Vulnerability Assessment Plan - Red TEAM

This vulnerability assessment plan aims to conduct comprehensive reconnaissance, vulnerability assessment, and exploitation activities to evaluate the security posture of our home lab environment in depth. Critical vulnerabilities were discovered across devices and services, with effective exploitation detected in multiple systems (Bee-Box and Metasploitable). To prevent such attacks, it is advised to segment the network, patch vulnerabilities as soon as they are discovered, and improve access controls.

Scope:

We have identified and will be using our home lab environment with an IP network of 10.0.69.0/24 and prioritize the vulnerabilities to enhance the security standards of the home lab environment. The primary objective is to gather comprehensive information about the network to identify vulnerabilities and attempt unauthorized access. Our objective as a team is to locate and isolate any vulnerabilities on the target network. Classifying vulnerabilities according to their degree of severity and creating a strategy for vulnerability mitigation to address vulnerabilities that are found effectively are our goals as a team.

We have utilized Nmap, OpenVAS, Metasploit and Wireshark to work on different responsibilities and tasks – such as monitoring and attacking the targeted network. Our team would be divided into two pairs: one would cover monitoring and perform the attack. Nmap and OpenVAS were chosen to perform port scanning and through vulnerable assessment reports. OpenVAS was responsible for targeting the selected vulnerable machine to identify the vulnerability to exploit based on the severity. Wireshark is used to monitor the network and the packet flow while the port and vulnerability scan is performed.

Vulnerabilities Assessment:

We have found vulnerabilities in both Bee-box and Metasploitable during simultaneous scans of both teams using Nmap and OpenVAS, and the screenshots provide more detail on the types of vulnerabilities found ranging from Vulnerable to High levels with their details:

Metasploitable:

The port numbers 21 (FTP), 22 (SSH), 80 (HTTP), and 3306 (MySQL) on the host "10.0.69.10" are open and could provide routes of entry for attackers. Data theft and system compromise concerns were raised after Nmap found directory traversal and outdated software on the Ubuntu Apache 2.4.7 server running on port 80. Additionally, the vulnerability to Slowloris attacks creates a Denial of Service (DoS) risk by creating many host connections, which could reduce the efficiency of the service.

Furthermore, our network is prone to SSL/TLS vulnerabilities due to weak cipher suites and the SSLv3 protocol, which is susceptible to POODLE attacks. Notably, in addition to the current vulnerability CVE-2020-9473, there are many CVEs, such as CVE-2015-3306, CVE-2016-7144, and older vulnerabilities from 1999 (CVE-1999-0501, -0502, -0507, -0508).

```
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       http://ha.ckers.org/slowloris/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
| http-enum:
|   /: Root directory w/ listing on 'apache/2.4.7 (ubuntu)'
|   /phpmyadmin/: phpMyAdmin
|_  /uploads/: Potentially interesting directory w/ listing on 'apache/2.4.7 (ubuntu)'
| http-sql-injection:
|   Possible sqli for queries:
|     http://10.0.69.10:80/?C=S%3BO%3DA%27%20OR%20sqlspider
|     http://10.0.69.10:80/?C=M%3BO%3DA%27%20OR%20sqlspider
|     http://10.0.69.10:80/?C=N%3BO%3DD%27%20OR%20sqlspider
|_    http://10.0.69.10:80/?C=D%3BO%3DA%27%20OR%20sqlspider
445/tcp  open   microsoft-ds
631/tcp  open   ipp
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       http://ha.ckers.org/slowloris/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
| http-enum:
|   /admin.php: Possible admin folder
|   /admin/: Possible admin folder
```

```
|   /admin/jscript/upload.html: Lizard Cart/Remote File upload
|   /admin/jscript/upload.pl: Lizard Cart/Remote File upload
|   /admin/jscript/upload.asp: Lizard Cart/Remote File upload
|   /admin/environment.xml: Moodle files
|   /classes/: Potentially interesting folder
|   /es/: Potentially interesting folder
|   /helpdesk/: Potentially interesting folder
|   /help/: Potentially interesting folder
|_  /printers/: Potentially interesting folder
3000/tcp closed ppp
3306/tcp open   mysql
8080/tcp open   http-proxy
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       http://ha.ckers.org/slowloris/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
8181/tcp closed intermapper
MAC Address: 08:00:27:66:31:37 (Oracle VirtualBox virtual NIC)

Host script results:
| smb-vuln-regsvc-dos:
|   VULNERABLE:
|   Service regsvc in Microsoft Windows systems vulnerable to denial of service
|     State: VULNERABLE
|       The service regsvc in Microsoft Windows 2000 systems is vulnerable to denial of service caused by a null defer
ence
|       pointer. This script will crash the service if it is vulnerable. This vulnerability was discovered by Ron Bowe
s
|       while working on smb-enum-sessions.
|
```

