



Information Security Analysis and Audit

Course Code: CSE3501

Slot: L47-48

Faculty: Dr. Anil Kumar K

Assessment: 3

18BCI0247

Rohan Allen

Exercise 1:

Experiments in Practical Threat Analysis(PTA) software.

Home page

The screenshot shows the 'Blank_pta.thm' project in the Practical Threat Analysis application. The top menu bar includes File, Edit, Entities, Attachments, Tools, Reports, and Help. Below the menu is a toolbar with various icons. The main area displays project statistics: Assets (0), Threats (0), Vulnerabilities (0), Countermeasures (0), Implemented Countermeasures (0), Entry Points (0), Attacker Types (0), and Tags (0). A link 'Set Project Properties' is visible. The 'Project Properties' section contains fields for Project Name (New), Project Type (Threat Model), Created, Last Update, Project File (Blank_pta.thm), Project Folder (D:\VIT\Fall 2020-2021\Lab\Week 4- Threat Analysis and risk management), Version (1.0.0.1), Author, Company, Categories, Keywords, and Description (Blank threat model template). A cursor icon is visible in the bottom right corner.

Adding Threat:

The screenshot shows the 'Blank_pta.thm' project in the Practical Threat Analysis application. The 'File' menu is open, displaying options: System's Status, New Project..., Open PTA Project... (which is highlighted with a yellow background), Project Properties, Save Changes, Save As..., Save As Library..., Exit, and Preferences. The main area shows the same project statistics and properties as the previous screenshot. A cursor icon is visible in the bottom right corner.

Practical Threat Analysis - [PTA_MedicalDevice_ThreatModel_1.6.thm]

File Edit Entities Attachments Tools Reports Help

PTA_MedicalDevice_ThreatModel_1.6.thm

Assets 4 Set Project Properties

Threats 9

Vulnerabilities 32

Countermeasures 27

Implemented Countermeasures 12

Entry Points 8

Attacker Types 3

Tags 15

Project Properties

Project Name: Patient monitoring device threat analysis

Project Type: Threat Model

Created: 23-07-2010

Last Update: 09-08-2010

Project File: PTA_MedicalDevice_ThreatModel_1.6.thm

Project Folder: C:\Users\Rohan\Downloads\MedicalDeviceThreatModel

Version: 1.4

Author: D. Lieberman

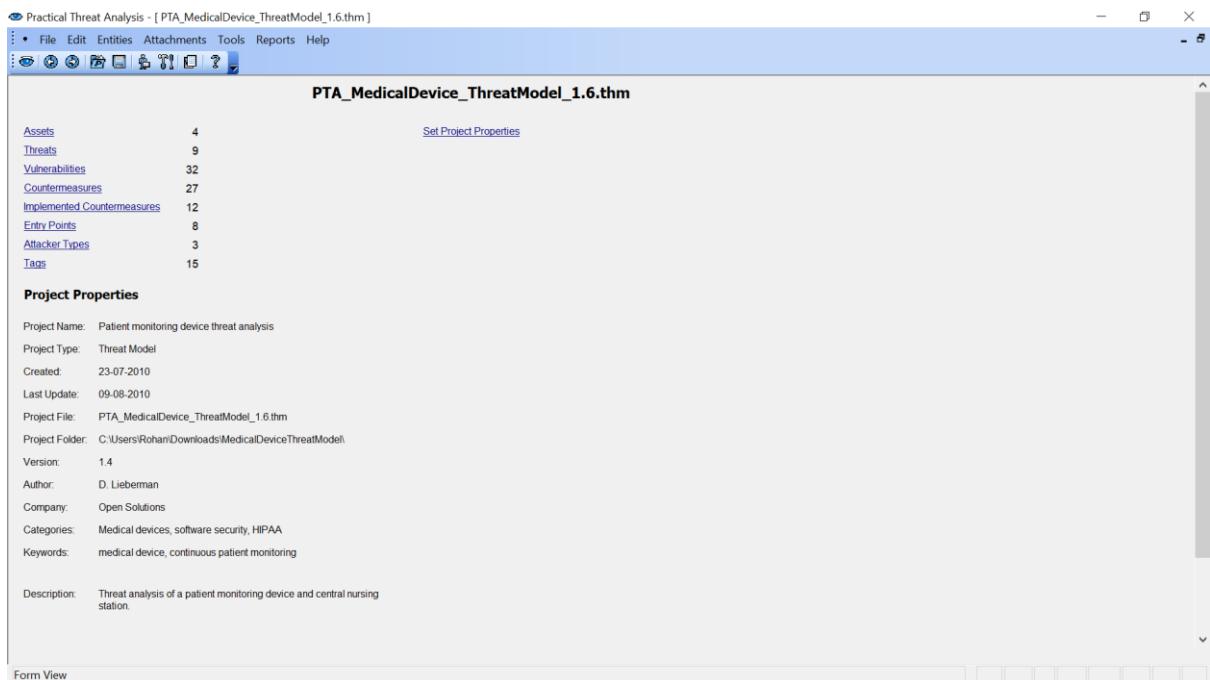
Company: Open Solutions

Categories: Medical devices, software security, HIPAA

Keywords: medical device, continuous patient monitoring

Description: Threat analysis of a patient monitoring device and central nursing station.

Form View



Adding another threat:

Practical Threat Analysis - [PTA_MedicalDevice_ThreatModel_1.6.thm]

Select threat model database

PTA > Samples > CaseStudy1

Search CaseStudy1

Organize New folder

Name Date modified

CallAccountingCaseStudy.thm 05-03-2007 18:14

File name: CallAccountingCaseStudy.thm All PTA Files(*.thm; *.thl)

Open Cancel

Author: D. Lieberman

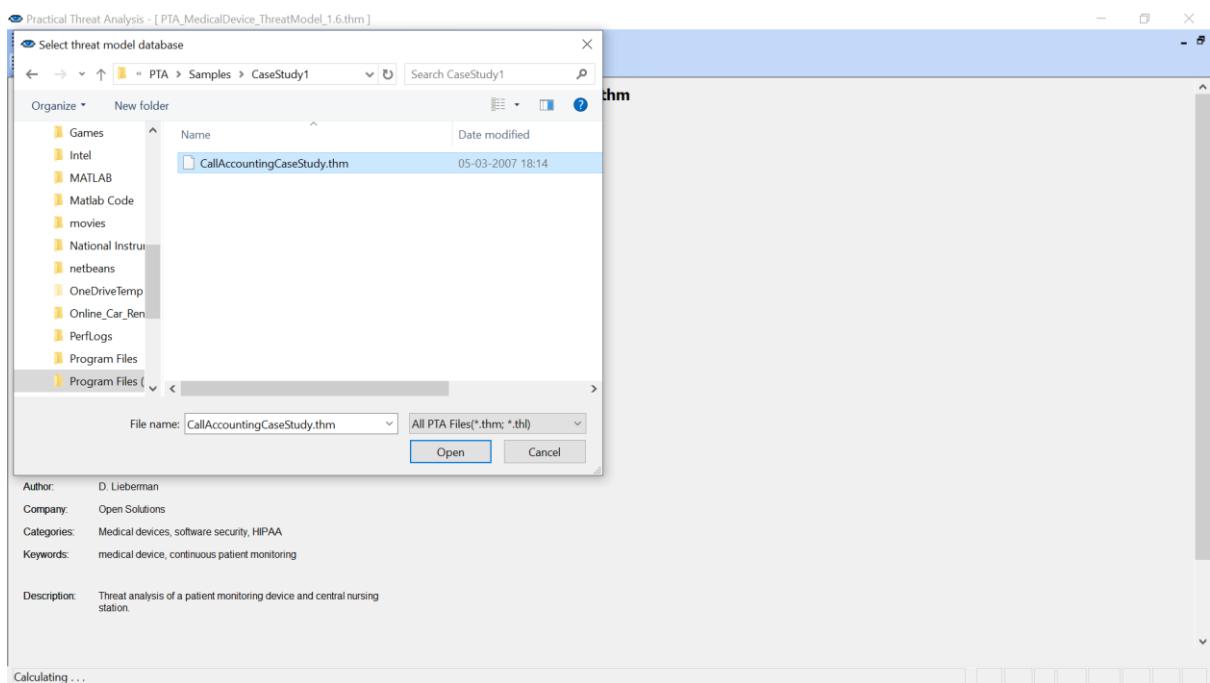
Company: Open Solutions

Categories: Medical devices, software security, HIPAA

Keywords: medical device, continuous patient monitoring

Description: Threat analysis of a patient monitoring device and central nursing station.

