|  |  |
| --- | --- |
| -rw-rw-r-- 1 giac giac 4.0k Jun 26 11:46 | This file in the directory would considered suspicious. |
| ./configure | This command will generate a makefile that is tune to the system that it is installed to. |
| /usr/share/wordlists | Worlists location in Kali |
| &giac | Used to access the address of a variable in the C programming language. |
| # | This indicates the text after it, is a comment |
| 2nd\_phone\_number | This variable will cause python to produce an error. |
| 755 | Allows the owner of a file to read, write, and execute a file while allowing everyone else to read and execute. |
| A client side attack that targets users that are browsing the site. Typically occurs in areas of the site where users input information | Cross site script attack |
| A directory traversal attack is an injection of directory code to try and navigate to a specific directory / file on a computer | Directory traversal attack |
| A flaw in a web application that takes advantage in how a web application process user input | Command injection |
| A flaw where the user can upload an arbitrary file to the server and then visit it to execute code | File upload vulnerability |
| A form of encryption that uses a public and private key to encrypt a message. | Asymmetric encryptions. |
| A hidden share on a remote host | \\fileserver2\network\_tools\software$ |
| A legal dept, HR, and the accounting dept | Phishing attacks strikes the most. |
| A penetration testing tool used to automatically execute exploits against targeted systems | Metasploit |
| A phishing attack but you have a specific target in mind for the attack | Spear phising. |
| A protection that involves randomizing the Memory address that a program gets loaded into each run | Address space layout randomization. |
| A result of adding resources on a page based on user input | Inclusion attack |
| A type of injection attack wherein the attacker exploits the web application to send unauthorized commands to a backend database server | SQL injection attack |
| A utility designed to create a binary or hexadecimal number that represents the uniqueness of a data set, such as a | Hashing algorithm |
| A Vulnerability Scanner | Used to test Web applications. |
| A word doc that can host malware | Word Macro |
| Adding www-data user to the server's administrator group | This will cause a permissions issue on an Apache web server. |
| After the patch was released | Is when you go public with a vulnerability found within a business website. |
| Always notify | This is one of 4 User Account Control (UAC) setting on a windows system. |
| An attack that relies on an attacker cloning a site and hosting it to have a user logging into and stealing their credentials | Credential harvesting attack |
| An email that encourages people to click on malicious links or download malicious files | Phishing |
| An encryption has an encryption key while encoding does not | Difference between encryption and encoding. |
| An encryption that uses the key to decrypt and encrypt a message | Symmetric encryption. |
| An encryption where the mathematical calculations are open to the public | This makes an encryption strong. |
| An interactive console will open for writing simple Python code | This will happen when you run the command “Python” on a Linux system where it is installed. |
| Asymmetric and symmetric | This is a form of encryptions that HTTPS uses. |
| Authentication, integrity and non-repudiation | Provided by encryption |
| Availability | This are the risks areas targeted by DDos. |
| Because you should never use applications or tech that is no longer supported from developers | End of support for applications or technology. |
| Buffer Overflow | Vulnerability within the FTP Service. |
| Canary | This is a buffer overflow mitigation and it places a value before the return pointer in the stack. |
| cd ~ | This command will change your directory to the current home folder. |
| Checking that the result of any change to a signed integer falls within an allowed range | The only way to mitigate an integer overflow/underflow. |
| Clickjacking | The admin has configured the option to use the values DENY,SAMEORGIN, or ALLOW-FROM. |
| Closing and reopening the terminal | This action will cause the updated $PATH variable change back to the original value. |
| CodeMeter Runtime Server  C:\Program Files (x86)\CodeMeter\Runtime\bin\CodeMeter.exe | This is an unquoted service path and it could be a target for privilege escalation. |
| Command injection | This happens when an exploit takes advantage of a web-page field that does not validate input. |
| Command injection | An attacker enters “cat/etc/passwd” into a filed on a website, this flaw would allow the input to be executed by the web server’s operating system. |
| Commit | This is when a user makes a change to the master code in a Git Repo. |
| CPU | Data from the GBD output is stored on the host. |
| Create users within Windows, create groups within Windows, Change your password | Local users management console. |
| Cross site request forgery | You can mitigate this by a web application configures to validate a unique token value for each submitted user request. |
| Cross Site request forgery | This can be mitigated when a web application is configured to validate a unique token for each submitted user request. |
| Daemon | This component of Docker builds, runs and deliver containers. |
| Data Link | An address would be used at this OSI layer. |
| Debugger | Tool that an attacker uses to identify potentially exploitable functions in a program and their memory address locations. |
| Deny, Same Origin, and Allow-FROM | # values within an X-Frame option header in an HTTPS response |
| Destroy data | Is how you remove data from a solid state drive. |