Beebox:

The Beebox system is vulnerable to many vulnerabilities, including Logjam, which can result in cryptographic errors and the eavesdropping of sensitive data. Along with potential Denial of Service (DoS) attacks and CSS injection vulnerabilities, additional security risks are associated with the CVE-2015-4000, CVE-2007-6750, CVE-2014-0160, and CVE-2010-4344 vulnerabilities. These issues affect the system's availability and integrity, allowing malicious actors to interrupt operations, implant malicious code, and exploit known gaps to gain unauthorized access or manipulate data.

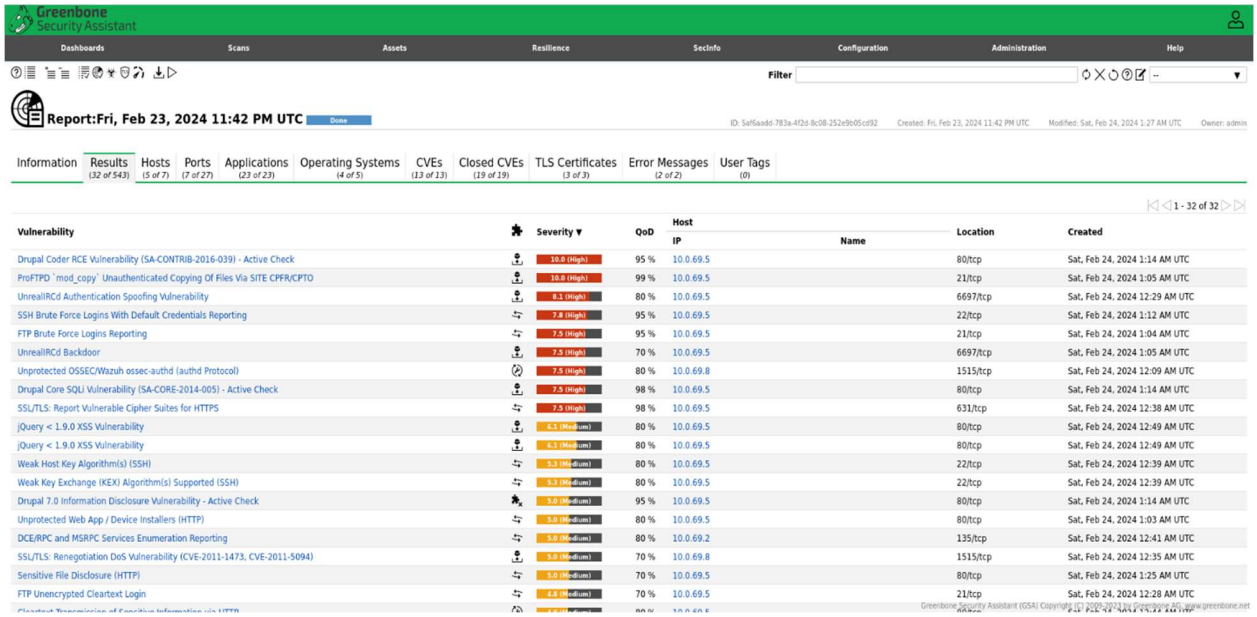
```
| http-cross-domain-policy:
|   VULNERABLE:
|   Cross-domain and Client Access policies.
|     State: VULNERABLE
|       A cross-domain policy file specifies the permissions that a web client such as Java
, Adobe Flash, Adobe Reader,
|       etc. use to access data across different domains. A client acces policy file is sim
ilar to cross-domain policy
|       but is used for M$ Silverlight applications. Overly permissive configurations enabl
es Cross-site Request
|       Forgery attacks, and may allow third parties to access sensitive data meant for the
 user.
|     Check results:
|       /crossdomain.xml:
|         <?xml version="1.0"?>
|         <!DOCTYPE cross-domain-policy SYSTEM "http://www.macromedia.com/xml/dtds/cross-do
main-policy.dtd">
|         <cross-domain-policy>
|           <allow-access-from domain="*" />
|         </cross-domain-policy>
|     Extra information:
|       Trusted domains:*
|
|     References:
|       https://www.adobe.com/devnet/articles/crossdomain_policy_file_spec.html
|       https://www.owasp.org/index.php/Test_RIA_cross_domain_policy_%28OTG-CONFIG-008%29
|       http://acunetix.com/vulnerabilities/web/insecure-clientaccesspolicy-xml-file
|       http://sethsec.blogspot.com/2014/03/exploiting-misconfigured-crossdomainxml.html
|       http://gursevkalra.blogspot.com/2013/08/bypassing-same-origin-policy-with-flash.htm
l
|_      https://www.adobe.com/devnet-docs/acrobatetk/tools/AppSec/CrossDomain_PolicyFile_Sp
ecification.pdf
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=10.0.69.6
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://10.0.69.6:80/drupal/
|     Form id: user-login-form
```