Calculating ...



Practical Threat Analysis - [CallAccountingCaseStudy.thm]

File Edit Entities Attachments Tools Reports Help

CallAccountingCaseStudy.thm

Assets 4 Set Project Properties

Threats 11

Vulnerabilities 16

Countermeasures 22

Implemented Countermeasures 0

Entry Points 6

Attacker Types 4

Tags 15

Project Properties

Project Name: Call Accounting Case Study

Project Type: Threat Model

Created: 16-11-2004

Last Update: 05-03-2007

Project File: CallAccountingCaseStudy.thm

Project Folder: C:\Program Files (x86)\PTA\Samples\CaseStudy1\

Version: 1.0.0.3

Author: PTA Development Team

Company: PTA Technologies

Categories: Case Studies

Keywords:

Description:

Form View

Statistics:

Practical Threat Analysis - [CallAccountingCaseStudy.thm]

File Edit Entities Attachments Tools Reports Help

CallAccountingCaseStudy.thm

Assets 4 Set Project Properties

Threats 11

Vulnerabilities 16

Countermeasures 22

Implemented Countermeasures 0

Entry Points 6

Attacker Types 4

Tags 15

Project Properties

Project Name: Call Accounting Case Study

Project Type: Threat Model

Created: 16-11-2004

Last Update: 05-03-2007

Project File: CallAccountingCaseStudy.thm

Project Folder: C:\Program Files (x86)\PTA\Samples\CaseStudy1\

Version: 1.0.0.3

Author: PTA Development Team

Company: PTA Technologies

Categories: Case Studies

Keywords:

Description:

Assets:

Practical Threat Analysis - [CallAccountingCaseStudy.thm]

The screenshot shows the software interface with a toolbar at the top and a main window titled "Assets (4)". Below the title is a table with the following data:

ID	Excluded	Name	Tags	Associated Threats	Fixed Value (?)	Recur. Value (?)	Annual Value (?)	Value (%)	Description
A002		The privacy of call details information	Data, Liability	T001, T002, T010, T011, T014	150,000	0	150,000	6.8	Calls details, especially the dialed and the caller numbers are considered private information that should be protected. The asset's value reflects the maximal liability according to the state's privacy-keeping regulations.
A003		The availability / integrity of the system's passwords	Data	T001	10,000	0	10,000	0.5	If passwords are disclosed then there is a need to run a password change procedure for users' passwords as well as CDRs buffers' passwords. Note that the asset in this case are the passwords themselves and not the damage that may be caused by a malicious use of the passwords.
A011		The availability of the system's Web application and service	Availability, Reputation	T001, T007, T009, T013, T016	0	50,000	50,000	2.3	If the Web application goes down, phone users and managers cannot view phone usage and utilization data. The value reflects the frustration, break of users' confidence and cost of manual handling of users' queries.
A012		The accuracy and integrity of the data in the system's database	Data, Financial	T001, T004, T010, T011, T012, T013, T016	0	2,000,000	2,000,000	90.5	The database includes call records and pricing programs that affect the billing and has direct financial values. The value of the asset reflects the maximal annual loss of income caused by corrupted data.

Threats:

Practical Threat Analysis - [CallAccountingCaseStudy.thm]

The screenshot shows the software interface with a toolbar at the top and a main window titled "Threats (11)". Below the title is a table with the following data:

ID	Excluded	Name	Tags	Probability	Threatened Assets	Exploited Vulnerabilities	Mitigation Plan	Risk (%)	Value At Risk (?)	Description
T001		Intruder accesses the system's application and database servers directly from the Internet	Networking, Application Servers	0.66	A002, A003, A011, A012	V001, V005	C001, C006, C013	66.0	1,458,600	An intruder gains access to the system's computers and database, steals or modifies data and disrupts system operation. This attack may damage most of the system's assets.
T002		Insider accesses database via LAN for extruding private calls data	Data, Networking, Users / Employees	0.49	A002	V003, V004, V005, V009	C002, C003, C004, C006, C007	3.3	73,500	The connection is established from a machine on the local area network.
T004		Intruder corrupts database by injecting malicious SQLs in input fields of Web pages	Data, Application Servers	0.49	A012	V010	C011, C012, C014	44.3	980,000	A sophisticated web attacker may reverse engineer the client side code of a web page and insert malicious SQL statements to be submitted as the value of a page field assuming that it will be transferred to the database 'as is'. The code may include instructions for deleting database objects, altering the data itself or querying the information.
T007		Denial of Service attack on the Web site	Networking, Application Servers	0.66	A011	V013	C018	1.5	33,000	DoS attack prevents data from being available to public.
T009		Intruder or an Internet worm uses HTTP vulnerabilities to break the Web server	Application Servers, Operating System	0.95	A011	V011	C013, C014	1.4	31,350	The attack is performed using well-known exploits in the IIS Web server. The hacker or a worm may change the content of page, insert offensive texts etc...

ID	Excluded	Name	Tags	Probability	Threatened Assets	Exploited Vulnerabilities	Mitigation Plan	Risk (%)	Value At Risk (?)	Description
T010		A malicious user with managerial rights manipulates calls data	Data, Application Servers, Users / Employees	0.49	A002, A012	V004, V014, V027	C019, C021, C022, C033	23.9	528,710	e.g. malicious employee at ASP offices may join forces with other parties for faking calls data or selling private calls information.
T011		Intruder sniffs CDR buffers passwords and then steals or corrupts calls data accumulated in buffers	Data, Telephony Equipment	0.49	A002, A012	V016, V019	C026, C030	47.1	1,040,270	The attack is on the CDR buffers that stores the calls info obtained from the PBX before its transfer to the system's processing pipeline
T012		Technician makes mistakes in scheduling call data collectors	Operational, Data	0.33	A012	V020	C028	9.9	217,800	Calls are lost until the configuration problem is identified and fixed.
T013		Intruder gets control of the call processing pipeline after hacking the Web server machine	Operational, Data	0.49	A011, A012	V011, V012, V020, V026	C013, C014, C028, C032	30.0	662,970	Normal operation of data collection pipeline may be disrupted and calls may be lost. The intruder may stop pipeline service processes, turn off MSMQ, disconnect the database etc.
T014		Managers abuse sensitive private call details	Data, Users / Employees	1	A002	V025	C031, C034	6.8	150,000	This is against Campton privacy regulations.

