Model the system security risk by an Attack Tree

Nayot Poolsappasit, John Edwards

Advisors: Dr. Indrajit Ray

1 Introduction

- Most currently Intrusion detection systems do not give the percep-tion on the potential of collabora-tion of attacks.
- What is missing from these report s is that they could not identify the possible logical connections among these vulnerabilities

2 Approaches

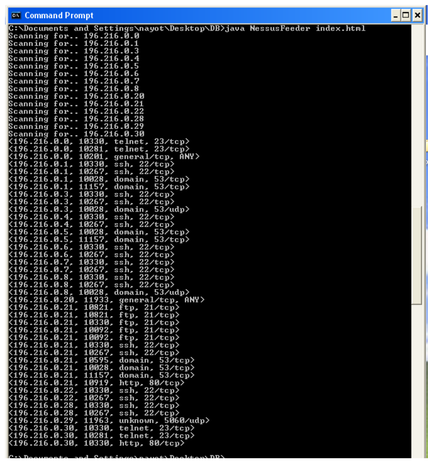
- Propose an attack tree model to represent the security breaches and collaboration among these breaches by illustrating potential attacking scenarios
- Develop an automate tool that generate an attack tree from a given list of initial vulnerabilities and network topology
- Conduct the experimental test on 400+ machines in the CS Department to discover the vulnerabilities and possible attack.

3 What is Attack Tree?

- Attack tree is a systematic met- hod to specify system security based on varying attacks. It helps organize intrusion and misuse scenarios by analyzing system dependencies, and re- presenting these dependencies in the form of a tree structure.

4 The Generation Phases

3. We obtained the vulnerabilities from the network vulnerabilities scanner called ***'Nessus'***
5. Parse the Nessus report to the database
   - This database is specially designed to store the fact about initial vulnerabilities and physical connectivity of a given network named this module as ***The Fact***.
   - On another hand, we retrieve the characteristic of an existing exploits from an outsourcing database and establish possible connections among them by the fact the one exploit can causes a change in system configurations in such a way that becomes a prerequisite of an- other exploit. We name this module ***The Knowledge.***
8. Implement the tool that sys- tematically searches the data- base and correlates attacks from the prerequisites and conseq-uences stored in the knowledge base.



Step 2: Use the Nessus Parser to parse the list of initial vulnerabilities to the database

NessusID	Name	Family	Consequence
10092	FTP Server Detection	Service Detection	Detect the service and version info.
10267	SSH Server type Detection	Service Detection	Detect the service and version info.
10330	Running Service Detection	Port Scan	Detect the service and version info.
10821	FTPD glob Heap Corruption	Remote BOF	Obtain root privilege
14771	Apache htpasswd BOF	Remote BOF	Obtain root privilege
15588	Detect Apache Https	Service Detection	Detect the service and version info.
19361	Compress::Zlib BOF	Local BOF	Obtain user privilege
		...	

Table : Exploits

Table : Connectivities

Host 1	Host 2
0.0.0.0	196.216.0.1
196.216.0.1	196.216.0.21
196.216.0.2	196.216.0.21

Host	Exploit
196.216.0.1	Apache htpasswd BOF
196.216.0.1	Detect Apache Https
196.216.0.2	Compress::Zlib BOF
196.216.0.21	FTP Server Detection
196.216.0.21	Running Service Detection
...	...

FACTS

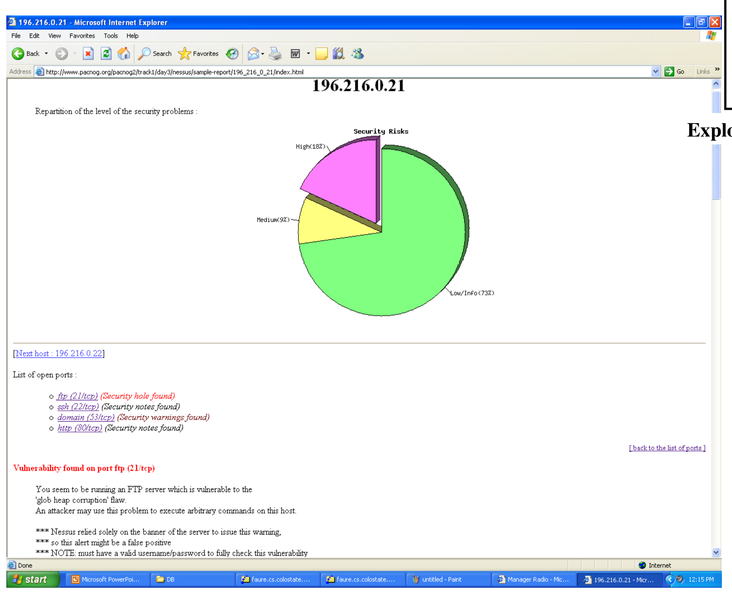
Family	PreRequisite	JoinType
Local BOF	Detect the service and version info.	AND
Local BOF	Obtain user privilege	AND
Port Scan	N/A	N/A
Remote BOF	Connectivity	AND
Remote BOF	Detect the service and version info.	AND
Service Detection	Vulnerable to Port Scan	N/A
...	...	

Relation : PreRequisite

Table : Vulnerabilities

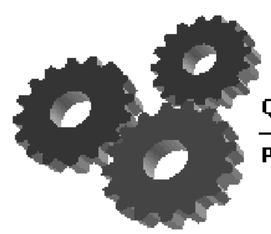
KNOWLEDGE BASE

OUTSOURCING DATABASES
- CVE
- BUGTRAQ
- NESSUS



Step 1: Use Nessus Scanner to obtain the list of system initial vulnerabilities

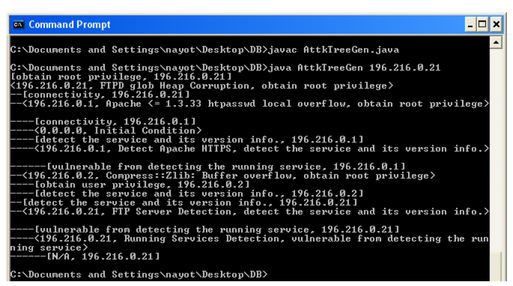
Exploit



Query:

PreRequisite ?

Attack Tree Generator



Step 3: Attack Tree generator recursively queries the database for the known fact and possible connection to the other and build an attack tree to represent the possible attacks scenarios of a given network

5 Conclusion

- We are able to implement an attack generation tool which used to generate an attack tree from a giving list of vulnerabilities from the scanners and network topology.
- Now we are developing the visualization tool to draw an attack tree graphic from a given text result from the tool