Computer Network Security

Lesson 4

Vulnerability Assessment and Mitigating Attacks

Lecturer: Dr. Msagha J Mbogholi, PhD

Flashback from Lesson 3

- Application attacks may occur on the server side (cross scripting, SQL/command injection, directory traversal attacks, access rights attacks, privilege attacks) or on the client side (drive-by download, header manipulation, cookies, session hijacking, session fixation, buffer overflow, malicious add-ons)
- Types of network attacks include DoS, DDoS, SIP bandwidth flood, http flood, reflector amplifier, ARP poisoning, DNS poisoning and DoS flood.
- Networks are protected using firewalls (packet filters, proxy firewalls or DMZs), cryptography, IPsec, SSL and Kerberos.
- Attack detection is achieved by the use of IDS; these are based on 3 classifications – host based, network based and anomaly detection based.
- Assessment is done through penetration testing and vulnerability assessment.
- RFC 2196 recommends steps to be followed in handling of security related incidents.

Content

- Vulnerability Assessment
- Assessment Techniques
- Tools for Assessing Vulnerability
- Vulnerability Scanning
- Penetration Testing
- Attack Mitigation

Part 1

Vulnerability Assessment

Vulnerability Assessment

- In lesson 1 a vulnerability was defined as a defect or weakness found in the network system, be it in design, operation or maintenance
- An attacker purposes to find vulnerabilities in the system (network and all its components) in order exploit them and attack it.
- Vulnerability assessment involves the steps taken to identify what resources are of value to the organization (this is what attackers will target), what are the likely threats to these resources, how vulnerable they are, the likelihood of their being attacked (risk), and what to do in the event they are successfully attacked.

Vulnerability Assessment Steps

- Different security experts have described steps taken in performing vulnerability assessment (see securityintelligence.com, purplesec.us and imperva.com for example). While the steps are not explicitly the same in all of them there is a common thread that runs through.
- Vulnerability assessment can be commonly undertaken through the following steps:
  - Identification of resources
  - Threat identification
  - Vulnerability analysis
  - Risk assessment
  - Remediation