Vulnerabilities:

ID	Excluded	Name	Tags	Associated Threats	Relevant Countermeasures	Description
V001		Application servers are vulnerable to exploits via the Internet	Networking, Application Servers	T001	C001, C013	Anyone can reach the server machines by scanning the organization network from the internet. This vulnerability can be mitigated by controlling incoming network traffic.
V003		The database passwords may be sniffed from the LAN when establishing connection with the database server	Networking, Application Servers	T002, T016	C003	Insider may learn passwords that are transferred in plain text by using sniffing equipment.
V004		Insiders and power users can access or modify data	Users / Employees	T002, T010	C019, C020, C021	Super-users such as technicians and administrators can modify data.
V005		System data can be extruded via email/http/ftp protocols	Data, Users / Employees	T001, T002	C006, C007	For example: since the application is managed in a campus-external site by an ASP (application service provider) party, there is always the possibility that ASP employee disclose calls sensitive information.
V009		The Web server and the database server machines may be reached from the LAN	Networking, Application Servers, Users / Employees	T002, T016	C002, C003, C004	Unauthorized personnel that have access to LAN can reach the server machines.

ID	Excluded	Name	Tags	Associated Threats	Relevant Countermeasures	Description
V010		MS SQL server is prone to injection of malicious code via Web pages	Data, Application Servers	T004	C011, C012, C014	Malicious SQL code may be injected via input fields and may cause damage to the data and the structure of the database.
V011		MS Server 2003 and IIS 6.0 have deficiencies that enable to exploit OS resources via HTTP protocol	Application Servers	T009, T013	C013, C014	For example: security exploits such as buffer overrun, url canonicalization and other weaknesses that enable malicious activities through HTTP requests.
V012		Web users can access the database	Data, Application Servers, Users / Employees	T013	C014, C032	Without appropriate authentication and authorization mechanism, anyone connected to the Web site may have access to data.
V013		Web servers are exposed to DoS attacks	Networking, Application Servers	T007	C018	A well-known vulnerability.
V014		Employee's personal weaknesses may be exploited by criminal elements	Users / Employees	T010	C022	Especially when working with external ASP.

Countermeasures:

ID	Excluded	Name	Already Implemented	Tags	Mitigated Vulnerabilities	Mitigated Threats	Fixed Cost (?)	Recur. Cost (?)	Annual Cost (?)	Description
C001		Install firewall		Networking, Hardware	V001	T001	5,000	1,000	3,500	The network should be secured by using industry standard firewall, which is configured to block traffic from the internet to the local area network, excluding HTTP requests to the Web site. The cost of the implementation is based on the one time cost of the firewall purchase and deployment.
C002		Enforce quality passwords policy for protecting each of the machines on the network		Operational	V009	T002, T016	0	5,000	5,000	Network users should choose strong passwords that are hard to guess or discover by brute force means. The cost expresses the yearly effort of enforcing the password policy by system administration.
C003		Use Windows integrated authentication policy		Operational	V003, V009	T002, T016	5,000	1,000	3,500	This type of secured login protocol requires the installation of Windows domain controller + Active Directory + Backup domain controller. The cost expresses the one time fee of purchasing the software and the deployment by system administration. Use windows integrated authentication for database login and IMob.
C004		Database login accounts should be given the minimal rights that are necessary for their functionality		Operational	V009	T002, T016	0	2,500	2,500	Web application account that is used for retrieving the daily rates will be assigned with read only permissions. User account should be given update privileges only on relevant data. Database administrator account is the only account with full rights on the database that can access and modify the database and the data. This cost reflects the
C006		Install content leakage prevention system		Operational, Hardware	V005	T001, T002	20,000	0	10,000	Implement extrusion prevention policy to protect personally identifiable information and system configurations from being lost e.g. analyze email content and alert on unauthorized transfer of sensitive assets.

Practical Threat Analysis - [CallAccountingCaseStudy.thm]

File Edit Entities Attachments Tools Reports Help

Countermeasures (22)

ID	Excluded	Name	Already Implemented	Tags	Mitigated Vulnerabilities	Mitigated Threats	Fixed Cost (?)	Recur. Cost (?)	Annual Cost (?)	Description
C007		Create acceptable use policy for email and Internet access		Operational	V005	T002	0	2,500	2,500	Have acceptable use policy, sign all employees and contractors that they have read and understood the policy.
C011		Implement validation of input fields in Web pages		Software Modules	V010	T004	15,000	0	7,500	The cost expresses the one time effort for developing this software feature.
C012		Enforce data access via stored procedures with formal parameters content validation		Data, Software Modules	V010	T004	20,000	0	10,000	Data in database should be manipulated only via stored procedures. The parameters of the stored procedures should be validated before executing the stored procedure. The cost here is the one time effort for developing this software feature.
C013		Enforce deployment of latest security patches for OS, database and Web server		Operational	V001, V011	T001, T009, T013	0	5,000	5,000	The current security patches for all software infrastructures in the system should be maintained. The cost estimation is bases on the yearly effort for deploying the patches by system administration.
C014		Enforce security code review		Software Modules	V010, V011, V012	T004, T009, T013	35,000	0	17,500	Review all system's source codes according to 'secure code writing' industry standards. The cost here is the one time effort for implementing this software review.

Attacker Types:

Practical Threat Analysis - [CallAccountingCaseStudy.thm]

File Edit Entities Attachments Tools Reports Help

Attacker Types (4)

ID	Name	Profile and Motivation	Available Tools and Accessibility
K002	Insider	Malicious insider may be an employee or a subcontractor.	Access to the LAN and calls database.
K003	Hacker		
K004	Commercial Opponent		
K005	Internet Worm		

Entry points:

Practical Threat Analysis - [CallAccountingCaseStudy.thm]

The screenshot shows a software application window titled "Practical Threat Analysis - [CallAccountingCaseStudy.thm]". The menu bar includes File, Edit, Entities, Attachments, Tools, Reports, and Help. Below the menu is a toolbar with various icons. The main area is titled "Entry Points (6)" and contains a table with the following data:

ID	Name	Description
E001	Page of Web application	which is available to the public
E003	Computer workstation on the LAN	
E004	Database Server	
E005	Network	by intrusion
E006	Telephony equipment and data buffers	

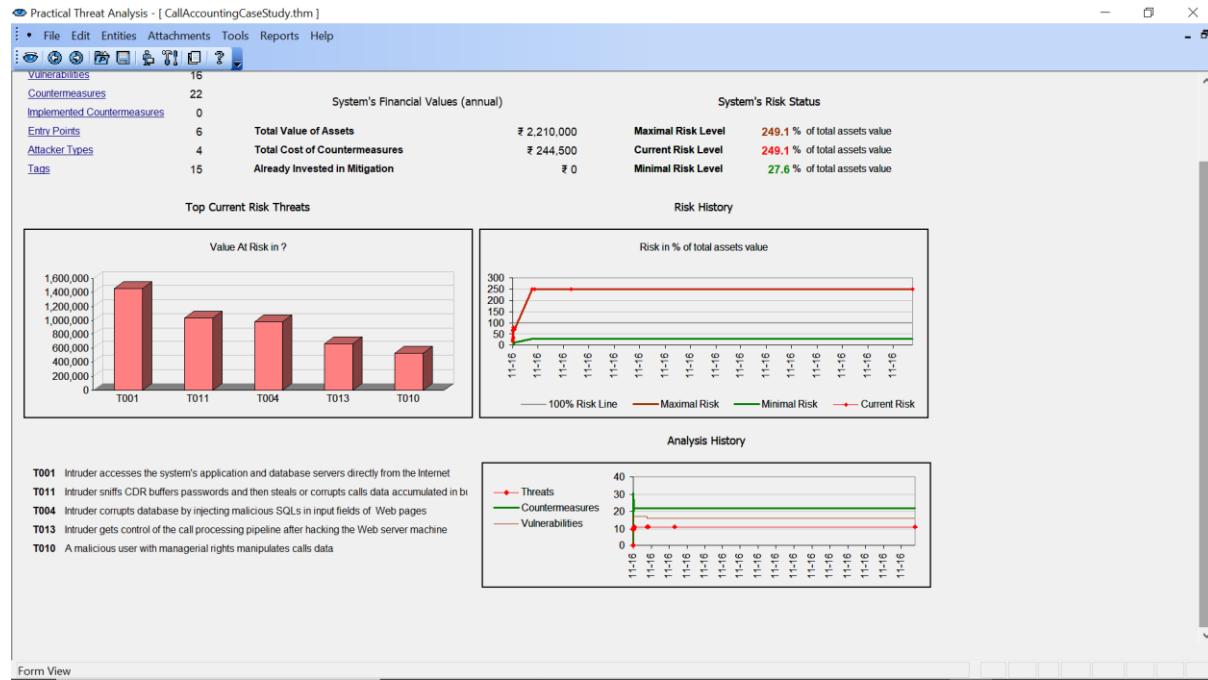
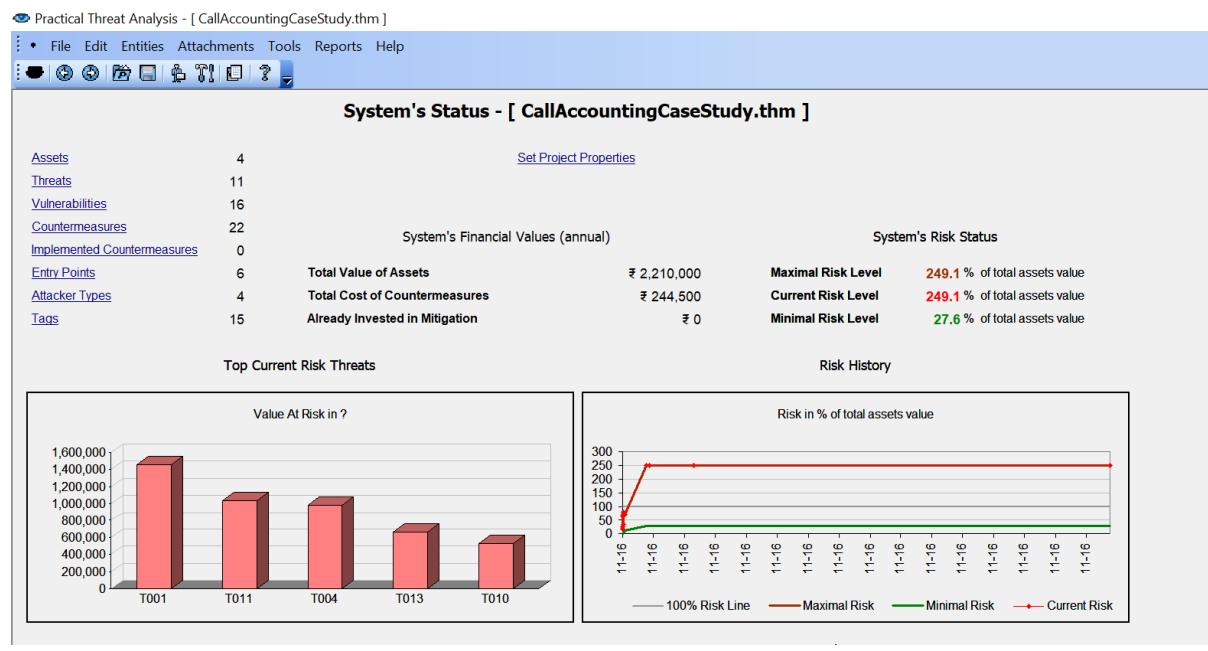
Tags:

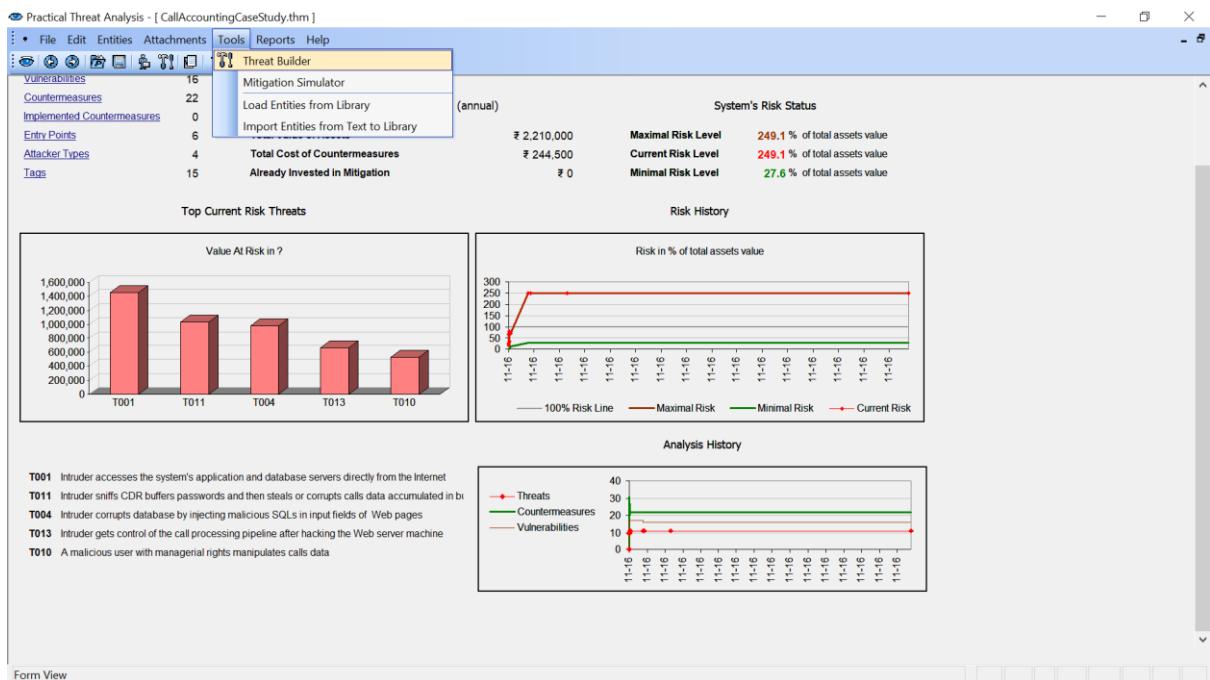
Practical Threat Analysis - [CallAccountingCaseStudy.thm]

The screenshot shows a software application window titled "Practical Threat Analysis - [CallAccountingCaseStudy.thm]". The menu bar includes File, Edit, Entities, Attachments, Tools, Reports, and Help. Below the menu is a toolbar with various icons. The main area is titled "Tags (15)" and contains a table with the following data:

ID	Name	Applicable to Assets	Applicable to Threats	Applicable to Vulnerabilities	Applicable to Countermeasures	Associated Entities
G001	Operational	V	V	V	V	T012, T013, C002, C003, C004, C006, C007, C013, C020, C022, C028, C033
G002	Regulations	V	V	V	V	C022, C034
G003	Data	V	V	V	V	T002, T004, T010, T011, T012, T013, T014, T016, V005, V010, V012, V025, V027, A002, A003, A012, C012, C032
G004	Networking		V	V	V	T001, T002, T007, V001, V003, V009, V013, V016, C001, C018
G005	Application Servers		V	V	V	T001, T004, T007, T009, T010, V001, V003, V009, V010, V011, V012, V013

Threat Assessment:





Creating new threat:

Practical Threat Analysis - [CallAccountingCaseStudy.thm]

File Edit Entities Attachments Tools Reports Help

Threat Builder

Threats (11)

- T001**
Intruder accesses the system's application and database servers directly from the Internet
Probability: 0.66 annual occurrences
- T002**
Insider accesses database via LAN for extruding private calls data
Probability: 0.49 annual occurrences
- T004**
Intruder corrupts database by injecting malicious SQLs in input fields of Web pages
Probability: 0.49 annual occurrences
- T007**
Denial of Service attack on the Web site
Probability: 0.66 annual occurrences
- T009**
Intruder or an Internet worm uses HTTP vulnerabilities to break the Web server

T001 - Intruder accesses the system's application and database servers directly from the Internet

Assets (4) that are damaged by the threat

Asset	Damage (%)
A002 The privacy of call details information	100
A003 The availability / integrity of the system's passwords	100
A011 The availability of the system's Web application and service	100
A012 The accuracy and integrity of the data in the system's database	100

Vulnerabilities (2) exploited by the threat

Vulnerability
V001 Application servers are vulnerable to exploits via the Internet
V005 System data can be extruded via email/http/ftp protocols

Countermeasures (4) that mitigate the threat's vulnerabilities

Countermeasure	In Mitigation
C001 Install firewall	V
C006 Install content leakage prevention system	V
C007 Create acceptable use policy for email and Internet access	
C013 Enforce deployment of latest security patches for OS, database and Web server	V

Practical Threat Analysis - [CallAccountingCaseStudy.thm]

File Edit Entities Attachments Tools Reports Help

Threat Builder

Threats (11)

- T016 Insider accesses database via LAN for corrupting calls data
 - Probability: 0.16 annual occurrences

Assets (2) that are damaged by the threat

	Damage (%)
A011 The availability of the system's Web application and service	100
A012 The accuracy and integrity of the data in the system's database	100

Vulnerabilities (3) exploited by the threat

- V003 The database passwords may be sniffed from the LAN when establishing connection with the database server
- V009 The Web server and the database server machines may be reached from the LAN
- V027 ASP employees can access system resources and data

Countermeasures (4) that mitigate the threat's vulnerabilities

	In Mitigation
C002 Enforce quality passwords policy for protecting each of the machines on the network	V
C003 Use Windows integrated authentication policy	V
C004 Database login accounts should be given the minimal rights that are necessary for their functionality	V
C033 Limit access of ASP employees and technicians to system resources	V

Add | Edit | Remove

Add | Edit | Remove

Form View

Creating new asset:

CallAccountingCaseStudy.thm

Asset Details

ID Name
A012 **The accuracy and integrity of the data in the system's database**

The database includes call records and pricing programs that affect the billing and has direct financial values. The value of the asset reflects the maximal annual loss of income caused by corrupted data.

Temporarily Excluded from threat model and risk calculations

Tags Attached Documents Associated Threats

Tags (2) relevant to the asset

- G003 Data
- G015 Financial

Add Tag... | Edit Tag... | Remove Tag

Asset's Value (in ?)

Fixed Value: last over a period of years

Recurring Value: % of total value of all system's assets

Threat's damage to asset % Threat's Damage Level to Asset ...

Apply | Cancel

Practical Threat Analysis - [CallAccountingCaseStudy.thm]

File Edit Entities Attachments Tools Reports Help

Threats (11)

Threat Builder

Asset Details

- CallAccountingCaseStudy.thm

Tag Details

ID	Name
G020	GRohan

Description Tag's Name

Applicable to Threats
 Applicable to Vulnerabilities
 Applicable to Countermeasures
 Applicable to Assets

Asset's Value (in ?)

Fixed Value: 0 last over a period of 1 years
 Recurring Value: 2,000,000 per year

Recalc Total 2,000,000 per year 90.5 % of total value of all system's assets

Threat's damage to asset 100 % Threat's Damage Level to Asset

Apply Cancel

Form View

Asset Details

ID Name

A012	The accuracy and integrity of the data in the system's database
------	---

The database includes call records and pricing programs that affect the billing and has direct financial values. The value of the asset reflects the maximal annual loss of income caused by corrupted data.

Temporarily Excluded from threat model and risk calculations

Tags Attached Documents Associated Threats

Tags (3) relevant to the asset

- G003 Data
- G015 Financial
- G020 Grohan

Add Tag... Edit Tag... Remove Tag

CallAccountingCaseStudy.thm

Asset Details

ID Name
A017 gRohan

Temporarily Excluded from threat model and risk calculations

Tags Attached Documents Associated Threats

Tags (0) relevant to the asset

Add Tag... Edit Tag... Remove Tag...

Apply Changes in Current Record

The changes introduced to the fields of the current record may impact the threat model parameters and the calculation of the system's risk.

Are you sure you would like to submit these changes to the threat model?

Do not display this prompt again and let PTA automatically submit changes to the current threat model.

[Yes] [No]

Asset's Value (in ?)

Fixed Value: 23,344,444 last over a period of 1 years

Recurring Value: 234,556,624,444 per year

Recalc Total per year % of total value of all system's assets

Threat's damage to asset 16 % Threat's Damage Level to Asset ...

Apply Cancel

Practical Threat Analysis - [CallAccountingCaseStudy.thm]

File Edit Entities Attachments Tools Reports Help

Threats (11)

T016 Insider accesses database via LAN for corrupting calls data

Probability: 0.16 annual occurrences

Threat Builder

T016 - Insider accesses database via LAN for corrupting calls data

Assets (3) that are damaged by the threat

	Damage (%)
A011 The availability of the system's Web application and service	100
A012 The accuracy and integrity of the data in the system's database	100
A017 gRohan	16

Vulnerabilities (3) exploited by the threat

V003 The database passwords may be sniffed from the LAN when establishing connection with the database server
V009 The Web server and the database server machines may be reached from the LAN
V027 ASP employees can access system resources and data

Practical Threat Analysis - [CallAccountingCaseStudy.thm]

File Edit Entities Attachments Tools Reports Help

Mitigation Simulator (0)

Countermeasures (22)		Check the countermeasures that you wish to simulate as implemented		
ID	Countermeasure Name	Cost in (?)	Simulate	
C001	Install firewall	3,500	<input type="checkbox"/>	No
C002	Enforce quality passwords policy for protecting each of the machines on the network	5,000	<input type="checkbox"/>	No
C003	Use Windows integrated authentication policy	3,500	<input type="checkbox"/>	No
C004	Database login accounts should be given the minimal rights that are necessary for their functionality	2,500	<input type="checkbox"/>	No
C006	Install content leakage prevention system	10,000	<input type="checkbox"/>	No
C007	Create acceptable use policy for email and Internet access	2,500	<input type="checkbox"/>	No
C011	Implement validation of input fields in Web pages	7,500	<input type="checkbox"/>	No
C012	Enforce data access via stored procedures with formal parameters content validation	10,000	<input type="checkbox"/>	No
C013	Enforce deployment of latest security patches for OS, database and Web server	5,000	<input type="checkbox"/>	No
C014	Enforce security code review	17,500	<input type="checkbox"/>	No
C018	Install anti-DoS appliance	2,500	<input type="checkbox"/>	No
C019	Develop module for logging changes in data initiated by users	40,000	<input type="checkbox"/>	No
C020	Develop operational protocol for manual changing of data that involves managerial personnel	30,000	<input type="checkbox"/>	No
C021	Develop fraud detection mechanism	20,000	<input type="checkbox"/>	No
C022	Security officer should assure the personal integrity of employees	10,000	<input type="checkbox"/>	No
C026	Use CDR buffers with secure transfer and login authentication protocols	7,500	<input type="checkbox"/>	No
C028	Develop monitoring mechanism for back-end processing (system health)	20,000	<input type="checkbox"/>	No
C030	Develop mechanism for secure managing of CDR buffers passwords	7,500	<input type="checkbox"/>	No
C031	Restrict display of phone numbers and sensitive information in detailed reports	7,500	<input type="checkbox"/>	No
C032	Develop secured passwords and role-based mechanism for Web users	25,000	<input type="checkbox"/>	No
C033	Limit access of ASP employees and technicians to system resources	2,500	<input type="checkbox"/>	No
C034	Enforce employees' liability for disclosing private calls information	5,000	<input type="checkbox"/>	No

[Edit Countermeasure...](#) [Mark](#)

System's Risk

Maximal Risk Level	249.1 %
Current Risk Level	249.1 %
Minimal Risk Level	27.6 %
Simulated Risk Level	249.1 %

System's Financial Values (annual)

Total Value of Assets	₹ 2,210,000
Total Cost of Countermeasures	₹ 244,500
Already Invested in Mitigation	₹ 0
Simulated Mitigation Cost	₹ 0
Simulated Mitigation Level (in %)	0.0

Simulated Top Risk Threats (in ?)

