OUR Journal: ODU Undergraduate Research Journal

Volume 7 *Special Issue: Interdisciplinary Cybersecurity Research*

Article 4

2020

Topical Review of Vulnerability Management for Local Hampton Roads Industry

Gregory W. Hubbard Jr.
Old Dominion University

Matthew Eunice
AECOM

Recommended Citation

Hubbard, Gregory W. Jr. and Eunice, Matthew (2020) "Topical Review of Vulnerability Management for Local Hampton Roads Industry," *OUR Journal: ODU Undergraduate Research Journal*: Vol. 7 , Article 4.
DOI: 10.25778/41cp-yf83
Available at: https://digitalcommons.odu.edu/ourj/vol7/iss1/4

Topical Review of Vulnerability Management for Local Hampton Roads Industry

Cover Page Footnote

This work was supported in part by the Center for Cyber security Education and Research (CCSER), Old Dominion University, and the National Science Foundation (NSF). Gregory Hubbard is with Old Dominion University, Norfolk, Virginia (ghubb002@odu.edu) under the supervision of Matthew J Eunice, Cybersecurity Manager, AECOM. Under the guidance and expertise of my mentor Matthew Eunice of AECOM, I conducted this particular topical study of current software vulnerability management. This cyber security research was supported by empirical data collected through relevant experimental protocol. Future research could easily be amended to this particular study due to the scalability of the topic. Furthermore, a comprehensive report and poster is included, covering experimental results and current management techniques.

TOPICAL REVIEW OF VULNERABILITY MANAGEMENT FOR LOCAL HAMPTON ROADS INDUSTRY

By Greg Hubbard[*] and Matthew Eunice

NOMENCLATURE

CVE – Common Vulnerabilities and Exposures

I. INTRODUCTION

Cyber security can be summarized as a two-party strategic battle between attacking "threats" and defending networks/systems. Cyber threats are constantly evolving to exploit weaknesses in cyber systems. Once manipulated, a threat (e.g. virus) can have devastating monetary or physical effects. To counteract these threats, defense involves the independent patching and constant update of used systems. Specifically, the study of vulnerability management concerns the prediction and identification of potential areas of cyber attack.

II. HISTORY OF CYBER SECURITY AWARENESS

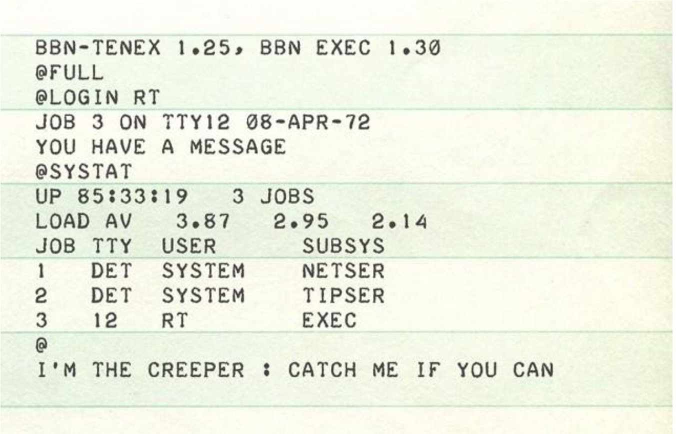
The principles of electronic hacking first began in the late 1800's as innocuous practical-joke-manipulating phone calls ("History of Hacking"). These pranks usually consisted of tinkering

[*] This research is supported in part under NSF grant DGE-1723635.

with telephone switchboards, which could disconnect or misdirect calls. One of the first “hacks” recorded was reported by Bell Telephone in 1878 when a group of teenage boys hired to operate switch boards intentionally interfered with calls (“History of Hacking”).

