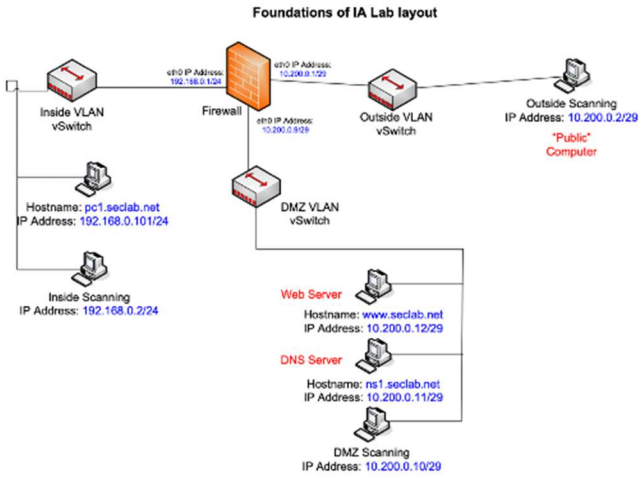
Project Final Report
695.601 Foundations of Information Assurance
Team 2: Craig Mazuranic, Laura Glessner, Parthiv Desai
Team "Better Watch Out"

I. Executive Summary/Introduction

The 'Better Watch Out' team, comprising three external students, conducted a security assessment via a remote pulse connection to VPN.JH.edu, accessing the JH Secure Lab environment 2. The team's project objective was to assess this secure lab environment, discovering, documenting, and suggesting risk-benefit mitigation strategies to leadership. The team utilized various vulnerability tools on Kali Linux inside-2, Kali Linux outside-2, and PC-2 for vulnerability interrogation of the remaining network server nodes (refer to figure 1).



Tests were conducted on available servers using both IP addresses and fully qualified domain names when available. For example, the DNS server, Web server, and DMZ server were accessible using both identifiers, resulting in six vulnerability interrogations. The 'Better Watch Out' team identified several areas of concern, both internal and external, exhibiting recurring themes that contribute to vulnerabilities. Notably, external vulnerabilities were less prevalent than internal ones, indicating a stronger defense against external threats while showing a lax attitude towards internal system updates and port security. This attitude increases the risk of internal attacks, such as Smurf attacks or zero-day exploits. The team identified several high-risk vulnerabilities needing immediate attention, with three requiring further research. Most medium and low-risk vulnerabilities also necessitate additional research and coordination, particularly regarding configuration management, documentation, upkeep, and possibly poor deployment practices. Implementing configuration changes or updates without testing their effects on similar systems and networks is a risk management concern that requires approval. Thus, it is recommended that Configuration Management and Information Assurance procedures and workflows be reviewed and updated. This need arises from potential lapses in adhering to system administration policies and procedures during and post-deployment. Such lapses could stem from either the technical capabilities of the system administrators or from inadequate risk management oversight by management. A notable example underscoring our findings comes from NMAP scans of the Web server, both internally and externally. These scans revealed nonstandard ports,

such as TCP port 8180, without any available documentation explaining their purpose. Questions arise: Should this port be closed? Is it part of a database replication stream or a vulnerability? Concerns also extend to ports allowing remote control connectivity and root sign-in capabilities. Why are multiple ports open for this connectivity if the policy mandates the use of an X11 terminal? If the policy allows SSH connectivity to execute an X11 terminal within encrypted tunnels, then only these should be permitted. This reinforces our contention regarding the importance of robust configuration management and documentation, which would identify the purpose of such ports and the approvals behind them, thereby clarifying the risks and rationales. Below, we detail the vulnerabilities found, the suggested mitigations by OpenVAS and OWASP Zap, and the steps we recommend securing the systems. It's important to note that NMAP reports ports and protocols differently, and mitigation steps, such as enabling or disabling ports, should be reviewed, and approved by leadership.

II. Vulnerabilities Found
Web Server Vulnerabilities: External

Host	High	Medium	Low	Log	False Positive
10.200.0.12 www.seclab.net	4	9	1	0	0
Total: 1	4	9	1	0	0

1. High (CVSS: 10.0) NVT: TWiki XSS and Command Execution Vulnerabilities
The host is running TWiki and is prone to Cross-Site Scripting (XSS) and Command Execution Vulnerabilities. Successful exploitation could allow execution of arbitrary script code or commands which could let attackers steal cookie-based authentication credentials or compromise the affected application. Vulnerability is due to URLPARAM variable not properly sanitized so attackers can conduct XSS attack. Also, SEARCH variable is not properly sanitized before being used in an eval () call so the attackers could execute perl code through eval injection attack.
Solution: VenderFix, upgrade TWiki to version 4.2.4 or later.
References: CVE-2008-5304, CVE-2008-5305.