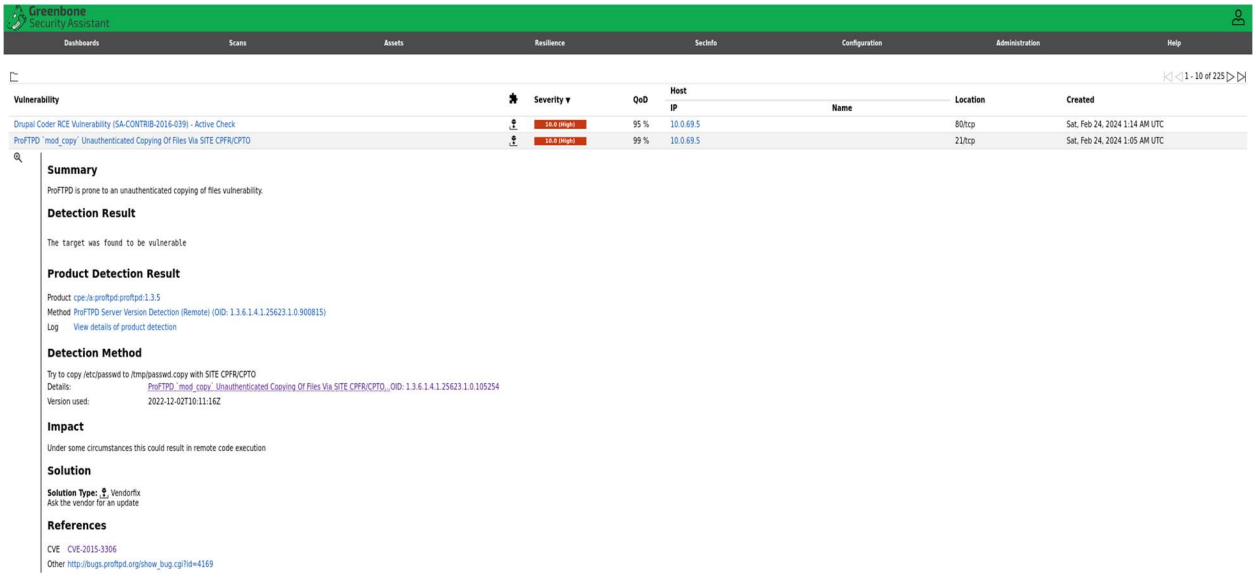
```
ecification.pdf
| ssl-ccs-injection:
|   VULNERABLE:
|   SSL/TLS MITM vulnerability (CCS Injection)
|     State: VULNERABLE
|     Risk factor: High
|       OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h
|       does not properly restrict processing of ChangeCipherSpec messages,
|       which allows man-in-the-middle attackers to trigger use of a zero
|       length master key in certain OpenSSL-to-OpenSSL communications, and
|       consequently hijack sessions or obtain sensitive information, via
|       a crafted TLS handshake, aka the "CCS Injection" vulnerability.
|
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224
|       http://www.cvedetails.com/cve/2014-0224
|_      http://www.openssl.org/news/secadv_20140605.txt
| http-enum:
|   /crossdomain.xml: Adobe Flash crossdomain policy
|_  /phpmyadmin/: phpMyAdmin
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_      http://ha.ckers.org/slowloris/
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=10.0.69.6
|   Found the following possible CSRF vulnerabilities:
|
|     Path: https://10.0.69.6:443/phpmyadmin/
|     Form id:
|     Form action: index.php
|
|     Path: https://10.0.69.6:443/phpmyadmin/
|     Form id: input_username
```

```
ecification.pdf
| http-enum:
|_  /crossdomain.xml: Adobe Flash crossdomain policy
8443/tcp open  https-alt
| ssl-heartbleed:
|   VULNERABLE:
|   The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic soft
ware library. It allows for stealing information intended to be protected by SSL/TLS encryp
tion.
|     State: VULNERABLE
|     Risk factor: High
|       OpenSSL versions 1.0.1 and 1.0.2-beta releases (including 1.0.1f and 1.0.2-beta1) o
f OpenSSL are affected by the Heartbleed bug. The bug allows for reading memory of systems
protected by the vulnerable OpenSSL versions and could allow for disclosure of otherwise en
crypted confidential information as well as the encryption keys themselves.
|
|     References:
|       http://www.openssl.org/news/secadv_20140407.txt
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160
|_      http://cvedetails.com/cve/2014-0160/
| ssl-poodle:
|   VULNERABLE:
|   SSL POODLE information leak
|     State: VULNERABLE
|     IDs:  BID:70574  CVE:CVE-2014-3566
|           The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
|           products, uses nondeterministic CBC padding, which makes it easier
|           for man-in-the-middle attackers to obtain cleartext data via a
|           padding-oracle attack, aka the "POODLE" issue.
|     Disclosure date: 2014-10-14
|     Check results:
|       TLS_RSA_WITH_AES_128_CBC_SHA
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
|       https://www.imperialviolet.org/2014/10/14/poodle.html
|       https://www.openssl.org/~bodo/ssl-poodle.pdf
|_      https://www.securityfocus.com/bid/70574
| ssl-dh-params:
|   VULNERABLE:
|   Diffie-Hellman Key Exchange Insufficient Group Strength
|     State: VULNERABLE
|       Transport Layer Security (TLS) services that use Diffie-Hellman groups
|       of insufficient strength, especially those using one of a few commonly
|       shared groups, may be susceptible to passive eavesdropping attacks.
```