Nearly 80 years later, the first authentic computer hackers began to “hack” using witty shortcuts to compute tasks quickly. At this time, the audience for computational design was primarily a tight knit community of computer engineers and related fields. These early pioneers in programming had to adapt to specific hardware mainframes for software development. Additionally, functional tooling that we take for granted in today’s programing environment, for example, “Save function, copy function, paste function,” occasionally failed, thereby resulting in loss of full days of work. Due to these primitive issues, computer engineers in the 1960’s were trained to become very innovative in their development. One of these innovations was created by two employees of Bell Lab, Dennis Ritchie and Ken Thompson, called UNIX. This “shortcut” hack was used to act as an open set of rules to run machines on a large scale ("The History of Cyber Security - Everything You Ever Wanted to Know", 2019).

The modern history of cybersecurity has evolved alongside network development dating back to the 1970’s. Bob Thomas at Bolt, Beranek, and Newman Inc. realized it was possible to spread programs across a network in 1971. An experimental program developed for the ARPANET was used to print the message “I'M THE CREEPER: CATCH ME IF YOU CAN” across the network.



```
BBN-TENEX 1.25, BBN EXEC 1.30
@FULL
@LOGIN RT
JOB 3 ON TTY12 08-APR-72
YOU HAVE A MESSAGE
@SYSTAT
UP 85:33:19   3 JOBS
LOAD AV   3.87   2.95   2.14
JOB TTY  USER      SUBSYS
1   DET  SYSTEM    NETSER
2   DET  SYSTEM    TIPSER
3   12   RT        EXEC
@
I'M THE CREEPER : CATCH ME IF YOU CAN
```

Fig. 1. Creeper program example output shown. Notice the tail of the program "I'm the creeper : catch me if you can" (http://corewar.co.uk/creeper.htm).

"CREEPER is a demonstration program which can migrate from computer to computer within the ARPA network while performing its simple task."

-Thomas, Robert H. Distributed Computation Research at BBN Dec 1974.

The CREEPER program was an experimental self-replicating program destined to demonstrate a mobile application. Ray Tomlinson, a colleague of Bob Thomas, recognized (perhaps unintentionally) the dangers of a self replicating "Creeper." He created a companion program coined "Reaper" which was designed to terminate instances of "Creepers" on the ARPAnet ("Core War: Creeper and Reaper").

Thus, if Creeper is considered the first network-based virus, Reaper was the first anti-virus software. This prospect of two programs actively spawning and eliminating each other inspired A. K. Dewdney's Core War, with "two programs doing battle in the dark and noiseless corridors of core" (Dewdney, 1984).

History of Cyber Security Awareness

Though the first computers were engineered in the 1930s, everyday computers were first developed in the 1980s. The release of IBM's 5150 Personal Computer revolutionized the technological world ("The Evolution of Technology in the Classroom", 2017). Between the years 1980 and 1986, the number of computers used in the United States increased from around one million to over 30 million units ("History of Hacking"). At this time, the concept of interfering or "hacking" was a very foreign topic. In 1983, however, a movie called "War Games," brought popularity to the idea of hackers operating on a grand scale ("History of Hacking").

Awareness Over The Past 10 Years

Today, nearly everyone is accustomed—at least to the premise—of computer viruses; however, the magnitude of danger is oftentimes overlooked. According to the Microsoft Security Intelligence Report, 40% of households in the United States are infected by malware. The estimated cost of all individual users can be estimated to be around $4.55 billion. Despite these shocking statistics, cyberspace is still a non-cooperative dynamic environment for both personal and organizational workers alike.