T001	Intruder accesses the system's application and database services
T011	Intruder sniffs CDR buffers passwords and then steals or corrupts them
T004	Intruder corrupts database by injecting malicious SQLs in input
T013	Intruder gets control of the call processing pipeline after hacking it
T010	A malicious user with managerial rights manipulates calls data

[Reset](#) [Use Optimization...](#) [Create Report...](#)

Practical Threat Analysis - [CallAccountingCaseStudy.thm]

File Edit Entities Attachments Tools Reports Help

Mitigation Simulator (1)

Countermeasures (22)		Check the countermeasures that you wish to simulate as implemented		
ID	Countermeasure Name	Cost in (?)	Simulate	
C001	Install firewall	3,500	<input checked="" type="checkbox"/>	Yes
C002	Enforce quality passwords policy for protecting each of the machines on the network	5,000	<input type="checkbox"/>	No
C003	Use Windows integrated authentication policy	3,500	<input type="checkbox"/>	No
C004	Database login accounts should be given the minimal rights that are necessary for their functionality	2,500	<input type="checkbox"/>	No
C006	Install content leakage prevention system	10,000	<input type="checkbox"/>	No
C007	Create acceptable use policy for email and Internet access	2,500	<input type="checkbox"/>	No
C011	Implement validation of input fields in Web pages	7,500	<input type="checkbox"/>	No
C012	Enforce data access via stored procedures with formal parameters content validation	10,000	<input type="checkbox"/>	No
C013	Enforce deployment of latest security patches for OS, database and Web server	5,000	<input type="checkbox"/>	No
C014	Enforce security code review	17,500	<input type="checkbox"/>	No
C018	Install anti-DoS appliance	2,500	<input type="checkbox"/>	No
C019	Develop module for logging changes in data initiated by users	40,000	<input type="checkbox"/>	No
C020	Develop operational protocol for manual changing of data that involves managerial personnel	30,000	<input type="checkbox"/>	No
C021	Develop fraud detection mechanism	20,000	<input type="checkbox"/>	No
C022	Security officer should assure the personal integrity of employees	10,000	<input type="checkbox"/>	No
C026	Use CDR buffers with secure transfer and login authentication protocols	7,500	<input type="checkbox"/>	No
C028	Develop monitoring mechanism for back-end processing (system health)	20,000	<input type="checkbox"/>	No
C030	Develop mechanism for secure managing of CDR buffers passwords	7,500	<input type="checkbox"/>	No
C031	Restrict display of phone numbers and sensitive information in detailed reports	7,500	<input type="checkbox"/>	No
C032	Develop secured passwords and role-based mechanism for Web users	25,000	<input type="checkbox"/>	No
C033	Limit access of ASP employees and technicians to system resources	2,500	<input type="checkbox"/>	No
C034	Enforce employees' liability for disclosing private calls information	5,000	<input type="checkbox"/>	No

[Edit Countermeasure...](#) [Un-Mark](#)

System's Risk

Maximal Risk Level	2.6 %
Current Risk Level	2.6 %
Minimal Risk Level	1.3 %
Simulated Risk Level	2.6 %

System's Financial Values (annual)

Total Value of Assets	₹ 234,582,178,888
Total Cost of Countermeasures	₹ 244,500
Already Invested in Mitigation	₹ 0
Simulated Mitigation Cost	₹ 3,500
Simulated Mitigation Level (in %)	0.0

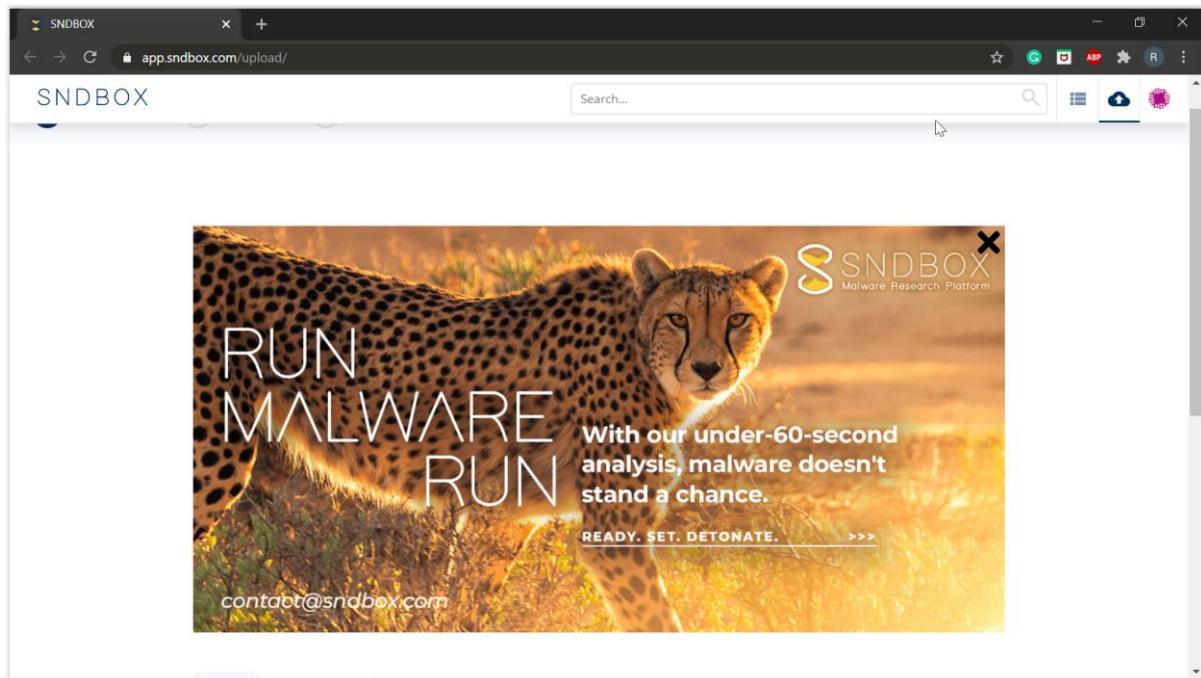
Simulated Top Risk Threats (in ?)

T016	Insider accesses database via LAN for computing calls data
T001	Intruder accesses the system's application and database services
T011	Intruder sniffs CDR buffers passwords and then steals or corrupts them
T004	Intruder corrupts database by injecting malicious SQLs in input
T013	Intruder gets control of the call processing pipeline after hacking it

[Reset](#) [Use Optimization...](#) [Create Report...](#)

Exercise 2:

Malware Analysis on SND BOX platform.