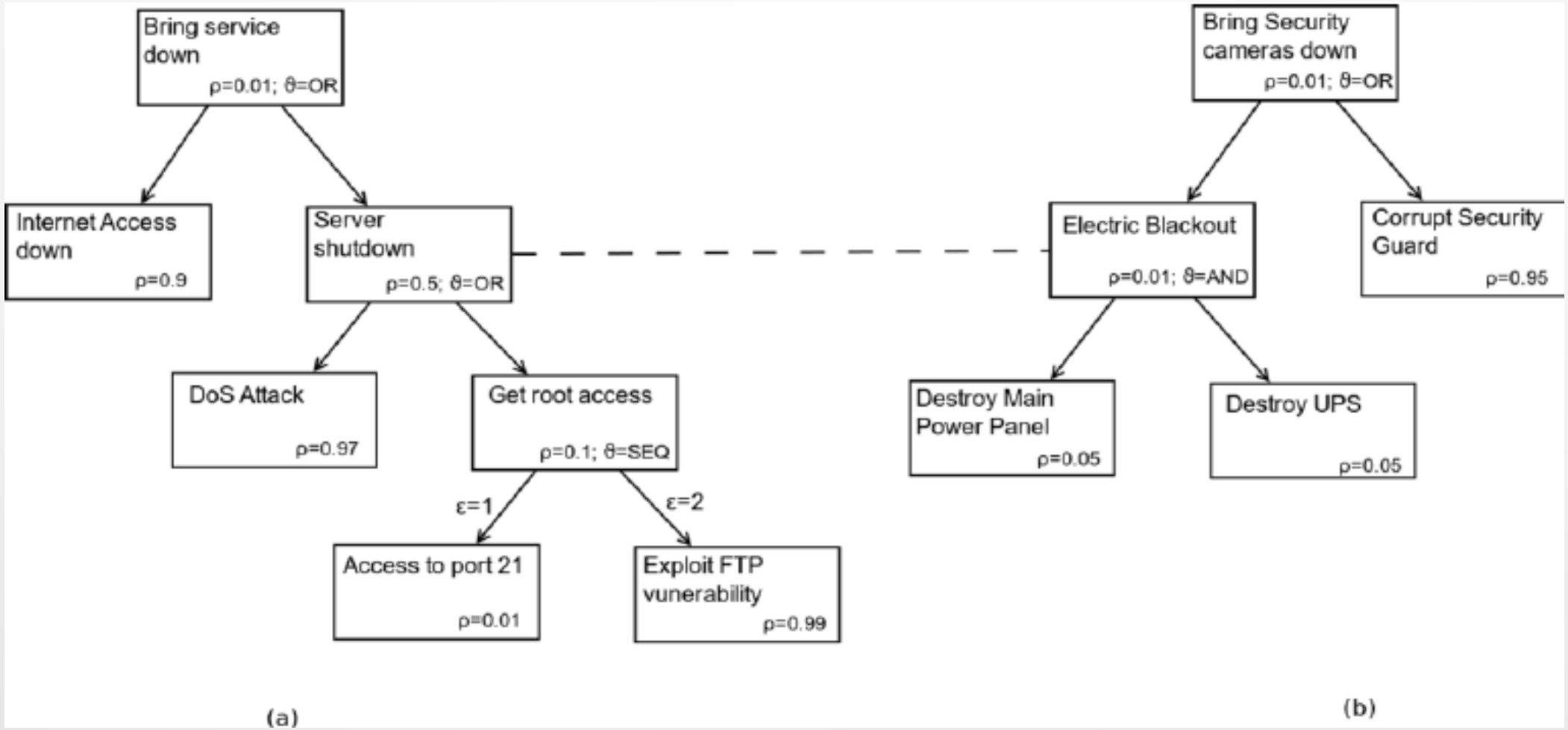
Vulnerability Assessment Steps

- Identification of resources – the purpose of this first step is to identify all the resources that the organization has. These resources should be listed preferably in the order of their value. Resources will include:
  - Human
  - Property (immovable)
  - Hardware
  - Software
  - Data (Information)
- Each resource has a certain value to the organization and the value should be itemized in terms of both monetary and objective value (how critical the resource is to the organization's goals and objectives)
- Objective values can be computed qualitatively, say for example using a Likert scale from 1 to 10, 1 being low objective value and 10 being maximum objective value. As an example the Enterprise Resource Planning (ERP) software will have a value of 10 (very valuable) while the General Manager's tablet might have a value of 2 (does not store valuable information and s/he uses it for informational purposes only; it is also easily replaceable)

Vulnerability Assessment Steps (cont'd)

- Threat identification – the next step is to identify all the likely threats that may be perpetrated by a threat agent. Agents were described in lesson 2. The best way to do this is to make a list of common threat agents. ISO 7498-2 lists destruction of information and/or other resources, corruption or modification of information, theft, removal or loss of information and/or other resources, disclosure of information, and interruption of services, as 5 major security threats. (Jouini et al., 2014) also list further threats in their paper. NIST SP 800-53 also identifies possible threats and their agents.
- Perhaps most importantly is to identify threats that are applicable to the system environment; this is not easy to do. One possible solution to this is to use threat modeling described in lesson 1. Another way to do this is to use an attack tree. An example of an attack tree is shown in fig 1. At the very top of the tree is the final intention, for example, to bring the service down. Subsequent lower levels show possible ways to achieve the level above. For example, to "bring service down" you can either "bring Internet access down" or perform a "server shutdown"…and so on down level by level.

Vulnerability Assessment Steps (cont'd)



- Fig 1. Source: Gribaudo, M., Iacono, M., & Marrone, S. (2015). Exploiting Bayesian Networks for the Analysis of Combined Attack Trees. Electronic Notes in Theoretical Computer Science. 310. 10.1016/j.entcs.2014.12.014.

Vulnerability Assessment Steps (cont'd)

- Vulnerability analysis – at this point the assets have been identified and categorized in terms of monetary and objective value. Further the likely threats against the system have also been identified and cataloged (in a table). The next step is to perform a vulnerability analysis; in this step every resource is listed against the current vulnerabilities it is exposed to. The purpose is to analyze (understand) what dangers currently exist against the resources so that they can be assessed and measures put in place to eliminate (which is near impossible) these dangers. The dangers are what are referred to technically as risks.

Vulnerability Assessment Steps (cont'd)

- Risk assessment – this step purposes to assess or establish what kind of damage is likely to occur should the attack succeed and whether the targeted vulnerability is actually a risk to the organization. The two issues that need to be established are:
  - cost (if and how it can be measured),
  - a measure of how risky the vulnerability is to the organization.
- There are a few suggested and acceptable ways to achieve this.

Vulnerability Assessment Steps (cont'd)

- Both ISO 27001 and NIST SP 800-30 discuss the issue of risk assessment outlining the steps that should be taken in performing risk assessment.
- ISO 27001 suggests assigning scores to risks, the likelihood of them occurring and the damage they can cause; this enables comparable assessment of vulnerabilities/threats in risk assessment. The standard only emphasizes consistency in the assessment.
- NIST SP 800-30 suggests performing an impact analysis that measures loss in terms of the CIA of the data/system, that is, what is the loss if Confidentiality, Integrity or Availability is compromised? The organization can then tabulate the impact in measures of high, medium or low. The SP goes further to suggest finding ways of finding a quantitative measure in assessing the risk in terms of impact. Lastly the document goes further to suggest further measures of impact of the risk.
- In terms of quantitative measures an organization may adopt using formulas such as Single Loss Expectancy (SLE) and Annualized Loss Expectancy (ALE).

Vulnerability Assessment Steps (cont'd)

- SLE = asset value * exposure factor, where the exposure factor is a measure of the impact of the risk (how it reduces) over an asset. For example if an asset (resource) is valued at $ 10000; and the impact of the risk is such that it is reduced by ½ then,
- SLE = 10000 * ½ = $ 5000…..this means that should the attack take place this is the loss in monetary value.
- ALE = SLE * ARO, where ARO is Annualized rate of occurrence of the attack. For example if the SLE is $5000 in the example above and it is determined that an attack can occur 4 times in a year then the ARO is 0.25 meaning,
- ALE = 5000 * 0.25 = $ 1250 ….this means that should the attacks take place then this is the annual loss in monetary value.

Vulnerability Assessment Steps (cont'd)

- Risk mitigation – it is desirable to eliminate risk completely. However, the reality is that this is not practically possible; possible reasons for this is that threats are dynamic and keep changing constantly, it is sometimes ineffective to implement a defense mechanism on a resource as it may affect something else in the system for example data; the reasons are myriad.
- The best thing that an organization can do is to contain the risk. Depending on the outcome of the risk assessment an organization can mitigate risk based on the classification of the risk (low, medium, high) or/and the monetary implications (observed through the SLE and ALE of the resource).
- In an earlier lesson TOM (technical, operational and managerial) controls were discussed and this is the first avenue of risk mitigation.
- However, there are other steps that can be deployed to mitigate risk. These are discussed next.

Vulnerability Assessment Steps (cont'd)

- Risk avoidance – eliminate all situations that may bring the risk about, that is, avoid the risk in the first place.
- Risk assumption – assume that the loss will occur but take insurance to protect against loss (in this case it's presumed that the loss will not be of high magnitude or the likelihood of it happening is low hence taking the risk)
- Risk limitation – limiting the impact of the risk especially in circumstances where it is unavoidable.
- Risk transference – transferring the risk to a third party; a good example of this is outsourcing.
- Risk planning – strategies put in place to manage the risk
- Research and development – research on the risk and develop appropriate countermeasure strategies.

Part 2

Assessment Techniques

Assessment Techniques

- Baseline reporting – this technique is what can be called a 'bare minimum' technique. It works well with small and medium sized organizations. The idea is to set a bare minimum in terms of security controls for the system based mostly on industry best practices; these standards can be obtained from NIST, ISO, CERT and such like standards bodies. This techniques aims to protect against common threats across the enterprise. This has the advantage that it is common across board; however, since it is a standard baseline it does not take special circumstances into consideration. For example security controls in one sector of the company may not work in others, and so on. Further there is always the danger that what is called 'bare minimum' might actually be too much security which might affect performance of the system; conversely it might be too little, which might expose the system to attacks.
- Informal assessment – as the name implies this approach does away with a structured approach to assessing risk. It happens in organizations which might not have the budget for a formal risk assessment, or where the system does not contribute as significantly to their business objectives. In this approach the organization uses the expertise of an outsider or an insider with sufficient knowledge. They will informally do the assessment and implement mitigation measures. Due to the informal nature of this approach consistency in assessment is a challenge as is implementation of the measures over time.

Assessment Techniques (cont'd)

- Detailed risk analysis – this involves following a structured approach to vulnerability analysis such as the one described in the previous section, that is, resource identification, threat identification, vulnerability appraisal, risk assessment and risk mitigation. The NIST SP 800-30 steps may also be followed.
- Combined approach – this involves combining elements of detailed risk analysis, baseline reporting and informal assessment. By incorporating informal assessments into a structured approach and incorporating a baseline reporting structure it is possible to get the best out of all the described approaches. ISO 13335 recommends this approach.

Part 3

Tools for Assessing Vulnerability

Tools

- There are several tools that can be used for performing vulnerability assessments. In this part the functionalities of these tools are discussed. Note that most vendors will have different models (and therefore different model names) for these tools; however, the functionality remains the same.
- Port scanners – when devices communicate over the Internet they use TCP/IP as the protocol of communication. From networking knowledge we know that different services communicate on different ports on the network. In order for a packet to be sent from one device to another using a service it has to be configured with the source and destination port numbers. This tells the receiving device which port the packet needs to access. In order for the packet to be accepted the port must be in an open state, otherwise it will be rejected. Different port numbers are assigned to different services and they listen by keeping the port open. A port may be open (listening meaning service is available), closed(no service listening hence unavailable), or blocked (no responses sent back by host). A hacker using a port scanner will scan all the ports to know which ones are open, closed or blocked. Once the hacker identifies an open port and by extension a service, they can now attempt an attack.

Tools (cont'd)

- Protocol analyzers – they are also known as sniffers or packet analyzers. They monitor packets on the network. They can decode layer 7 network protocols, including http. Protocol analyzers are used by network administrators for troubleshooting and analysis purposes. However, the same device can be used in a mode known as promiscuous mode by a hacker. In this mode the sniffer captures all the packets in the network for analysis purposes, that is to explore vulnerabilities. These devices can operate in two modes: unfiltered mode (promiscuous mode – captures all packets and saves them locally) or filtered mode (packets meeting a certain criteria).
- Vulnerability scanners – these are devices that are used to monitor the network system for vulnerabilities. Functionalities of the vulnerability scanners include:
  - Network environmental weaknesses
  - Risk measure of vulnerabilities based on inbuilt database
  - Mitigation recommendations
  - Application tracking vulnerabilities
  - Tracking of all communicating devices and networks
  - Alerts when port scanning is taking place internally
  - Port usage
  - Identification of sensitive data and which hosts/application have them.

Tools (cont'd)

- Honeypots – these are devices (computers) that are placed in a vulnerable position in the network. They are then loaded with software similar to the ones in the live network but copies/imitations. They are placed there to lure attackers into attacking them. The purpose of this is to observe the hackers' techniques and thus be more prepared to counter them in a live environment.
- Honeynets – similar concept to the honeypot, only this time it is effected in a network that appears to be vulnerable. The net will contain several honeypots as well. When a hacker accesses the network then their methods will have been exposed and thus the real network can be protected further.

Part 4

Vulnerability Scanning

Vulnerability Scanning

- Vulnerability scanning is the use of software to scan an existing system for known vulnerabilities and then producing a report of the findings. Characteristics of vulnerability scanning are:
  - Conducted on existing systems
  - Should be compared against baseline reports
  - Is done in passive mode (testing of the controls)
  - Performed inside security perimeter
  - Does not interfere with normal day to day routine operations

Part 5

Penetration Testing

Penetration Testing

- Penetration testing is normally done by ethical hackers working together in teams popularly known as tiger teams.
- As they are ethical hackers they follow a code of do's and don'ts.
- Characteristics of penetration testing are:
  - Is done in active mode (testing of the controls)
  - Performed outside security perimeter
  - Interferes with normal day to day routine operations
- The result of penetration testing is a report just like in vulnerability scanning.
- Penetration testing (also called pentesting) involves 3 steps:

Penetration Testing: Steps

- Black – box : the tester has no prior knowledge of the network. This is similar to a hacker attempting to access the network from outside; however, in this case the tester may be given an IP address and asked to attempt to hack into the network or website.
- White – box: this mimics an attacker who has knowledge of the network and is now attempting to hack it from the outside. In this case the tester is given all the knowledge and working of the internal network and now attempts to hack from the outside.
- Gray – box (crystal box): this is an in-between. It is similar to an employee (an insider threat) with limited information and access, and now attempts to hack into the system.

Penetration Testing: The Test Plan

- Time when the test will be done?
- Which systems are being targeted in the pentest?
- Types of applications allowed (malicious) for testing purposes?
- What type of testing: black, white or gray?
- Should network admin team be made aware of the testing? (not a good idea)
- What type of damage is allowed, for example can attempts be made to bring down the website?
- What are the do's and don'ts of existing data on the network? (for example attempt to remove the data?)
- Recall that the pentest is a test that aims to protect the CIA of the data. Attacks against these are sometimes called DAD attacks (disclosure, alteration, destruction). …why do you think they are called DAD?