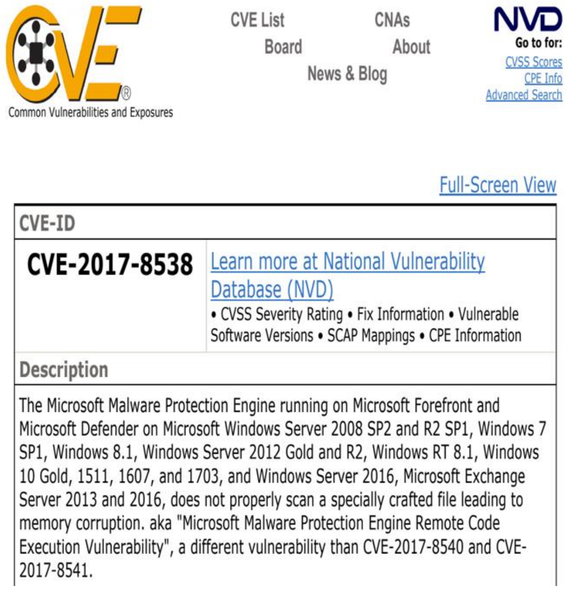
III. PREVENTING CYBER ATTACKS

Prevention Practice

Cyberattacks are often opportunistic responses to vulnerabilities in computer defenses. A vulnerability by definition is “the quality or state of being exposed to the possibility of being attacked or harmed.” In the field of cybersecurity, a vulnerability is a weakness in a system’s design that may potentially allow malicious entry. Common vulnerabilities are documented in the Common Vulnerabilities and Exposures (CVE) database. Automated tools are used to look for vulnerabilities under the process of vulnerability scanning. These scans search for issues in a system that could lead to backdoor, denial-of-service, direct-access, eavesdropping, polymorphic, phishing, privilege escalation, social engineering, spoofing, or tampering attacks.

CVE Database

The Common Vulnerabilities and Exposures (CVE) provide a dictionary set of known security vulnerabilities and exposures. In the field of vulnerability management, CVE has become the de facto standard for uniquely identifying vulnerabilities (Adinolfi, 2017). Individual vulnerabilities are correlated with a specific ID and are labeled with correlating information between security protocols and services. Due to the fluid nature of cyber vulnerabilities, the CVE can never preemptively predict a source vulnerability (Adinolfi).



CVE-ID	
CVE-2017-8538	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information
Description	
The Microsoft Malware Protection Engine running on Microsoft Forefront and Microsoft Defender on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016, Microsoft Exchange Server 2013 and 2016, does not properly scan a specially crafted file leading to memory corruption. aka "Microsoft Malware Protection Engine Remote Code Execution Vulnerability", a different vulnerability than CVE-2017-8540 and CVE-2017-8541.	

Fig. 2. Sample CVE database entry shown. Notice the specific CVE-ID (CVE-2017-8538).

http://corewar.co.uk/creeper.htm

Scanners

Inspection of "weaknesses" in a computer system is conventionally done by automated scanners. Scanners are computer programs designed to search for known flaws using a dictionary set (e.g. CVE). The key point of the scanner is best summarized by Cristian Florian, Product Manager at GFI Software, who remarks that:

> A vulnerability scan outlines the gates that malware can use to reach the network. Some of these gates are easy to detect and remediate because they are represented by vulnerabilities that have been disclosed to the public and for which a security update is available. In this case all that's necessary to close the vulnerability is to apply the security patch. However, vulnerability scanning also outlines security misconfigurations, open ports, running services, open shares and other security sensitive information that

collectively help administrators to detect and close unnecessary services in order to minimize the attack surface and provide protection from zero-day exploits.

GFI LandGuard

GFI LanGuard is a proprietary scanning software designed for the Network Security on small to medium-sized business. Once initialized, the GFI LanGuard scans each IP in the local network. While scanning, LanGuard automatically detects specific vulnerabilities on the network. Specifically, the scanner reports information on service level of the machine, security patch information, wireless access points, USB devices, key registry entries, weak passwords, and other relevant security solutions.