Choosing Malwares:

A screenshot of the SND BOX Public uploads feed. The page title is "Public uploads feed". It displays four recent uploads in a grid format. 1. A file named "file" with a star icon, MD5 hash "cc509a9ed74f566458d78851f2bb7583", and a note "File Dropped". It was uploaded 10 minutes ago and is identified as PE32, Score 100%, and Malicious. 2. A file named "148.csv.exe" with a star icon, MD5 hash "cc1fb6ec9ba914a9672fa1d1051b42d", and a note "File Dropped". It was uploaded 10 minutes ago and is identified as PE32, Score 100%, and Malicious. 3. A file named "24749205" with a star icon, MD5 hash "b775b2bbfd4e587e5bb8de32f18f3000", and a note "File Dropped". It was uploaded 11 minutes ago and is identified as PE32, Score 43%. 4. A file named "file" with a star icon, MD5 hash "bfabae0caa9df130ea1060eb85fcfad", and a note "File Dropped". It was uploaded 11 minutes ago and is identified as PE32, Score 43%.

First Malware:

The screenshot shows the SNDBOX interface with the following details:

OVERVIEW tab selected.

VERDICT: MALICIOUS (highlighted in red).

GENERAL INFORMATION section:

METADATA	
File Name	VC_redist.x64.exe
Tags	+
Upload Date	02/09/2020 10:41 (13 minutes ago)
File size	790.77 KB
MD5	5248ce93557ccb172ccce30ce4360ad4
SHA1	f3c7f66c0f632624db2f5652d1d59fe40eda637
SHA256	3bdbba01701588d005d8ac232e35ear77e408a64d9d04dac524c81292bfba1d11
File type	PE32 executable (GUI) Intel 80386, for MS Windows

PRIVACY DISCLAIMER: This analysis is public. Therefore, it may be accessed by anyone.

ENVIRONMENT SETUP SETTINGS:

- Execution time set to 60 seconds (checked)
- Timebombs enabled with mode calm (checked)
- Command line is disabled (checked)
- RPC Monitoring is enabled (checked)
- Ultrafast mode is disabled (checked)

The screenshot shows the SNDBOX interface with the following details:

SIGNATURES tab selected.

DETECTED BEHAVIOR AND CHARACTERISTICS section:

Behavior	Description	Source	Detection
File Dropped	Dropper Triggered when a process creates an executable	Dynamic Execution	Sandbox Behavior Analyzer
Write To Temp	Generic Writing files to Windows temp folder.	Dynamic Execution	Sandbox Behavior Analyzer
Creation	Process Relationship Process creation by itself is relatively considered a normal behavior for programs to do, for example a browser usually opens child processes and it's legitimate. However in a different context a process creation can be considered malicious. There are processes which in their normal behavior, they do not execute a new process. When an event of such weird behavior occurs, of a not legitimate process creation by an unusual process, there is a high chance it is malicious.	Dynamic Execution	Sandbox Behavior Analyzer

SIGNATURE BREAKDOWN: Signatures sum 4

- Dynamic analysis (red dot)
- Network analysis (red dot)

NAVIGATION sidebar: General Information, Signatures, Dynamic.

Static Analysis:

The screenshot shows the SNDBOX interface with the STATIC ANALYSIS tab selected. On the left, there's a navigation sidebar with a file icon and '99% Malicious' status. The main area displays sections like 'SECTIONS' and 'IMPORT TABLE'. The 'SECTIONS' table includes columns for Name, virtual Size, Virtual Address, Raw Size, and Entropy. The 'IMPORT TABLE' section lists libraries and their functions.

Name	virtual Size	Virtual Address	Raw Size	Entropy
.text	0x00039384	0x00001000	0x00039400	6.507866294463439
.rdata	0x0001a0ec	0x0003b000	0x0001a200	4.96037600549743
.data	0x000030c0	0x00056000	0x00001000	2.7885172697061162
.wixburn	0x00000038	0x0005a000	0x00000200	0.5734966016060967
.tls	0x00000009	0x0005b000	0x00000200	0
.rsrc	0x00003910	0x0005c000	0x00003a00	5.509200780061565
.reloc	0x000688ee	0x00060000	0x000688ee	7.964921883057757

Library	Functions	Address
gdiplus.dll	13	▼
ADVAPI32.dll	44	▼
USER32.dll	25	▼
OLEAUT32.dll	4	▼

The screenshot shows the SNDBOX interface with the NETWORK ANALYSIS tab selected. It displays sections like 'PE VERSIONINFO' and 'CERTIFICATES'. The 'PE VERSIONINFO' section lists various file metadata. The 'CERTIFICATES' section shows a certificate with fields for Subject, Issuer, and Validity Period. At the bottom, there's a 'STRINGS' section with a checkbox for 'Show interesting strings (1)'.

LegalCopyright	Copyright (c) Microsoft Corporation. All rights reserved.
InternalName	setup
FileVersion	14.12.25810.0
CompanyName	Microsoft Corporation
ProductName	Microsoft Visual C++ 2017 Redistributable (x64) - 14.12.25810
ProductVersion	14.12.25810.0
FileDescription	Microsoft Visual C++ 2017 Redistributable (x64) - 14.12.25810
OriginalFilename	VC_redist.x64.exe
Translation	0x0409 0x04e4

Subject	Issuer	Validity Period
countryName: US stateOrProvinceName: Washington localityName: Redmond organizationName: Microsoft Corporation organizationalUnitName: AOC commonName: Microsoft Corporation	countryName: US stateOrProvinceName: Washington localityName: Redmond organizationName: Microsoft Corporation commonName: Microsoft Code Signing PCA	2017-08-11 20:11:15 - 2018-08-11 20:11:15

Show interesting strings (1)

Dynamic Analysis:

The screenshot shows the SNDBOX interface for dynamic analysis. The main navigation bar includes 'OVERVIEW', 'STATIC ANALYSIS', 'DYNAMIC ANALYSIS' (selected), and 'NETWORK ANALYSIS'. A search bar at the top right contains 'Search...'. On the left, a sidebar displays a circular progress indicator showing '99% Malicious' and a list of 'BEHAVIORAL INDICATORS' including 'Process Relationship', 'Generic', and 'Dropper'. The central area features a process flow diagram with two 'EXE' icons connected by a line labeled 'CREATION'. Below the diagram, file names 'vc-redis-x64.pe32' and '3524' are listed. At the bottom, tabs for 'Insights', 'API', and 'API Statistics' are visible, along with 'Info' and 'Community' buttons.

Second Malware:

The screenshot shows the SNDBOX interface for an overview of a second malware sample. The main navigation bar includes 'OVERVIEW' (selected), 'STATIC ANALYSIS', 'DYNAMIC ANALYSIS', and 'NETWORK ANALYSIS'. A search bar at the top right contains 'Search...'. On the left, a sidebar displays a circular progress indicator showing '100% Malicious' and a 'NAVIGATION' section with 'General Information', 'Signatures', and 'Dynamic' options. The central area displays a red box with the 'VERDICT: MALICIOUS' message. Below it, the 'GENERAL INFORMATION' section is titled 'METADATA' and lists file details: File Name (148.csv.exe), Tags (+), Upload Date (02/09/2020 10:48 (11 minutes ago)), File size (977.14 KB), MD5 (ccf1be6e9baf914a9672fa1d1051b42d), SHA1 (4ea486b0bc3dd149fe2f262556533b37e8147f80), SHA256 (added86b964a1e8adbede112fd3d8cc99111014cc87decce1161), and File type (PE32 executable (GUI) Intel 80386, for MS Windows). To the right, the 'ENVIRONMENT SETUP SETTINGS' section includes checkboxes for: Execution time set to 60 seconds (checked), Timebombs enabled with mode calm (checked), Command line is disabled (checked), RPC Monitoring is enabled (checked), and Ultrafast mode is disabled (checked). A note states: 'This analysis is public. Therefore, it may be accessed by anyone.'

