Cat Scan Vulnerabilities

Executive Summary

In this document, we will go over the findings of the network scan and the vulnerabilities that have been discovered on the network. Using the greenbone application to run a network wide scan, we can run a scan on all the devices connected to the network to discover vulnerabilities. When finding these vulnerabilities we can then form mitigation responses to remedy the vulnerabilities. For the purposes of this report, we will be looking into 3 different types of vulnerabilities to the network, ranging from high priority to low priority, to fully understand the steps that need to be taken to secure the network further.

Scan Results

The vulnerability scan on Greenbone, shows multiple vulnerabilities across the network, that consists of one windows workstation, one linux server, and one windows server. After an hour of letting the scan run across the network, The windows workstation presented 4 vulnerabilities, the windows server presented 6 vulnerabilities, and the linux server presented 8 vulnerabilities. Amongst the vulnerabilities we can also see from the scan other information like, the information of all the devices that were scanned on the network, such as the IP addresses, open ports on a machine which can lead to more vulnerabilities, along with several other bits of information that help in identifying vulnerabilities. For this document we will focus on the vulnerabilities that are open to malicious attackers to exploit, using the identifiers known as CVE numbers (Common Vulnerabilities and Exposures). These numbers from the National Vulnerability Database (NVD) will show us the general calculations for severity, but we will recalculate them to better suit the company and its needs.

Methodology

First of all, to run Greenbone on the kali system, we first must run a command to run the OpenVAS program on kali. OpenVAS is a vulnerability scanner that will run any type of scan on a network with specified parameters, for this scan we will run a deep scan to find out every bit of information and vulnerability we can find. The command we will run is “sudo gmv-start” sudo to access admin privileges, and gmv-start to enable the vulnerability scanner. This will take us into the Greenbone application. After going into Greenbone, we then head over to the scans tab to set up a new scan with the target being the network “172.16.14.0/24” which will run the scan and after it is done, we will see all the information it has gathered. The next step is to look at the vulnerabilities in question. After picking our example vulnerabilities, we will then enter their impacts into a Common Vulnerability Scoring System (CVSS) calculator which will help us tailor the impact levels on how if the vulnerabilities would be exploited, how badly it would impact the company, its functionality, and its privacy.

Findings

There are other vulnerabilities that the scan did reveal, but the vulnerabilities shown below have Common Vulnerability and Exposure (CVE) numbers. As stated before these numbers are used in the National Vulnerability Database (NVD) for easier research.

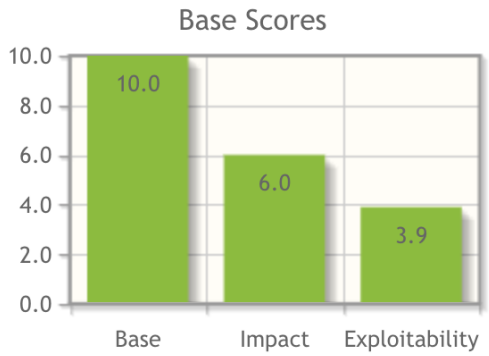
CVE	NVT	Hosts	Occurrences	Severity ▼
CVE-1999-0501 CVE-1999-0502 CVE-1999-0507 CVE-1999-0508	HTTP Brute Force Logins With Default Credentials Reporting	1	1	7.5 (High)
CVE-2013-2566 CVE-2015-2808 CVE-2015-4000	SSL/TLS: Report Weak Cipher Suites	1	1	5.0 (Medium)
CVE-2011-1473 CVE-2011-5094	SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)	1	1	5.0 (Medium)
CVE-2011-3389 CVE-2015-0204	SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	2	2	4.3 (Medium)
CVE-1999-0524	ICMP Timestamp Reply Information Disclosure	7	7	2.1 (Low)

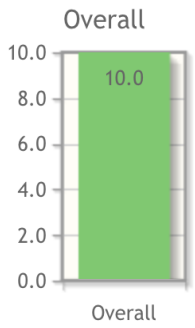
pplied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity) 1 - 5 of 5

Along with these vulnerabilities the scan produced the discoverable systems on the network, the scan has provided the ip addresses, operating systems, (OS) and their versions, all except for the kali system, as it is running the scan from that machine it will not appear on the scan. Kali as a linux system specializing in cyber security and security monitoring, Kali also has built in protection to deny access to any type of scan that would provide confidential data, or any type of data that would compromise the system.

Risk Assessment

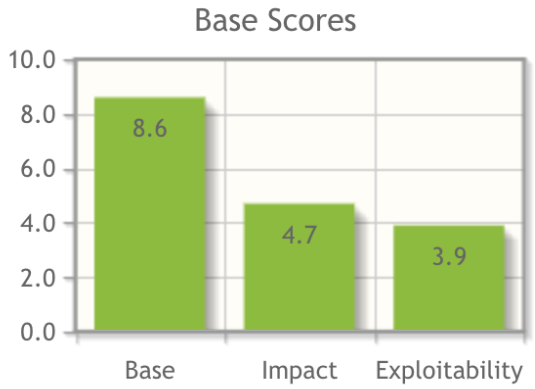
The first risk we will take a look at is what Greenbone has categorized as a high risk at a 7.5 (high) score, the Brute Force attack. The general information given to this type of vulnerability defines the impact of the attack to be low or partial in terms of what types of information is accessed as well as the ability for the machines to run. The adjusted scores that reflect more on the company show that any data breach would result in a greater impact as they would be dealing with sensitive user data, as well as disrupting the access to the machine. The new adjusted scores are at a score of a 10 (high), the impact it would have is a 6 (medium) and exploitability is shown at a 3.9 (low). Compared to the other 2 vulnerabilities we will discuss, this vulnerability has the most impact and most effect on the network if exploited. The screen capture below shows the data charts of the score and where they stand compared to each other.