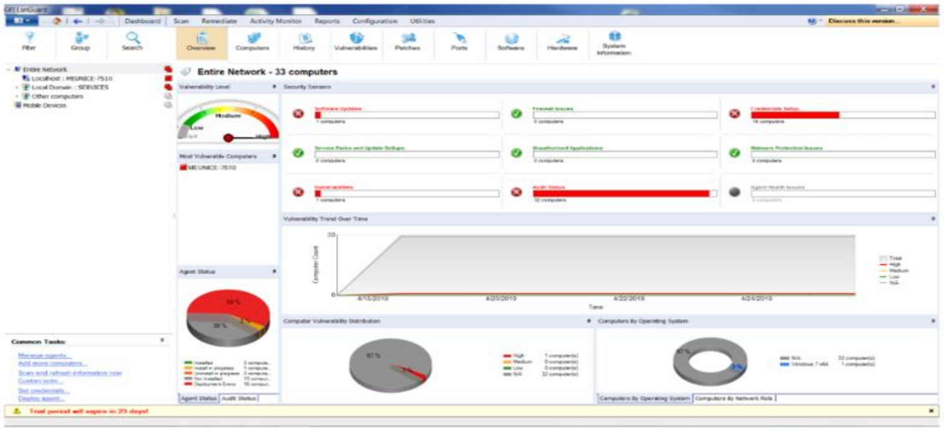


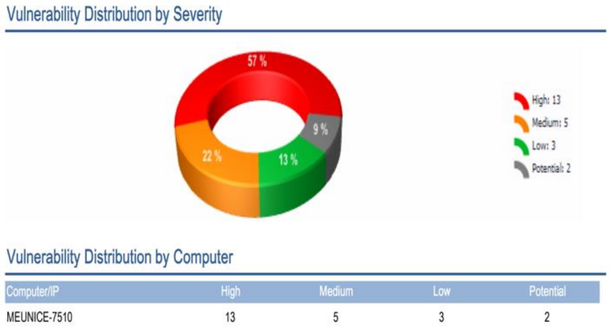
Fig. 3. Sample GFI LandGaurd Scan shown. Note that the network scanned is at high danger of exploitation based on automated scan.

Network Scan Example

In industry practice, the vulnerability management processes shown above can be briefly consolidated into the steps shown below. An executive report showing network vulnerability levels, most vulnerable computers, agent status, vulnerability trends, and additional relevant information on operating systems is displayed by the first scan of GFI LanGuard.

Vulnerability Status Test

Using a single workstation as an example host for vulnerabilities, the practice of identifying potential threats can be clearly seen.


Vulnerability Distribution by Severity

Vulnerability Distribution by Computer

Computer/IP	High	Medium	Low	Potential
MEUNICE-7510	13	5	3	2

Fig. 4. Sample GFI LandGaurd Scan for local network labeled (MEUNICE-7510)

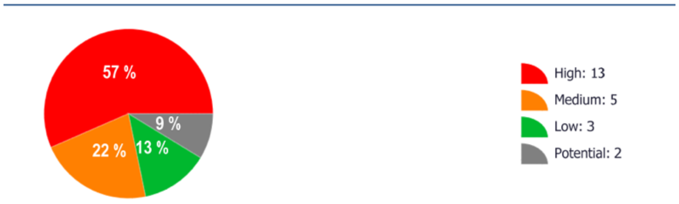


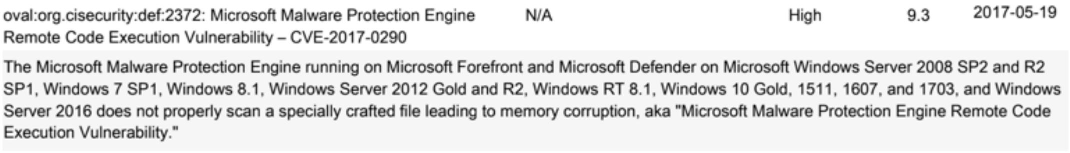
Fig. 5. Sample GFI LandGaurd Scan with threat resolution shown in a pie diagram.

This initial portion of the GFI LandGard scan offers the user a clear understanding of the severity of threats on the network. The classification of vulnerability concerns adheres to their Common Vulnerabilities and Exposures (CVE) database itemization. The classification of high, medium, low, and potential vulnerabilities are enumerated by CVSS according to CVSS documentation version 3.1.

Rating	**CVSS Score**
None	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10

Fig. 6. Enumerated CVSS scores using Ratings vs. CVSS Scores.

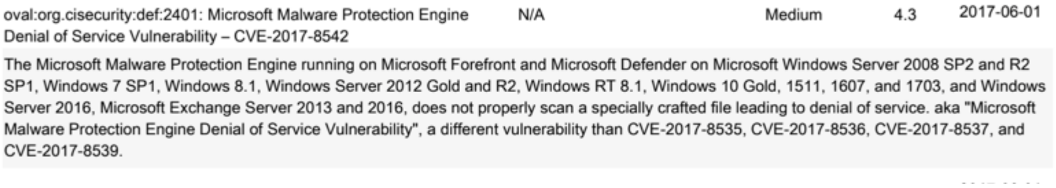
A vulnerability description of respective high (13), medium (5), low (2), and potential (2) issues are shown below:



oval:org.cisecurity:def:2372: Microsoft Malware Protection Engine Remote Code Execution Vulnerability – CVE-2017-0290	N/A	High	9.3	2017-05-19

The Microsoft Malware Protection Engine running on Microsoft Forefront and Microsoft Defender on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 does not properly scan a specially crafted file leading to memory corruption, aka "Microsoft Malware Protection Engine Remote Code Execution Vulnerability."

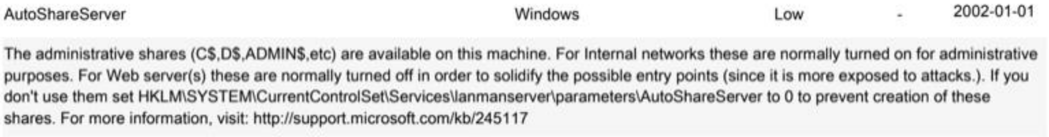
Fig. 7. High ranking (9.3) vulnerability found on test station



oval:org.cisecurity:def:2401: Microsoft Malware Protection Engine Denial of Service Vulnerability – CVE-2017-8542	N/A	Medium	4.3	2017-06-01

The Microsoft Malware Protection Engine running on Microsoft Forefront and Microsoft Defender on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016, Microsoft Exchange Server 2013 and 2016, does not properly scan a specially crafted file leading to denial of service. aka "Microsoft Malware Protection Engine Denial of Service Vulnerability", a different vulnerability than CVE-2017-8535, CVE-2017-8536, CVE-2017-8537, and CVE-2017-8539.

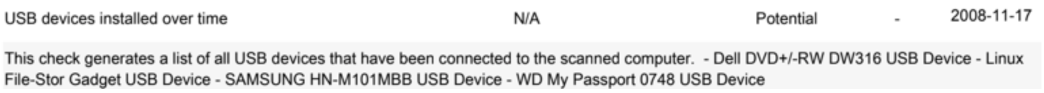
Fig. 8. Medium ranking (4.3) vulnerability found on test station



AutoShareServer	Windows	Low	-	2002-01-01

The administrative shares (C$,D$,ADMIN$,etc) are available on this machine. For Internal networks these are normally turned on for administrative purposes. For Web server(s) these are normally turned off in order to solidify the possible entry points (since it is more exposed to attacks.). If you don't use them set HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\AutoShareServer to 0 to prevent creation of these shares. For more information, visit: http://support.microsoft.com/kb/245117

Fig. 9. Low ranking (NA) vulnerability found on test station



USB devices installed over time N/A Potential - 2008-11-17

This check generates a list of all USB devices that have been connected to the scanned computer. - Dell DVD+/-RW DW316 USB Device - Linux File-Stor Gadget USB Device - SAMSUNG HN-M101MBB USB Device - WD My Passport 0748 USB Device

Fig. 10. Potential (NA) vulnerability found on test station

In practice, the given classification of vulnerabilities reflects only a loose assessment of actual issues. The enumerated classification of vulnerability depends on the value of the system. For example, a critical vulnerability on a low value asset will often rank lower than unimportant vulnerability on a high value asset. The CVSS ranking takes into account the fluid nature of such vulnerabilities.

AWARE Program

Beginning in 2020, the US government will mandate an enforced cyber vulnerability analysis on all government agencies (Nycezepir, 2019). This mandate will rank agencies based on an algorithm calculated according to the number of scanned vulnerabilities, unpatched configurations, and overall cyber hygiene reports. This algorithm is appropriately coined AWARE or Agency-Wide Adaptive Risk Enumeration. Kevin Cox, the current program manager of Homeland Security's Department of Continuous Diagnostic and Mitigation, claims that the AWARE initiative will allow governing officials "to have a scale as to what agencies are doing well, what agencies might need some additional support, and help get us a sense of one of the most important factors in combating the threat: basic cyber hygiene—getting things patched, getting things configured (Nextgov, 2018)."