2. High (CVSS: 7.5) NVT: phpinfo() output Reporting
Many PHP installation tutorials instruct the user to create a file called phpinfo.php or similar containing the phpinfo() statement. Such a file is often left back in the webserver directory. Some of the information in this file: username of user running the PHP process, if it is a sudo user, the IP address of the host, the web server version, the system version (Unix, Linux, Windows…) and the root directory of the web server.
Solution: Workaround, delete the listed files or restrict access to them.

3. High (CVSS: 7.5) NVT: PHP-CGI-based setups vuln. when parsing query string parameters from php files.
PHP is prone to an information-disclosure vulnerability. Exploiting this issue allows remote attackers to view the source code of files in the context of the server process. This may allow the attacker to obtain sensitive information and to run arbitrary PHP code on the affected computer. Other attacks are also possible.
Solution: VenderFix, PHP has released version 5.4.3 and 5.3.13. PHP is recommending users upgrade to the latest version of PHP.
References: CVE-2012-1823, CVE-2012-2311, CVE-2012-2336, CVE-2012-2335.

4. High (CVSS: 7.5) NVT: Test HTTP dangerous methods
Misconfigured web servers allow remote clients to perform dangerous HTTP methods such as PUT and DELETE. This script checks if they are enabled and can be misused to upload or delete files. Enabled PUT method could allow an attacker to upload and run arbitrary code on this web server. Enabled DELETE method could allow an attacker to delete additional files on this web server.
Solution: Mitigation, use access restrictions to these dangerous HTTP methods or disable them completely.

Web Server Vulnerabilities: Internal

Host	High	Medium	Low	Log	False Positive
10.200.0.12 www.seclab.net	12	21	2	0	0
Total: 1	12	21	2	0	0

1. High (CVSS: 10.0) NVT: OS End of Life Detection
The “Ubuntu” operating system on the remote host has reached the end of life and should not be used anymore.
Solution: Mitigation, terminate use of current operating system in use.

2. High (CVSS: 9.0) NVT: VNC Brute Force Login
Try to login with given passwords via VNC protocol. The vulnerability was detected due to it being possible to connect to the VNC server with the password: password. This script tries to authenticate to a VNC server with the passwords set in the password preference. It will also test and report if no authentication/password is required. Some VNC servers have a blacklisting scheme that blocks IP addresses after five unsuccessful connection attempts for a period of time. The script will abort the brute force attack if it encounters that it gets blocked. Passwords can be max. 8 characters long.
Solution: Mitigation, change the password to something hard to guess or enable password protection, enable block of IP addresses after five unsuccessful connection attempts.

3. High (CVSS: 10.0) NVT: Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities

Systems using Distributed Ruby (dRuby/DRb), which is available in Ruby versions 1.6 and later, may permit unauthorized systems to execute distributed commands. By default, Distributed Ruby does not impose restrictions on allowed hosts or set the $SAFE environment variable to prevent privileged activities. If other controls are not in place, especially if the Distributed Ruby process runs with elevated privileges, an attacker could execute arbitrary system commands or Ruby scripts on the Distributed Ruby server.

Solution: Mitigation, administrators of environments that rely on Distributed Ruby should ensure that appropriate controls are in place. Code-level controls may include: implementing taint on untrusted input, setting $SAFE levels appropriately (>=2 is recommended if untrusted hosts are allowed to submit Ruby commands, and >=3 may be appropriate) and including drb/acl.rb to set ACLEntry to restrict access to trusted hosts.

4. High (CVSS: 10.0) NVT: Possible Backdoor: Ingreslock

A backdoor is installed on the remote host shown since the service is answering to an 'id;' command with the following response: uid=0(□→root) gid=0(root). Attackers can exploit this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the affected system.

Solution: Workaround, terminate use of Ingreslock to remediate backdoor.

5. High (CVSS: 7.5) NVT: vsftpd Compromised Source Packages Backdoor Vulnerability

The vsftpd is prone to a backdoor vulnerability. Attackers can exploit this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the affected application.

Solution: VendorFix, the repaired package can be downloaded from the referenced link. Validate the package with its signature.

6. High (CVSS: 9.3) NVT: DistCC Remote Code Execution Vulnerability

DistCC 2.x, as used in XCode 1.5 and others, when not configured to restrict access to the server port, allows remote attackers to execute arbitrary commands via compilation jobs, which are executed by the server without authorization checks. It was possible to execute the "id" command, result: uid=1(daemon) gid=1(daemon). DistCC by default trusts its clients completely and in turn could allow a malicious client to execute arbitrary commands on the server.