| DHCP | Protocol used to obtain an IP address. |
| Disable the banner | This is how Apache server administrator prevents version information from leaking. |
| docker images | This command is used to generate a list of images that are store locally and provides arguments for handling them. |
| Encryption is the process of converting data from one form to another | Encryption. |
| exFAT | Storage systems in USBs |
| Exploiting Services, Exploiting the Kernel, SUID Files | Some of the ways to perform privilege escalation. |
| export | This command will set or modify an environment table. |
| File Inclusion | Type of vulnerability illustrated where the code is in the webpage. |
| Find a flaw in the encryption and to guess the encryption key that was used | This are 2 ways to break encryption |
| Firewall | Likely a source of logs for HTTP network traffic data. |
| Gaining a shell with root access | Using this Linux command. sudo find /etc -exec sh -i /; |
| Generates a software interrupt | The users starts Microsoft Word and clicks file 1 open. |
| Get-Content aliases.ps1 | This PowerShell command string will display the contents of the file aliases.ps1. |
| Harder for attackers to overwrite logs | Benefits of moving from local logging to using a log server provided organizations. |
| Hashing | This is a form of one-way encryption. |
| HEAD | Is an HTTP protocol requests that asks a web server to retrieve metadata without the data. |
| HKLM\System\CurrentControlSet\Services | This is where you check if malware is launching with local administrator privileges when the compromised host starts and persist with each reboot. |
| Hypervisor | Software or firmware platform that host a virtual machine. |
| ICMP echo requests with varying data field sizes | This packet header file characteristic is a strong indicator of data exfiltration. |
| Identifies the output format for data at address ox80448ef | Debugging a program with pwngdb. |
| Identify services running on network hosts | An alert indicates that a compromised host was used by an attacker to run a command like $ nmap -sS 192.168.10.0/24 |
| Identifying open ports that could be used to compromise a host | # nmap -vv -sS -p- 10.10.1.1 |
| Image | This is a recipe for building docker containers. |
| IMAP | This protocol is used to access email on an email server. |
| In a GET Request | User agent used, found in the HTTP protocol. |
| In a GET Request | If the user agent is used, this would be found in the HTTP protocol |
| Input is not properly restricted by an application and is exploited by an attacker to run code of the attacker's choosing | Buffer overflow. |
| Integrating a branch into the main code | Code management platform used pull requests for this purpose. |
| It is a value that sits before the return pointer of the stack. | Stack Canary |
| It is to not use user input when making file system calls | Best way to mitigate a directory traversal attack. |
| It is to not user an insecure method of passing queries to the database | Best way to mitigate SQL injection |
| It occurs when you run printf in C without a format string | Format string vulnerability |
| Kali Linux | Is used when running Metasploit. |
| Kernel | It is a computer component that manages the ongoing access to a computer’s shared RAM and drive storage resources. |
| Kernel | If malicious software (malware) infects a computer, this is where it will require the most effort the detect and remove. |
| Lessons Learned | Stage of the incidence response where the adequacy should of the policy be exanimated. |
| List of secure shell processes running under the root user | ps aux | grep -i sshd | grep root |
| Local Users Management Console | Windows configuration utility that can be used by a local administrative user to create an account which requires the password to be reset upon first login. |
| Make sure every HTTP request submitting a form or any other kind of input comes from the same origin Use a Cross Site Request Forgery Token which is required by every form or input on a site | Best way to mitigate a Cross site request forgery |
| Make sure that the web server itself sends the X-Frame Options header in the HTTP response | Best way to mitigate clickjacking attack. |
| Metadata | A type of artifact that a blue team member can use to identify the name that is associated to the file. |
| Methods | This is the name given to the behaviors that objects have in a object oriented programming. |
| net user kirk | This command string will display information about the “kirk:” user on a windows system. |
| Never use printf without a format string | Best way to mitigate a format string vulnerability. |
| Nmap | A tool used to fingerprint the operating system of a host. |
| Non-repudiation | This feature tells an investigator that they know a specific message was sent leaking proprietary information because of the type of encryption used by the suspect to protect it. |
| Notifies users of software installation | Default setting for user account control (UAC) that improves windows security. |
| Parent Folder | A new file is created inherits this permissions. |
| PNW\_states = [ 'Washington' , 'Oregon' , 'Idaho' , 'Montana' , 'Wyoming' ]  print(PNW\_states[1]) | Oregon |
| Posing as a figure higher up in order to get an employee to perform wire transfers via electronic communication | CEO fraud |
| Process | When a program runs on a computer, it temporarily loads code into memory that contains information about the program. The code is then deleted when the program is closed. |
| Program assumes that a value is always positive, overflow makes signed integer wrap and become negative | Integer overflow |