Bridge to The Community

While the federal security is the foremost concern of a nation, related layaways must be embedded in the community. Hampton Roads has always been a region heavily dependent on government contracts. While this symbiotic relationship is incredibly vested in the community, local businesses must be prepared to act independently as the federal procurement dwindles. Small businesses must be given specific attention as they lack the outstanding infrastructure and resources given to large corporations. To make matters worse, Hampton Roads is currently facing an extreme shortage of cyber security workers. Larry Filer, associate professor of the Economics Department at Old Dominion University states, "[local] companies often need to look outside the state and region to fill open positions (Carballo, 2018)." According to *The Virginian Pilot*—the local press newspaper—Hampton Roads is faced with a dynamic issue with filling cyber security jobs in the private sector due to a low supply of workers and low cyber industry awareness (Carballo, 2018). This incredibly high demand for knowledgeable workers has forced local companies to employ university students in positions normally reserved for candidates with years of experience.

IV. Conclusion

Software vulnerabilities provide a constantly evolving threat for computer systems. Due to the cyclical nature of vulnerabilities, it is imperative to understand the current management of such threats in anticipation for the future. In a topical overview of a local Hampton Roads cyber management group, the importance and methodologies of vulnerability management are summarized. Specifically, this overview covers the joint usage of both the CVE database and the GFI Landguard scanner.

Acknowledgment

This work was supported in part by the Center for Cyber Security Education and Research (CCSER), Old Dominion University, and the National Science Foundation (NSF).

Gregory Hubbard is with Old Dominion University, Norfolk, Virginia (ghubb002@odu.edu) under the supervision of Matthew J Eunice, Cybersecurity Manager, AECOM.

Under the guidance and expertise of my mentor Matthew Eunice of AECOM, I conducted this particular topical study of current software vulnerability management. This cyber security research was supported by empirical data collected through relevant experimental protocol. Future research could easily be amended to this particular study due to the scalability of the topic. Furthermore, a comprehensive report and poster is included, covering experimental results and current management techniques.

References

Adinolfi, Daniel. “CVE IDs and How to Get Them.” https://Cve.mitre.org/CVEIDsAndHowToGetThem.pdf, 2017.

Carballo, Rebecca. “Hampton Roads Struggles to Fill Cyber Security Skill Gap.” The Virginian-Pilot, 14 July 2018.

“Core War: Creeper and Reaper.” Creeper & Reaper, corewar.co.uk/creeper.htm.

Dewdney, A. K. "Computer Recreations: In a game called core war hostile programs engage in a battle of bits." Scientific American (May 1984): 14–22.

“History of Hacking,” plaza.ufl.edu/ysmgator/projects/project2/history.html.

“Microsoft: Microsoft Security Intelligence Report,” Volume, July through December 2013. https://crypto.stanford.edu/~dabo/cs55N/MSIR.pdf.

Nextgov. Agencies Will Soon Have a Cyber Hygiene Score-And Will Know Where They Rank,2018, brica.de/alerts/alert/public/1238534/agencies-will-soon-have-a-cyber-hygiene-scoreand-will-know-where-they-rank/.

Nyczepir, Dave. “This Agency Is Preparing to Score Its Cyber Risk with a New Algorithm.” FedScoop, FedScoop, 26 Apr. 2019, www.fedscoop.com/cyber-risk-aware-algorithm/.

“The Evolution of Technology in the Classroom.” Purdue University Online, 1 Aug. 2017, online.purdue.edu/ldt/learning-design-technology/resources/evolution-technology-classroom.

“The History of Cyber Security - Everything You Ever Wanted to Know.” SentinelOne, 16 Apr. 2019, www.sentinelone.com/blog/history-of-cyber-security/.

Thomas, Robert H. Distributed Computation Research at BBN. Massachusetts: Bolt, Beranek and Newman Inc, Dec 1974.