Solution: VendorFix, Vendor updates are available. Please see the references for more information. For more information about DistCC's security see the references.

References: CVE-2004-2687.

7. High (CVSS: 7.5) NVT: vsftpd Compromised Source Packages Backdoor Vulnerability

The vsftpd is prone to a backdoor vulnerability. Attackers can exploit this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the affected application.

Solution: VendorFix, the repaired package can be downloaded from the referenced link. Validate the package with its signature.

8. High (CVSS: 9.0) NVT: PostgreSQL weak password
It was possible to login into the remote PostgreSQL as user postgres using weak credentials. It was possible to login as user postgres with password "postgres".
Solution: Mitigation, change the password as soon as possible.

9. High (CVSS: 10.0) NVT: TWiki XSS and Command Execution Vulnerabilities
The host is running TWiki and is prone to Cross-Site Scripting (XSS) and Command Execution Vulnerabilities. Successful exploitation could allow execution of arbitrary script code or commands which could let attackers steal cookie-based authentication credentials or compromise the affected application. Vulnerability is due to URLPARAM variable not properly sanitized so attackers can conduct XSS attack. Also, SEARCH variable is not properly sanitized before being used in an eval() call so the attackers could execute perl code through eval injection attack.
Solution: VenderFix, upgrade TWiki to version 4.2.4 or later.
References: CVE-2008-5304, CVE-2008-5305.

10. High (CVSS: 7.5) NVT: phpinfo() output Reporting
Many PHP installation tutorials instruct the user to create a file called phpinfo.php or similar containing the phpinfo() statement. Such a file is often left back in the webserver directory. Some of the information in this file: username of user running the PHP process, if it is a sudo user, the IP address of the host, the web server version, the system version (Unix, Linux, Windows…) and the root directory of the web server.
Solution: Workaround, delete the listed files or restrict access to them.

11. High (CVSS: 7.5) NVT: PHP-CGI-based setups vuln. when parsing query string parameters from php files.
PHP is prone to an information-disclosure vulnerability. Exploiting this issue allows remote attackers to view the source code of files in the context of the server process. This may allow the attacker to obtain sensitive information and to run arbitrary PHP code on the affected computer. Other attacks are also possible.
Solution: VenderFix, PHP has released version 5.4.3 and 5.3.13. PHP is recommending users upgrade to the latest version of PHP.
References: CVE-2012-1823, CVE-2012-2311, CVE-2012-2336, CVE-2012-2335.

12. High (CVSS: 7.5) NVT: Test HTTP dangerous methods
Misconfigured web servers allow remote clients to perform dangerous HTTP methods such as PUT and DELETE. This script checks if they are enabled and can be misused to upload or delete files. Enabled PUT method could allow an attacker to upload and run arbitrary code on this web server. Enabled DELETE method could allow an attacker to delete additional files on this web server.
Solution: Mitigation, use access restrictions to these dangerous HTTP methods or disable them completely.

DNS Server Vulnerabilities:

Host	High	Medium	Low	Log	False Positive
10.200.0.11 ns1.seclab.net	16	22	6	11	0
Total: 1	16	22	6	11	0

1. High (CVSS: 7.5) NVT: OpenSSH 'schnorr.c' Remote Memory Corruption Vulnerability
OpenSSH is prone to a remote memory-corruption vulnerability. An attacker can exploit this issue to execute arbitrary code in context of the application. Failed exploits may result in denial-of-service conditions. The hash_buffer function in schnorr.c in OpenSSH through 6.4, when Makefile.inc is modified to enable the J-PAKE protocol, does not initialize certain data structures, which might allow remote attackers to cause a denial of service (memory corruption) or have unspecified other impact via vectors that trigger an error condition.
Solution: VendorFix, updates are available, see references for more information.
References: CVE-2014-1692.

2. High (CVSS: 7.8) NVT: OpenSSH Denial of Service And User Enumeration Vulnerabilities (Linux)
This host is installed with openssh and is prone to denial of service and user enumeration vulnerabilities. Successfully exploiting this issue allows remote attackers to cause a denial of service (crypt CPU consumption) and to enumerate users by leveraging the timing difference between responses when a large password is provided. Multiple faws exist due to: the auth_password function in 'auth-passwd.c' script does not limit password lengths for password authentication and the sshd in OpenSSH, when SHA256 or SHA512 are used for user password hashing uses BLOWFISH hashing on a static password when the username does not exist and it takes much longer to calculate SHA256/SHA512 hash than BLOWFISH hash.
Solution: VendorFix, upgrade to OpenSSH version 7.3 or later.
References: CVE-2016-6515, CVE-2016-6210.

