mouse and keyboard actions. Upon further exploration, researchers discovered a channel named MS_T120 contained a vulnerability in which if a specially crafted packet is sent, the channel itself is freed. However, the pointer to the function is not freed and thus can be accessed on the channel, thus bypassing any prior authentication [4]. A scanner for BlueKeep can therefore bind this MS_T120 channel, send appropriate packets, and compare the output to that of a patched machine. If they differ, then the host can be classified as being vulnerable to BlueKeep [1].

6. CONCLUSIONS

7. REFERENCES

[1] S. Dillon. @zerosum0x0: reverse engineering, penetration testing, exploit development, May 2019.

[2] X. Han and X. Du. A new method about operating system identification. In *2010 2nd IEEE International Conference on Information and Financial Engineering*, pages 882–885, Sep. 2010.

[3] X. Li, P. Avellino, J. Janies, and M. P. Collins. Software asset analyzer: A system for detecting configuration anomalies. In *MILCOM 2016 - 2016 IEEE Military Communications Conference*, pages 998–1003, Nov 2016.

[4] Z. S. Research. Bluekeep and forthcoming rdp attacks, 2019.