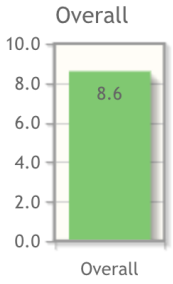




CVSS Base Score: 10.0
Impact Subscore: 6.0
Exploitability Subscore: 3.9
CVSS Temporal Score: NA
CVSS Environmental Score: NA
Modified Impact Subscore: NA
Overall CVSS Score: 10.0

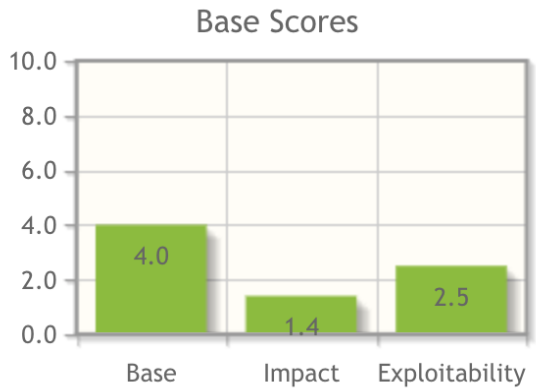
The next vulnerability is categorized as a 5.0 (medium) vulnerability according to NVD, but when specified to the companies assets using the CVSS calculator, we then get a score of 8.6 (high). This vulnerability is a Denial of Service (DoS) attack. This type of attack utilizes a lot of data requests to a server weaponizing them attempting to overwhelm the network and effectively shut down the network's ability to function. As a security company a denial of service would be a major detriment to the security services provided and used to monitor our own network. Keeping all of these consequences in mind, we can then enter our values into the CVSS calculator which gives us a score of 8.6 (high), the impact it would have is a 4.7 (medium) and exploitability is shown at a 3.9 (low). Once again the charts will be shown below.

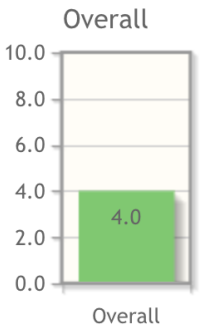




CVSS Base Score: 8.6
Impact Subscore: 4.7
Exploitability Subscore: 3.9
CVSS Temporal Score: NA
CVSS Environmental Score: NA
Modified Impact Subscore: NA
Overall CVSS Score: 8.6

The last vulnerability we are going to take a look at leads to an attack called an Internet Control Message Protocol (ICMP) timestamp reconnaissance attack. This type of attack uses the timestamps of certain machines in order to understand any time based algorithms linked to the machine, such as time based security measures in place to authenticate a user. The score given to this type of attack is a 2.1 (low) vulnerability. When inserting the specifications of the company, we get a score of 4.0 (low) as well. The score is slightly higher, but there is no change in urgency of mitigation. The attacker does not gain any sort of access or denial of service from this type of attack, and therefore it would not need an immediate remedy. If left unchecked for too long it could be scored higher eventually as any time based algorithms on the company's network could then be exposed and used in a separate attack. Charts provided below.





CVSS Base Score: 4.0
Impact Subscore: 1.4
Exploitability Subscore: 2.5
CVSS Temporal Score: NA
CVSS Environmental Score: NA
Modified Impact Subscore: NA
Overall CVSS Score: 4.0

Recommendations

The mitigations for each vulnerability are relatively simple to implement as well as cost effective, as they will not require many external resources to secure the vulnerabilities from being exploited, they also offer monitoring services to set thresholds as well as warnings for any Indicators of Compromise (IoC's). The first mitigation for the most prevalent issue is the brute force attack shown in the first section of the 'risk assessment' section. The brute force attack utilizes its best use on machines that have little to no password protection, hence the "Brute Force logins with Default Credentials" name. This means ensuring each user has password protected accounts is the best form of mitigation for this type of attack. Industry best practice also suggests setting up any type of Multi-factor Authentication (MFA) methods or 2 Factor Authentication (2FA) methods, to even better secure user accounts from being accessed by an unauthorized user. This includes things like Captcha puzzles, or sending a verification email for example.

The second mitigation method is for the Denial of Service (DoS) attack. The best form of mitigation for this type of attack is to monitor the traffic being sent to the network using tools such as PRTG and applying a sensor to monitor network traffic, for example 'MySQL' sensor. The industry best practice is to use these types of sensors to monitor what normal traffic to the network looks like, then set thresholds that would exceed that normal traffic in the case where the traffic exceeds the threshold, the sensor would send a warning to notify the security team. This action of installing a monitoring tool will help response times against a DoS attack, and to help prevent them from fully denying network services.

The last mitigation method which can be implemented simply by applying a firewall that blocks timestamp requests. This denies the attacker the ability to send timestamp requests on the Internet Message Control Protocol (ICMP) layer, as it blocks incoming and outgoing requests, and is an industry best practice.

Work Cited

***NVD CVSS*. NVD. (n.d.). https://nvd.nist.gov/vuln/search**

CVE security vulnerability database. security vulnerabilities, exploits, references and more. CVE security vulnerability database. Security vulnerabilities, exploits, references and more. (n.d.). https://www.cvedetails.com/

***ICMP timestamp response and request vulnerability fix: Beyond security*. Vulnerability Security Testing & DAST | Beyond Security. (2023, February 6). https://www.beyondsecurity.com/resources/vulnerabilities/icmp-timestamp-request**

***You are viewing this page in an unauthorized frame window.* NVD. (n.d.). https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator**