Vulnerability Assessment and Reverse Engineering

Lecture

01

Introduction to Vulnerability Management

Department of Cyber-Security,
Faculty of Computing and Artificial Intelligence,
Air University, Islamabad, Pakistan.

Tentative Course Contents

- Introduction to Vulnerability Management
- Sources of Information
- Program and Organization
- Technology- Vulnerability Scanners
- Automating Vulnerability Management and Dealing With Vulnerabilities
- Hands-On Vulnerability Management
- Preparing to Reverse
- Identification and Extraction of Hidden Components
- The Low-Level Language
- Static and Dynamic Reversing
- RE in Windows and Linux Platforms

Marks Distribution of Course

- Assignments 8%
- Quizzes 8%
- Paper write-up 14%
- Mid-term Exam 25%
- Final 45%

Recommended Readings

- • Practical Vulnerability Management: A Strategic Approach to Managing Cyber Risk by Andrew Magnusson
- • Vulnerability Management 2nd Edition by Park Foreman
- • Mastering Reverse Engineering: Re-engineer your ethical hacking skills by Reginald Wong

Security ??

- A condition that results from the
  - establishment and maintenance of **protective measures**
  - that enables an enterprise to perform its **mission**
  - despite **risks** posed by the threats.

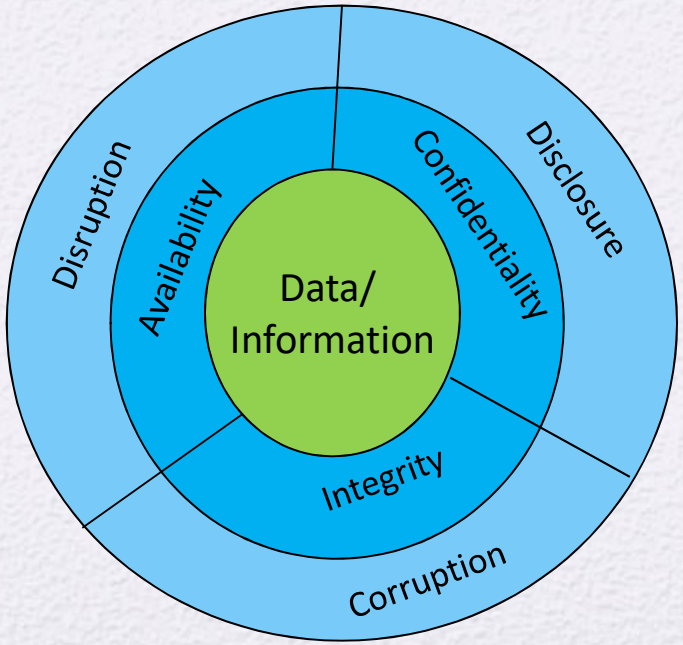
- Ref: NIST Glossary of Key Information Security Terms NIST IR 7298 Rev. 2, 2013
- National Institute of Standards and Technology (NIST), USA

Security ??


“Security is not the goal.
Security is a means by which
we avoid disruptions in order
to reach the company’s goal.”
Tim Crothers
Senior Director of Cybersecurity, Target

Core Concepts of Information Security

- Core concepts of information security are Confidentiality, Integrity, and Availability
- These must be supported by adequate security controls to mitigate the risks of disclosure, corruption, and disruption.



Confidentiality

- Only authorized individual/processes should have access to information on a need-to-know basis
- Supports the principle of least privilege
- Data Classification helps to enforce least privilege
- Access Control through identification, authentication, and authorization helps to stop the access of unauthorized persons to information
- Encryption helps to protect the information even if attacker has access to data

Integrity

- Information should be protected from intentional unauthorized, or accidental changes
- Integrity is related to the Accuracy of information
- Transactions that retain the integrity of the system are sometimes termed as Well formed Transactions
- Change Control helps controls the Integrity of the system and information
- Segregation of Duties and Approval Checkpoints are the administrative controls to maintain the integrity

Availability

- Information is available and accessible to users when needed
- Factors effecting availability
  - Denial of Service Attacks
  - Loss of Service due to Disaster (man-made or natural)
- Controls that support Availability
  - Incident Management Plans,
  - Disaster Recovery Plans,
  - Business Continuity Plan