| Query language is kept separate from user supplied data | This is how prepared statements help prevent SQL injection attacks |
| RCE | CVE-2019-9874: Deserialization of Untrusted Data in the Sitecore.Security.AnitCSRF (aka anti CSRF) module in Sitecore CMS 7.0 to 7.2 and Sitecore XP 7.5 to 8.2 allows an unauthenticated attacker to execute arbitrary code by sending a serialized .NET object in the HTTP POST parameter \_\_CSRFTOKEN. |
| Redirect the scanner to the same page in a loop | A Captcha do to a scanner |
| Registry | Windows database of setting for both the operating system and applications. |
| Registry Key | HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run |
| Resend the entire packet | Computer A sends 20 bytes of data Computer B responds with Computer A's acknowledgment number + 15 |
| robots.txt | Web server used to tell search engines to avoid certain locations. |
| robots.txt | This file is located in the root of the website and contains a list of web pages that should be omitted from a search engine spidering. |
| RST | Packet that is used when a graceful TCP teardown fails. (Abruptly) |
| runlevel | Linux command that shows the mode that the operating system is currently running under. |
| Runs multiple chunks of code concurrently | Computer program “multi-threaded” |
| Search for directories not linked to public areas of a website | root@kali: ~/target# dirb https:www.sans.org /usr/share/wordlists/dirb/small.txt |
| Search for subdomains based upon the wordlist provided | dnsmap myfakedomain.local -w /usr/share/wordlists/dnsmap.txt |
| Sending a website user's session cookie to an attacker | Common result of a reflected cross-site scripting attack. |
| SGID set | find / -per -2000 -user root -type f -print 2>/dev/null |
| SHA2 | A good hashing encryption algorithm. |
| sudo | This Linux command will allow a user to run a command with escalate privileges using their own password. |
| Sudo is allowed by the admin to run a command while su is to become the admin | Difference between sudo and su. |
| SUID set | find / -perm -4000 -user root -type f -print 2>/dev/null |
| Sysprep | C:\Windows\System32 subdirectories may provide store credentials from unattended installs. |
| SYSTEM | Highest level of privilege on a windows machine. |
| The best way to avoid being vulnerable to this attack is to avoid dynamically adding files based on user input | Best way to mitigate inclusion attack. |
| The debugger executes the code within function A and moves to the next instruction | This happens when debugging an executable with pwndbg with a function named function A is stepped over, instead of into. |
| The encrypted data, The encryption key for decryption, and the encryption algorithm | This is needed in order to decrypt data |
| The original unencrypted message, the Encryption key, and the encryption algorithm | This is needed in order to encrypt data |
| The POST Request | CSRF tokens should be located here to keep user’s sessions from being vulnerable. |
| The program will be run with root permissions | -rwsr-xr-x 1 root root 44k May 7th 2014 /bin/ping |
| The user directories for every user other than the root | Are located in the home folder. |
| The victim must be authenticated with the target site | This is a requirement for cross-site request forgery (CSRF) to work. |
| The Website's SSL certificate | This can be used to check the symmetric and asymmetric encryption |
| The Website's SSL certificate | HTTPS feature encryption solves the trust problem in the asymmetric key exchange. |
| They are all of the functions called up to this point | Items listed in pwbdbg’s Backtrace. |
| To ask the administrator for the permissions | Easiest way to bypass UAC. |
| To keep all organizations up to date for all technology that it uses to protect them against new and old vulnerabilities | Importance of patch cycles. |
| To program the web application without a third party entity and to sanitize the user input | Best way to mitigate command injection |
| To read sensitive data within the web application | Directory traversal vulnerability. |
| To sanitize the user input and to use a 3rd party library and not implement your own filter | Best way to mitigate cross site scripting |
| To use truly random session tokens that expire | Best way to mitigate a guess session attack. |
| User Directories for every user on the system excluding the root user | Found in the home folder. |
| var | This is where Linux logs are generally found. |
| Volatility | This tool is used to perform live analysis on a host’s RAM. |
| When a new event occurs that requires attention from the processor | This is a software interrupt issued by a computer. |
| When creating a script to run against a network service | A security analysts creates a “TCP Socket” in a python program |
| Where a user can be tricked into clicking on something without realizing that they did | ClickJacking attack |
| Where a user uses unauthorized commands submitted from a user that the web application trusts | Cross site request forgery |
| Where an attacker guesses a Session Token and logs into a site under your information | Session guessing |
| Where the attacker compromises a site that their target visits often and installs malware | Drive by download attack. |
| Where the CPU goes to next after completing a function | Return Pointer |
| Where you gain the highest level of access within a system | Privilege escalation. |
| Where you pretend to be someone else over email or phone | Pretexting |
| Where you take advantage of a code but supplementing wildcards within the code | Wild card injection. |
| Where you trick someone into doing something for you that goes against company policy | Social engineering. |
| Zero bytes | In both the TCP handshake and teardown, the ACK number increases by one. |