Analysis and Results:

The risk and vulnerability impact are observed using OpenVAS, where vulnerabilities of Metasploitable machines





There are a few vulnerabilities in Metasploitable machines:

1. RCE for Drupal Code Vulnerability: A severe security vulnerability that lets an attacker execute any code on the Drupal application's hosting server.
2. A significant vulnerability in ProFTPD's 'mod_copy' module enables unauthenticated users to perform file operations, potentially resulting in unauthorized file copying or relocating.
3. A high-severity vulnerability in UnrealIRCd could allow an attacker to pretend to be an IRC server administrator.
4. **SSH Brute Force:** This is a high-severity vulnerability because attackers may use brute force attacks on SSH services to gain access.
5. **Reports on FTP Brute Force Logins:** This poses a severe risk of unauthorized access, like brute force SSH attacks.
6. **UnrealIRCd Backdoor:** A security vulnerability makes unauthorized access to the server possible.

Remediation Planning:

The remediation strategy for our group includes short, medium, and long-term steps to resolve the vulnerabilities found successfully. Patches and upgrades will be applied to the Ubuntu Apache server immediately, along with service hardening and ProFTPD vulnerability mitigation.

In the future, security flaws on the Bee-box system will be fixed along with improvements to the SSH password policy and configuration changes. Network segmentation, ongoing monitoring, security awareness instruction, creating incident response plans, and frequent vulnerability assessments are examples of long-term strategies. Regular reviews will guarantee that the network's security posture is continuously improved by incorporating lessons we will learn and input into the plan. By implementing these measures, our group can mitigate security risks and enhance security against cyber threats.