Penetration Testing: The Need?

- Organizations are moving away from the Titanic syndrome, and thus the need for pentesters is increasing by the day.
- Another need for penetration is the dynamism of networking systems today, for example, new malicious code, newer and more user friendly hacking tools, software updates (means more vulnerabilities and malicious code), increased use of Internet and telecommuters (especially since advent of the corona virus), cyber warfare, use of open source software (exposing users to further vulnerabilities since hackers can access source code) , and so on.

Penetration Testing: Attack Stages

- Information gathering – this could be active (using discovery tools) or passive (using publicly available information)
- Scanning – for vulnerabilities using tools like port scanners
- Penetrating – after finding vulnerabilities the tester attempts to penetrate the system, noting where they were successful and where they were not.
- Maintaining access – once the tester has found an entry point (door), they install applications that will allow them to enter and leave at will repeatedly.
- Removing traces – tester attempts to remove any evidence that they were ever there, for instance through erasing log files or checking the events log.

Penetration Testing

- Choosing a penetration tester is a very sensitive task; they should be chosen after doing proper due diligence. This is because the faults they discover may be used against the organization should they fall in the wrong hands.
- After choosing a pentester the final steps should be:
  - How the test will be carried out (engagement rules)
  - NDAs (non-disclosure agreement)
  - How reports will be made and to whom they will be sent.
  - How to dispose of the reports/ or keep in safe custody

Part 6

Attack Mitigation

Attack Mitigation: Techniques

- There are several techniques that can be used to mitigate attacks. These are techniques that can even assist in the deterrence of attacks in some instances. These are:
- Security posture –NIST SP 800-128 defines security posture as "the security status of an enterprise's networks, information, and systems based on information security resources (e.g., people, hardware, software, policies) and capabilities in place to manage the defense of the enterprise and to react as the situation changes." Security posture therefore involves strategy used to defend the enterprise and to react to the different risks. Elements that make up a posture include:
  - Continuous monitoring of the system
  - Baseline configuration – similar to when a baseline report is made
  - Mechanisms to address vulnerabilities before they are attacked.

Attack Mitigation: Techniques

- Configuration of controls – security systems should be put in place for both prevention and deterrence of attacks. They should be configured as such with clear objectives and what they should do in the event of an attack.
- Hardening – this is using different means to protect the system; this is similar to the defense-in-depth concept. In essence it encourages the use of multiple defense mechanisms in different layers.
- Reporting - there should be reporting mechanisms that alert on events occurring in the system. This helps to create awareness and appropriate steps may be taken.

Summary

- Vulnerability assessment can be commonly undertaken through the following steps: Identification of resources, threat identification, vulnerability analysis, risk assessment, remediation
- Assessment techniques are baseline reporting, informal assessment, detailed risk analysis and combined approach
- Tools for assessing vulnerabilities include port scanners, protocol analyzers, vulnerability scanners, honeypots and honeynets.
- Vulnerability scanning is the use of software to scan an existing system for known vulnerabilities and then producing a report of the findings.
- Penetration testing involves 3 steps: black-box, white-box, and gray-box
- Attack mitigation techniques include security posture, configuration of controls, hardening and reporting.

References

- Ciampa, M. D. (2012). *Security+ guide to network security fundamentals* (4th ed.). Course Technology, Cengage Learning.
- Cole, E., Krutz, R. L., & Conley, J. W. (2005). *Network security bible*. Wiley Pub.
- Gribaudo, M.,Iacono, M. & Marrone, Stefano. (2015). Exploiting Bayesian Networks for the Analysis of Combined Attack Trees. Electronic Notes in Theoretical Computer Science. 310. 10.1016/j.entcs.2014.12.014.
- Jouini, M., Rabai, L. B., & Aissa, A. B. (2014). Classification of Security Threats in Information Systems. *Procedia Computer Science*, *32*, 489–496. https://doi.org/10.1016/j.procs.2014.05.452
- Stallings, W., & Brown, L. (2018). *Computer security: Principles and practice* (5th ed.). Pearson.
- Whitaker, A., & Newman, D. P. (2007). *Penetration testing and network defense*. Cisco Press.
- https://www.nist.gov/privacy-framework/nist-sp-800-30
- https://csrc.nist.gov/publications/detail/sp/800-128/final
- https://www.iso.org/isoiec-27001-information-security.html
- https://www.iso.org/standard/14256.html
- https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final