→ Technical
→ Management

Privacy

- Many definitions of privacy exist

- The right of individuals to control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.
  - Internet Security Glossary, Version 2
  - RFC 4949, 2007
  - https://tools.ietf.org/html/rfc4949

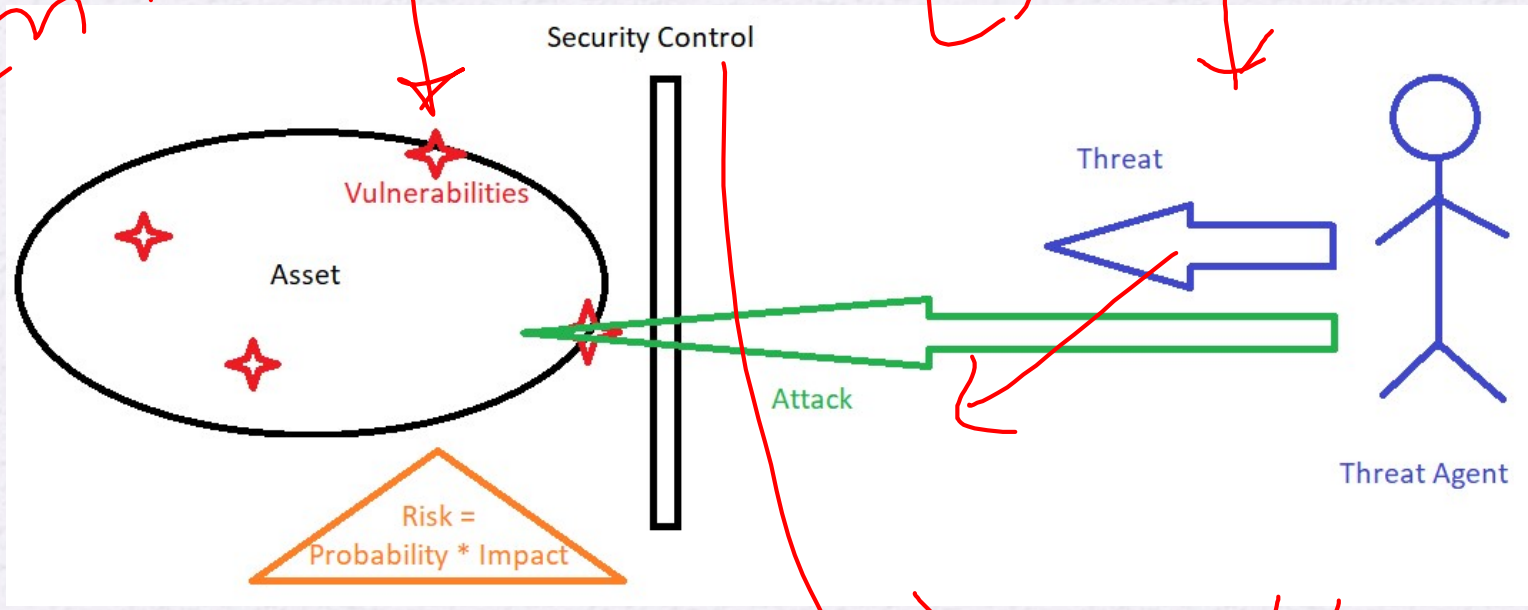
Basic Terminology

- **Vulnerability:** Weakness or lack of a countermeasure (in system or process)
- **Threat agent:** Entity that can potentially exploit a vulnerability.
- **Threat:** The danger of a threat agent exploiting a vulnerability.
- **Risk:** The probability of a threat agent exploiting a vulnerability and the associated impact.
- **Attack:** Realization of the threat.
- **Control:** Safeguard that is put in place to reduce a risk, also called a **countermeasure.**

Threat and Risk

- **Threat** is the combination of:
  - Intent
  - Capability
  - Opportunity
- **Risk** is the combination of the threat and the vulnerability.
- Three key elements to consider are:
  - What to protect (Assets)
  - From whom to protect (Threats)
  - How to protect (Mitigating Controls)

Basic Terminology: Example



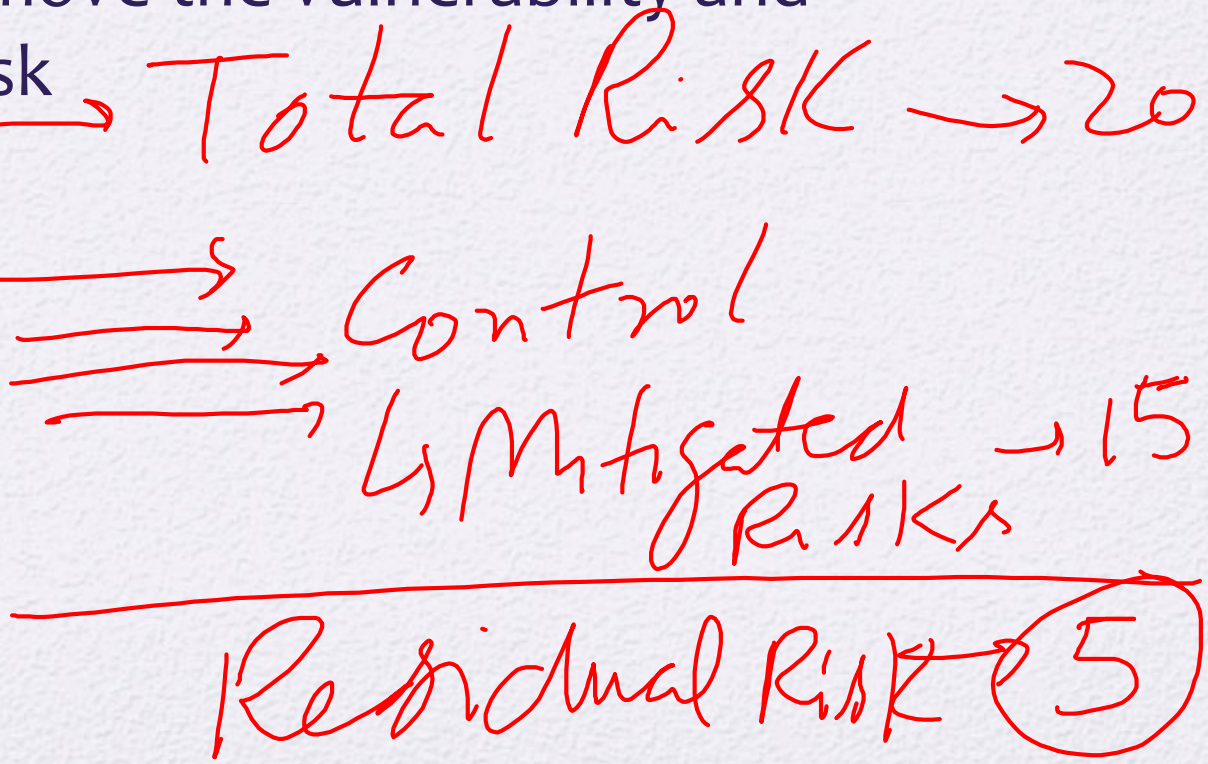
Internal

External

Multiple

Residual Risk

- The amount of risk that is left over even after properly applying the appropriate controls to reduce or remove the vulnerability and associated risk



Protection Provisioning

- Protection for all types of the organizational assets:
  - **Financial Assets** are taken care of by the Finance Department
  - **Human Resource Assets** are taken care of by the HR Department
  - **Physical Assets** are taken care of by the Physical Security Department
  - **Information Assets** are taken care of by the Information Security Department

Security Controls

- NIST SP 800-53r4, 2015
- NIST SP 800-53r5
- Security and Privacy Controls for Information Systems and Organizations
- 20 Control Families with hundreds of controls

ID	FAMILY	ID	FAMILY
AC	Access Control	MP	Media Protection
AT	Awareness and Training	PA	Privacy Authorization
AU	Audit and Accountability	PE	Physical and Environmental Protection
CA	Assessment, Authorization, and Monitoring	PL	Planning
CM	Configuration Management	PM	Program Management
CP	Contingency Planning	PS	Personnel Security
IA	Identification and Authentication	RA	Risk Assessment
IP	Individual Participation	SA	System and Services Acquisition
IR	Incident Response	SC	System and Communications Protection
MA	Maintenance	SI	System and Information Integrity