3. High (CVSS: 8.5) NVT: OpenSSH Multiple Vulnerabilities
This host is running OpenSSH and is prone to multiple vulnerabilities. Successful exploitation will allow an attacker to gain privileges, to conduct impersonation attacks, to conduct brute-force attacks or cause a denial of service. Multiple flaws due to use-after-free vulnerability in the 'mm_answer_pam_free_ctx' function in monitor.c in sshd, the vulnerability in 'kbdint_next_device' function in auth2-chall.c in sshd and the vulnerability in the handler for the MONITOR_REQ_PAM_FREE_CTX request.
Solution: VendorFix, upgrade OpenSSH to 7.0 or later.
References: CVE-2015-6564, CVE-2015-6563, CVE-2015-5600.

4. High (CVSS: 7.5) NVT: OpenSSH Multiple Vulnerabilities Jan17 (Linux)
This host is installed with OpenSSH and is prone to multiple vulnerabilities. Successfully exploiting this issue allows local users to obtain sensitive private-key information, to gain privileges, conduct a senial-of-service condition and allows remote attackers to execute arbitrary local PKCS#11 modules. Multiple flaws due to: an 'authfile.c' script does not properly consider

the effects of realloc on buffer contents, shared memory manager (associated with pre-authentication compression) does not ensure that a bounds check is enforced by all compilers, sshd in OpenSSH creates forwarded Unix-domain sockets as root, when privilege separation is not used, an untrusted search path vulnerability in ssh-agent.c in ssh-agent and NULL pointer dereference error due to an out-of-sequence NEWKEYS message.
Solution: VendorFix, upgrade OpenSSH to version 7.4 or later.
References: CVE-2016-10009, CVE-2016-10010, CVE-2016-10011, CVE-2016-10012, CVE-2016-10708.

5. High (CVSS: 7.2) NVT: OpenSSH Privilege Escalation Vulnerabilitity - May16
This host is installed with openssh and is prone to privilege escalation vulnerability. Successfully exploiting this issue will allow local users to gain privileges. The flaw exists due to an error in 'do_setup_env function' in 'session.c' script in sshd which triggers a crafted environment for the /bin/login program when the UseLogin feature is enabled and PAM is configured to read. pam_environment files in user home directories.
Solution: VendorFix, upgrade OpenSSH to version 7.2p2-3 or later.
References: CVE-2015-8325.

6. High (CVSS: 7.5) NVT: OpenSSH X11 Forwarding Security Bypass Vulnerability (Linux)
This host is installed with openssh and is prone to security bypass vulnerability. Successfully exploiting this issue allows local users to bypass certain security restrictions and perform unauthorized actions. This may lead to further attacks. An access flaw was discovered in OpenSSH, it did not correctly handle failures to generate authentication cookies for untrusted X11 forwarding. A malicious or compromised remote X application could possibly use this flaw to establish a trusted connection to the local X server, even if only untrusted X11 forwarding was requested.
Solution: VendorFix, upgrade OpenSSH to version 7.2 or later.
References: CVE-2016-1908.

7. High (CVSS: 7.5) NVT: SSH Brute Force Logins With Default Credentials Reporting
It was possible to login into the remote SSH server using default credentials. As the NVT 'SSH Brute Force Logins with default Credentials' (OID: 1.3.6.1.4.1.25623.1.0.108013) might run into a timeout the actual reporting of this vulnerability takes place in this NVT instead. The script preference 'Report timeout' allows you to configure if such a timeout is reported.
Solution: Mitigation, change the password as soon as possible.

8. High (CVSS: 10.0) NVT: BIND End of Life Detection (Linux)
The BIND version on the remote host has reached the end of life and should not be used anymore. An end-of-life version of BIND is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host.
Solution: VendorFix, update the BIND version on the remote host to a still supported version.

9. High (CVSS: 7.8) NVT: ISC BIND ‘buffer.c’ Assertion Failure Denial of Service Vulnerability
The host is installed with ISC BIND and is prone to denial-of-service vulnerability. Successful exploitation will allow remote attackers to cause a denial of service (assertion failure and daemon exit) via a crafted query. The flaw exists due to the 'buffer.c' script in named in ISC BIND does not properly construct responses.
Solution: VendorFix, upgrade to ISC BIND version 9.9.9-P3 or 9.10.4-P3 or 9.11.0rc3 or later on Linux.

10. High (CVSS: 7.8) NVT: ISC BIND ‘buffer.c’ Script Remote Denial of Service Vulnerability - Jan16
The host is installed with ISC BIND and is prone to remote denial of service vulnerability. Successful exploitation will allow remote attackers to cause denial of service. The flaw is due to an error in 'buffer.c' script in ISC BIND.
Solution: VendorFix, upgrade to ISC BIND version 9.9.7-P3 or 9.10.2-P4 or later.
References: CVE-2015-5722.

