Chapter 1:

This chapter focuses on network security assessment and will also discuss some common attacking ways. State of the art in network security is that there is a defending competition among attackers and defenders because new attacks are emerging every day. A report of International Institute for Applied Systems Analysis (IIASA) reported that if internet service is stopped in a country, it will lead to food shortage within 3 days. This shows the importance of internet now-a-days, the security of which is really important.

The more the numbers of elements in a network, the more that network will be at risk. There can be many attack surfaces, the most common and famous of which are, as reported by many enterprises: client systems, internet based servers, web applications and the network infrastructure.

1. Client software vulnerabilities and Man in the middle attacks are the main problems of client software.
2. Server side developers don’t look backwards or they are not security conscious as Nginx found chunked encoding security flaw that was already found in Apache HTTP server in 2002.
3. Web application vulnerabilities emerge due to increasing feature support and web API’s exposure among components.

Exposed logic is a way to detect attack surface in a computer system, which an attacker can exploit for its interest. An example of exposed logic was shellshock by which attacker can execute any bash command using important environment variables. Exploiting an exposed logic requires using a chain of defects. A specific attack surface is evaluated at a time. There are 2 main types of security assessment: static analysis and dynamic analysis.

In static analysis, technical audit approaches are:

1. Application code review:

It includes reviewing application code for any leaked code paths, API’s abuse and any other accessible paths. NIST and Wikipedia also provides tools for static code analysis.

1. Design review:

It includes reviewing security controls placement, efficiency and location of these controls within system architecture. An international standard for computer security, Common Criteria, that proposes 7 different security assessment levels from EAL1 to EAL7. But this costs a lot, so mostly experienced security professional highlights most common pitfalls and loop holes in the system.

1. Configuration review:

It includes low-level audit of configurations of system’s components. Some organizations like NIST, NSA and DISA provide complete guidelines for configuration settings regarding security of system components. Most common scanners check for vulnerabilities due to lack of these configuration settings.

In dynamic testing, following components are reviewed during running system states:

1. Network infrastructure testing:

Famous scanners like Nmap and Rapidy7 nexpose assess network infrastructure of a system and scan for known vulnerabilities at OSI layer 2 & 3

1. Web application testing;

OWASP is a list of web application flaws. Tools like BurpSuite and IBM Security AppScan check these vulnerabilities thoroughly in a web application.

1. Web service testing:

A lot of web application processing is done on server side APIs. So web service testing is done for checking any accessible API that can be manipulated and used for privileged access.

1. Internet based social engineering:

The employees in large organizations are not trained to access only valid data online. Due to which spear phishing attacks are an easy way to gain privileged access to organization’s private data.

Chapter 2:

This chapter focuses on most common approaches and tools for vulnerability assessment and the most easily available virtualized environments for security assessments of a system. There is a complete methodology to evaluate a system but there is always a lack of proper approach, due to which there is the difference of results between the evaluation of different evaluators. The best assessment methodology involves 4 main steps:

1. Reconnaissance to identify networks, hosts and users of interests:

This step involves knowing your target as much as possible. There are many websites available where a lot of such information can be found like WHOIS and Google database. We can find private information by this like internal IP addresses.

1. Vulnerability scanning to identify exploitable points:

The information gathered through above step is further scrutinized to identify accessible or vulnerable network services by examining each component individually.

1. Investigation of vulnerabilities and probing manually:

Researchers, when finds the vulnerabilities, they either disclose them to the product vendors/public platforms or sell them to the private organizations i.e. Zero Day Initiative (ZDI). To identify vulnerabilities in a system, a security professional should consult both private and public domains. Public vulnerability sources are:

* + - * NIST National Vulnerability Database
      * Offensive-Security Exploit Database
      * The Full Disclosure mailing list
      * The HackerOne Internet bountybug
      * SecurityFocus
      * Packet Storm
      * CERT vulnerability notes

There are many private or government organizations that sells found vulnerabilities to their customers according to their policies. i.e:

* ZERODIUM
* Exodus Intelligence
* Netragard
* ReVuln

1. Exploitation of vulnerabilities:

These exposed logics are then used by attackers for their own interests by exploiting. There are many well known frameworks for exploitation and also exists the module that extends the frameworks. Most popular frameworks are:

* Rapid7 Metasploit
* CORE Impact
* Immunity CANVAS

There is another iterative assessment approach:

In this approach, the IP addresses, MAC addresses and hostnames found during scanning is again fed to network scanning module that again search for new information within these addresses/information. In this way, more and more exploitable information is searched iteratively.

Testing platform:

There are many tools publicly available for each purpose running on any platforms i.e. windows, Mac OS or Linux based systems. One of the most famous operating system made for security purposes containing most of the security related tools is available known as Kali Linux. It can be made to run on virtualized environments in any platform. There are many online resources available for learning security utilities’ commands i.e:

* [Pentesting Lab---Metasploitable2](https://chousensha.github.io/blog/2014/06/03/pentest-lab-metasploitable-2/)
* [Computer Security Student](http://www.computersecuritystudent.com/)