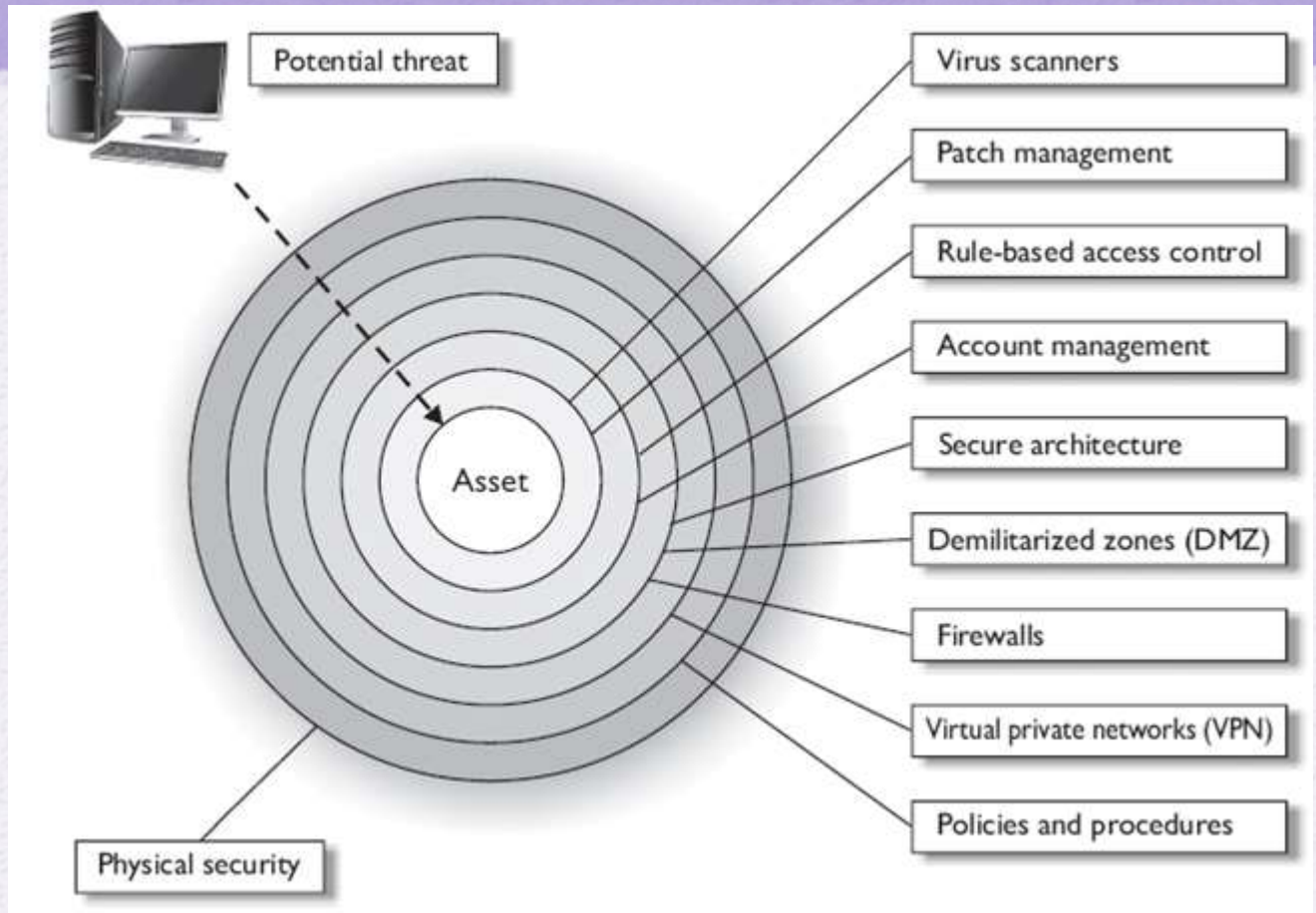
Types of Security Controls

- **Administrative Controls**
  - Risk Management, Security Policy, Regulations, Documentation, Trainings
- **Technical Controls**
  - Software or Hardware Controls
  - Firewall, IDS, Encryption, Authentication
- **Physical Controls**
  - Locks, Security Guards, Alarms, Lighting, Fencing

Control Functionalities

- **Directive:** Specifies acceptable rules of behavior
- **Deterrent:** Discourage a potential attacker
- **Detective:** Identify an incident's activities after it took place
- **Preventive:** Stop an incident from occurring
- **Recovery:** Restore necessary components to return to normal operations
- **Compensating:** Alternate for the loss of primary control
- **Corrective:** Fix items after an incident has occurred

Defense Lines



Defense in Depth Principle: Security should never rely on a single method.
It should be implemented in layers.