11. High (CVSS: 7.8) NVT: ISC BIND Delegation Handling Denial of Service Vulnerability
The host is installed with ISC BIND and is prone to denial-of-service vulnerability. Successful exploitation will allow attackers to cause denial of service to clients. The flaw is due to ISC BIND does not handle delegation chaining properly.
Solution: VendorFix, upgrade to ISC BIND version 9.9.6-p1 or 9.10.1-p1 or later for branches of BIND (9.9 and 9.10).
References: CVE-2014-8500.

12. High (CVSS: 7.8) NVT: ISC BIND Denial of Service Vulnerability
ISC BIND is prone to a denial-of-service vulnerability. A remote attacker may cause a denial-of-service condition. A crafted query could crash the BIND name server daemon, leading to a denial of service. All server roles (authoritative, recursive, and forwarding) in default configurations are affected.
Solution: VendorFix, Upgrade to 9.9.9-P3, 9.9.9-S5, 9.10.4-P3, 9.11.0rc3 or later.
References: CVE-2016-2776.

13. High (CVSS: 7.8) NVT: ISC BIND Denial of Service Vulnerability - 06 - Jan16
The host is installed with ISC BIND and is prone to remote denial of service vulnerability. Successful exploitation will allow remote attackers to cause denial of service. The flaw is due to an error in handling TKEY queries that can cause named to exit with a REQUIRE assertion failure.
Solution: VendorFix, upgrade to ISC BIND version 9.9.7-P2 or 9.10.2-P3 or later.
References: CVE-2015-5477.

14. High (CVSS: 7.8) NVT: ISC BIND Denial of Service Vulnerability - Oct15
The host is installed with ISC BIND and is prone to denial-of-service vulnerability. Successful exploitation will allow attackers to cause denial of service to clients. The flaw is due to an error in 'name.c' script in ISC BIND when configured as a recursive resolver with DNSSEC validation.
Solution: VendorFix, upgrade to ISC BIND version 9.9.7-P1 or 9.10.2-P2 or later.

References: CVE-2015-4620.

15. High (CVSS: 7.8) NVT: ISC BIND DNS RDATA Handling Remote Denial of Service Vulnerability - Jan16

The host is installed with ISC BIND and is prone to remote denial of service vulnerability.
Successful exploitation will allow attackers to cause denial of service. The flaw exists due to an error in DNS RDATA Handling in ISC BIND.
Solution: VendorFix, upgrade to ISC BIND version 9.7.7 or 9.7.6-P4 or 9.6-ESV-R8 or 9.6-ESV-R7-P4 or 9.8.4 or 9.8.3-P4 or 9.9.2 or 9.9.1-P4 later.
References: CVE-2012-5166.

16. High (CVSS: 7.8) NVT: ISC BIND DNS64 Remote Denial of Service Vulnerability - Jan16

The host is installed with ISC BIND and is prone to remote denial of service vulnerability.
Successful exploitation will allow attackers to cause denial of service. The flaw exists due to some unspecified error in ISC BIND when DNS64 is enabled.
Solution: VendorFix, upgrade to ISC BIND version 9.8.4-P1 or 9.9.2-P1 or later.
References: CVE-2012-5688.

III. Recommended Mitigations

Based on the below guidance from NIST due to the CVSS, the first step in ensuring the security of this network would be to create a corrective action plan and then remediate the critical and high vulnerabilities from section II following the below timeframe.

- **Critical (CVSS 9-10) Vulnerabilities:**
  - Create a corrective action plan within two weeks.
  - Remediate vulnerability within one month.
- **High (CVSS 7-8.9) Vulnerabilities:**
  - Create corrective action plan within one month.
  - Remediate vulnerability within three months.
- **Other Vulnerabilities:**
  - Can be resolved based on availability of staff resources.

10.200.0.12 external web server mitigations:

- Upgrade TWiki to version 4.2.4 or later.
- Delete the listed files or restrict access to them.
- PHP has released versions 5.4.3 and 5.3.13. PHP is recommending users upgrade to the latest version of PHP.
- Use access restrictions to these dangerous HTTP methods or disable them completely.

10.200.0.12 internal web server mitigations:

- Terminate use of current operating system.
- Change the password to something hard to guess or enable password protection, enable block of IP addresses after five unsuccessful connection attempts.
- Administrators of environments that rely on Distributed Ruby should ensure that appropriate controls are in place. Code-level controls may include implementing taint on untrusted input, setting $SAFE levels appropriately and drb/acl.rb to set ACLEntry to restrict access to trusted hosts.
- Terminate use of Ingreslock to remediate backdoor.

- Upgrade TWiki to version 4.2.4 or later.
- Delete the listed files or restrict access to them.
- PHP has released versions 5.4.3 and 5.3.13. PHP is recommending users upgrade to the latest version of PHP.
- Use access restrictions to these dangerous HTTP methods or disable them completely.

10.200.0.11 DNS server mitigations:

- Upgrade OpenSSH to version 7.4 or later.
- Change the password as soon as possible.
- Upgrade to ISC BIND version 9.7.7 or 9.7.6-P4 or 9.6-ESV-R8 or 9.6-ESV-R7-P4 or 9.8.4 or 9.8.3-P4 or 9.9.2 or 9.9.1-P4 later.

IV. Conclusions/Summary

In conclusion, the 'Better Watch Out' team returns to the initial comments in the introduction. Many of the identified vulnerabilities, both internal and external, do raise concerns. However, making configuration changes, updating files as recommended, locking down ports, or adding software without understanding the second and third-order ramifications could do more harm than good. The 'Better Watch Out' team continues to stress the structural issues within the organization that need to be addressed for the efficient and effective deployment of information assurance strategies; otherwise, underlying issues will persist. This drives the team back to our introductory recurring theme: external vulnerabilities were fewer than internal, suggesting decisions favored network efficiency over internal security – a 'trusted person' approach. This indicates a minimal exposure to information assurance and an underestimation of the risks to vulnerabilities within the internal network. This stance reduces the workload for the information systems support staff but exposes the network to undue risk. If management understands and accepts this risk balance, then no action might be needed, as they are prepared to accept these vulnerabilities as part of their operating condition. The 'Better Watch Out' team maintains that the main task is to ensure management understands the pros and cons of the risks taken. We request a decision be made on whether to implement changes to lower internal vulnerabilities to Smurf attacks or zero-day exploits, or to enable unauthorized user access to both the Web and DNS servers at the root level. Essentially, after every decision is made, it must be integrated into a proper configuration management and documentation lifecycle to assess, identify, and understand the risks behind it, including the '5W's' (Who, What, Where, When, Why), and identify the risk owner if the situation has changed.

V Background NMAP reports.
DNS IP

```
Starting Nmap 7.80 ( https://nmap.org ) at 2023-11-26 01:00 EST
Initiating Parallel DNS resolution of 1 host. at 01:00
Completed Parallel DNS resolution of 1 host. at 01:00, 0.00s elapsed
Initiating SYN Stealth Scan at 01:00
Scanning ns1.seclab.net (10.200.0.11) [1000 ports]
Discovered open port 53/tcp on 10.200.0.11
Discovered open port 22/tcp on 10.200.0.11
Completed SYN Stealth Scan at 01:00, 0.13s elapsed (1000 total ports)
Nmap scan report for ns1.seclab.net (10.200.0.11)
Host is up, received user-set (0.00019s latency).
Scanned at 2023-11-26 01:00:48 EST for 0s
Not shown: 998 closed ports
Reason: 998 resets
PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack ttl 63
53/tcp open  domain  syn-ack ttl 63

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.37 seconds
        Raw packets sent: 1000 (44.000KB) | Rcvd: 1000 (40.008KB)
```

DNS FQDN

```
Starting Nmap 7.80 ( https://nmap.org ) at 2023-11-26 01:46 EST
Initiating Parallel DNS resolution of 1 host. at 01:46
Completed Parallel DNS resolution of 1 host. at 01:46, 0.00s elapsed
Initiating SYN Stealth Scan at 01:46
Scanning ns1.seclab.net (10.200.0.11) [1000 ports]
Discovered open port 22/tcp on 10.200.0.11
Discovered open port 53/tcp on 10.200.0.11
Completed SYN Stealth Scan at 01:46, 0.11s elapsed (1000 total ports)
Nmap scan report for ns1.seclab.net (10.200.0.11)
Host is up, received user-set (0.00040s latency).
Scanned at 2023-11-26 01:46:10 EST for 0s
Not shown: 998 closed ports
Reason: 998 resets
PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack ttl 63
53/tcp open  domain  syn-ack ttl 63

Read data files from: /usr/bin/../share/nmap
```

Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds
Raw packets sent: 1000 (44.000KB) | Rcvd: 1000 (40.008KB)
Starting Nmap 7.80 (https://nmap.org) at 2023-11-26 01:45 EST
Initiating Parallel DNS resolution of 1 host. at 01:45
Completed Parallel DNS resolution of 1 host. at 01:45, 0.00s elapsed
Initiating SYN Stealth Scan at 01:45
Scanning www.seclab.net (10.200.0.12) [1000 ports]
Discovered open port 23/tcp on 10.200.0.12
Discovered open port 3306/tcp on 10.200.0.12
Discovered open port 111/tcp on 10.200.0.12
Discovered open port 5900/tcp on 10.200.0.12
Discovered open port 139/tcp on 10.200.0.12
Discovered open port 53/tcp on 10.200.0.12
Discovered open port 445/tcp on 10.200.0.12
Discovered open port 80/tcp on 10.200.0.12
Discovered open port 21/tcp on 10.200.0.12
Discovered open port 513/tcp on 10.200.0.12
Discovered open port 2049/tcp on 10.200.0.12
Discovered open port 5432/tcp on 10.200.0.12
Discovered open port 514/tcp on 10.200.0.12
Discovered open port 8180/tcp on 10.200.0.12
Discovered open port 1099/tcp on 10.200.0.12
Discovered open port 2121/tcp on 10.200.0.12
Discovered open port 512/tcp on 10.200.0.12
Discovered open port 8009/tcp on 10.200.0.12
Discovered open port 6000/tcp on 10.200.0.12
Discovered open port 22/tcp on 10.200.0.12
Discovered open port 25/tcp on 10.200.0.12
Discovered open port 6667/tcp on 10.200.0.12
Discovered open port 1524/tcp on 10.200.0.12

Web Ip
Completed SYN Stealth Scan at 01:45, 1.15s elapsed (1000 total ports)
Nmap scan report for www.seclab.net (10.200.0.12)
Host is up, received user-set (0.00093s latency).
Scanned at 2023-11-26 01:45:11 EST for 1s
Not shown: 977 closed ports
Reason: 977 resets
PORT STATE SERVICE REASON
21/tcp open ftp syn-ack ttl 63
22/tcp open ssh syn-ack ttl 63
23/tcp open telnet syn-ack ttl 63
25/tcp open smtp syn-ack ttl 63
53/tcp open domain syn-ack ttl 63

```
80/tcp   open  http        syn-ack ttl 63
111/tcp  open  rpcbind     syn-ack ttl 63
139/tcp  open  netbios-ssn  syn-ack ttl 63
445/tcp  open  microsoft-ds syn-ack ttl 63
512/tcp  open  exec        syn-ack ttl 63
513/tcp  open  login       syn-ack ttl 63
514/tcp  open  shell       syn-ack ttl 63
1099/tcp open  rmiregistry  syn-ack ttl 63
1524/tcp open  ingreslock   syn-ack ttl 63
2049/tcp open  nfs         syn-ack ttl 63
2121/tcp open  ccproxy-ftp  syn-ack ttl 63
3306/tcp open  mysql       syn-ack ttl 63
5432/tcp open  postgresql   syn-ack ttl 63
5900/tcp open  vnc         syn-ack ttl 63
6000/tcp open  X11         syn-ack ttl 63
6667/tcp open  irc         syn-ack ttl 63
8009/tcp open  ajp13       syn-ack ttl 63
8180/tcp open  unknown     syn-ack ttl 63

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.33 seconds
        Raw packets sent: 1006 (44.264KB) | Rcvd: 1000 (40.092KB)
Starting Nmap 7.80 ( https://nmap.org ) at 2023-11-26 01:01 EST
Initiating Parallel DNS resolution of 1 host. at 01:01
Completed Parallel DNS resolution of 1 host. at 01:01, 0.01s elapsed
Initiating SYN Stealth Scan at 01:01
Scanning www.seclab.net (10.200.0.12) [1000 ports]
Discovered open port 5900/tcp on 10.200.0.12
Discovered open port 111/tcp on 10.200.0.12
Discovered open port 21/tcp on 10.200.0.12
Discovered open port 80/tcp on 10.200.0.12
Discovered open port 23/tcp on 10.200.0.12
Discovered open port 22/tcp on 10.200.0.12
Discovered open port 53/tcp on 10.200.0.12
Discovered open port 512/tcp on 10.200.0.12
Discovered open port 8009/tcp on 10.200.0.12
Discovered open port 1099/tcp on 10.200.0.12
Discovered open port 514/tcp on 10.200.0.12
Discovered open port 5432/tcp on 10.200.0.12
Discovered open port 1524/tcp on 10.200.0.12
Discovered open port 2121/tcp on 10.200.0.12
Discovered open port 6000/tcp on 10.200.0.12
Discovered open port 6667/tcp on 10.200.0.12
Discovered open port 8180/tcp on 10.200.0.12
```

Discovered open port 2049/tcp on 10.200.0.12
Discovered open port 3306/tcp on 10.200.0.12
Discovered open port 25/tcp on 10.200.0.12
Discovered open port 445/tcp on 10.200.0.12
Discovered open port 139/tcp on 10.200.0.12
Discovered open port 513/tcp on 10.200.0.12
Completed SYN Stealth Scan at 01:01, 1.15s elapsed (1000 total ports)
Nmap scan report for www.seclab.net (10.200.0.12)
Host is up, received user-set (0.0014s latency).
Scanned at 2023-11-26 01:01:50 EST for 2s
Not shown: 977 closed ports
Reason: 977 resets
PORT STATE SERVICE REASON
21/tcp open ftp syn-ack ttl 63
22/tcp open ssh syn-ack ttl 63
23/tcp open telnet syn-ack ttl 63
25/tcp open smtp syn-ack ttl 63
53/tcp open domain syn-ack ttl 63
80/tcp open http syn-ack ttl 63
111/tcp open rpcbind syn-ack ttl 63
139/tcp open netbios-ssn syn-ack ttl 63
445/tcp open microsoft-ds syn-ack ttl 63
512/tcp open exec syn-ack ttl 63
513/tcp open login syn-ack ttl 63
514/tcp open shell syn-ack ttl 63
1099/tcp open rmiregistry syn-ack ttl 63
1524/tcp open ingreslock syn-ack ttl 63
2049/tcp open nfs syn-ack ttl 63
2121/tcp open ccproxy-ftp syn-ack ttl 63
3306/tcp open mysql syn-ack ttl 63
5432/tcp open postgresql syn-ack ttl 63
5900/tcp open vnc syn-ack ttl 63
6000/tcp open X11 syn-ack ttl 63
6667/tcp open irc syn-ack ttl 63
8009/tcp open ajp13 syn-ack ttl 63
8180/tcp open unknown syn-ack ttl 63

Firewall IP

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.29 seconds
Raw packets sent: 1005 (44.220KB) | Rcvd: 1000 (40.092KB)
Starting Nmap 7.80 (https://nmap.org) at 2023-11-26 01:09 EST

Initiating Parallel DNS resolution of 1 host. at 01:09
Completed Parallel DNS resolution of 1 host. at 01:09, 0.00s elapsed
Initiating SYN Stealth Scan at 01:09
Scanning 10.200.0.9 [1000 ports]
Completed SYN Stealth Scan at 01:09, 5.08s elapsed (1000 total ports)
Nmap scan report for 10.200.0.9
Host is up, received user-set (0.00034s latency).
All 1000 scanned ports on 10.200.0.9 are filtered because of 990 no-responses and 10 host-prohibiteds

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 5.22 seconds
    Raw packets sent: 1991 (87.604KB) | Rcvd: 10 (720B)

DMZ IP
Starting Nmap 7.80 (https://nmap.org) at 2023-11-26 01:17 EST
Initiating Ping Scan at 01:17
Scanning 10.200.0.10 [4 ports]
Completed Ping Scan at 01:17, 6.04s elapsed (1 total hosts)
Nmap scan report for 10.200.0.10 [host down, received host-unreach]
Read data files from: /usr/bin/../share/nmap
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 6.18 seconds
    Raw packets sent: 8 (304B) | Rcvd: 3 (196B)
Starting Nmap 7.80 (https://nmap.org) at 2023-11-26 02:09 EST
Initiating Parallel DNS resolution of 1 host. at 02:09
Completed Parallel DNS resolution of 1 host. at 02:09, 0.00s elapsed
Initiating SYN Stealth Scan at 02:09
Scanning pc1.seclab.net (10.200.0.101) [1000 ports]
SYN Stealth Scan Timing: About 15.05% done; ETC: 02:12 (0:02:55 remaining)
SYN Stealth Scan Timing: About 30.05% done; ETC: 02:12 (0:02:22 remaining)
SYN Stealth Scan Timing: About 45.05% done; ETC: 02:12 (0:01:51 remaining)
SYN Stealth Scan Timing: About 60.05% done; ETC: 02:12 (0:01:20 remaining)
SYN Stealth Scan Timing: About 75.10% done; ETC: 02:12 (0:00:50 remaining)
Completed SYN Stealth Scan at 02:12, 201.27s elapsed (1000 total ports)
Nmap scan report for pc1.seclab.net (10.200.0.101)
Host is up, received user-set.
All 1000 scanned ports on pc1.seclab.net (10.200.0.101) are filtered because of 1000 no-responses

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 201.41 seconds
    Raw packets sent: 2000 (88.000KB) | Rcvd: 0 (0B)