The screenshot shows the SNDBOX web application interface. At the top, there's a navigation bar with tabs: OVERVIEW, STATIC ANALYSIS, DYNAMIC ANALYSIS, and NETWORK ANALYSIS. The OVERVIEW tab is selected. On the left, a sidebar titled 'NAVIGATION' includes 'Recently uploaded' (with a 100% Malicious file icon), 'General Information', 'Signatures', and 'Dynamic'. The main content area has a title 'SIGNATURES' and a section 'DETECTED BEHAVIOR AND CHARACTERISTICS' listing four behaviors: 'Startup Persistence', 'File Dropped', 'Write To Temp', and 'Creation'. Each entry includes a 'Source' (Dynamic Execution) and 'Detection' (Sandbox Behavior Analyzer). To the right is a 'SIGNATURE BREAKDOWN' section with a circular gauge showing 'Signatures sum 10' and a legend for 'Dynamic analysis' and 'Network analysis'.

Static Analysis:

The screenshot shows the SNDBOX interface with the STATIC ANALYSIS tab selected. The left sidebar includes 'Recently uploaded' (100% Malicious), 'Sections', 'Import Table', and 'Strings'. The main content area is titled 'SECTIONS' and displays a table with columns: Name, virtual Size, Virtual Address, Raw Size, and Entropy. The table lists various sections of the analyzed file, such as CODE, DATA, BSS, .idata, .tls, .rdata, .reloc, .rsrc, .aspack, .adata, .avtpq, .vbp, .ksj, .gl, and .d, along with their respective memory addresses and entropy values.

Name	virtual Size	Virtual Address	Raw Size	Entropy
CODE	0x0005c000	0x00001000	0x00026800	7.998732756332533
DATA	0x00002000	0x0005d000	0x00000aa0	7.101797874285138
BSS	0x00001000	0x0005f000	0x00000000	0
.idata	0x00003000	0x00060000	0x00000e00	7.879040303226979
.tls	0x00001000	0x00063000	0x00000000	0
.rdata	0x00001000	0x00064000	0x00000200	0.6046612093836843
.reloc	0x00007000	0x00065000	0x00000000	0
.rsrc	0x00008000	0x0006c000	0x00002200	6.701349464085594
.aspack	0x00003000	0x00074000	0x00003000	4.939982544304246
.adata	0x00001000	0x00077000	0x00000000	0
.avtpq	0x00001000	0x00078000	0x00000200	0.8360098342079104
.vbp	0x00001000	0x00079000	0x00000200	1.2295900535469335
.ksj	0x00001000	0x0007a000	0x00000200	3.833145973592239
.gl	0x00001000	0x0007b000	0x00000200	4.627762942667361
.d	0x00001000	0x0007c000	0x00000200	1.024061892702

The screenshot shows the SNDBOX web application interface for static analysis. The main header includes the SNDBOX logo, a search bar, and navigation icons. The left sidebar features a 'Recently uploaded' section with a large red '100% Malicious' badge and a circular progress bar. Below it are sections for 'Sections', 'Import Table', and 'Strings'. The main content area has tabs for 'OVERVIEW', 'STATIC ANALYSIS' (which is selected), 'DYNAMIC ANALYSIS', and 'NETWORK ANALYSIS'. Under the 'STATIC ANALYSIS' tab, the 'IMPORT TABLE' section displays a list of DLL imports with their counts: kernel32.dll (3), user32.dll (1), advapi32.dll (1), oleaut32.dll (1), advapi32.dll (1), version.dll (1), gdi32.dll (1), user32.dll (1), oleaut32.dll (1), ole32.dll (1), oleaut32.dll (1), comctl32.dll (1).

Dynamic Analysis:

The screenshot shows the SNDBOX web application interface for dynamic analysis. The layout is similar to the static analysis view, with tabs for 'OVERVIEW', 'STATIC ANALYSIS', 'DYNAMIC ANALYSIS' (selected), and 'NETWORK ANALYSIS'. The left sidebar includes a 'Recently uploaded' section with a '100% Malicious' badge and a 'BEHAVIORAL INDICATORS' section with options for 'Process Relationship', 'Persistency', and 'Generic'. The main content area displays a process flow diagram where '148-csv.pe32' (3368) creates 'HelpMe.exe' (3472). Below the diagram, the 'Insights' and 'API Statistics' sections are visible. The bottom right corner shows an 'Overview' panel with tables for 'Process' and 'Indicators'.

Process	Indicators
148-csv.pe32	4 indicators
HelpMe.exe	1 indicators

Third Malware:

The screenshot shows the SNDBOX web application interface. At the top, there's a navigation bar with tabs for OVERVIEW, STATIC ANALYSIS, DYNAMIC ANALYSIS, and NETWORK ANALYSIS. The OVERVIEW tab is selected. A large red box highlights the 'VERDICT: MALICIOUS' status. Below this, under 'GENERAL INFORMATION', there's a 'METADATA' section containing file details like File Name (CTFMON.EXE), Tags (+), Upload Date (02/09/2020 10:50), File size (6.91 MB), MD5 (797b00d0bdc5e4906ecaf3d92e8b18b8), SHA1 (f4cdc2c571953afb30859980d2de3256d6e68ef), SHA256 (1648bb750dd1e36907b489795c746e156def53c3d1290c4ae98685a266aa9760), and File type (PE32 executable (GUI) Intel 80386, for MS Windows). To the right, there's a 'PRIVACY DISCLAIMER' section stating 'This analysis is public. Therefore, it may be accessed by anyone.' Below that is an 'ENVIRONMENT SETUP SETTINGS' section with several checkboxes: 'Execution time set to 60 seconds' (unchecked), 'Timebombs enabled with mode calm' (checked), 'Command line is disabled' (checked), 'RPC Monitoring is enabled' (unchecked), and 'Ultrafast mode is disabled' (checked).

This screenshot shows the same SNDBOX interface as above, but with different sections filled. The 'SIGNATURES' section has a 'DETECTED BEHAVIOR AND CHARACTERISTICS' panel stating 'No signatures were captured' and a 'SIGNATURE BREAKDOWN' panel also stating 'No signatures were captured'. The 'ARTIFACTS' section has a 'DETECTED ARTIFACTS' panel stating 'No artifacts were captured'. The 'DYNAMIC' section has a 'PROCESS TREE' panel.

Static Analysis:

The screenshot shows the SNDBOX web application interface for static analysis. The main navigation bar includes links for Overview, Static Analysis (which is selected), Dynamic Analysis, and Network Analysis. A search bar is at the top right. On the left, there's a navigation sidebar with sections for Recently uploaded files (one file shown with 75% completion, labeled 'Malicious'), Sections, Import Table, Version Info, and Strings.

STATIC ANALYSIS

SECTIONS

Name	virtual Size	Virtual Address	Raw Size	Entropy
.text	0x00002ab8	0x00001000	0x00002c00	6.752195275800204
.data	0x00000210	0x00004000	0x000010200	1.0665753701393992
.rsrc	0x00000880	0x00005000	0x00000a00	3.8621182631311743

IMPORT TABLE

Library	Functions	Address
msvcrt.dll	15	
ADVAPI32.dll	6	
KERNEL32.dll	32	
USER32.dll	18	
MSCTF.dll	7	
MSUTB.dll	2	

This screenshot continues the static analysis interface. The navigation bar and sidebar are identical to the previous screen.

PE VERSIONINFO

LegalCopyright	© Microsoft Corporation. All rights reserved.
InternalName	CTFMON
FileVersion	5.1.2600.2180 (xpsp_sp2_rtm.040803-2158)
CompanyName	Microsoft Corporation
ProductName	Microsoft® Windows® Operating System
OleSelfRegister	
ProductVersion	5.1.2600.2180
FileDescription	CTF Loader
OriginalFilename	CTFMON.EXE
Translation	0x0409 0x04b0

STRINGS

Show interesting strings (7)

```
ProfileInitialized
\PM\spip.dll
TF_CreateLangProfileUtil
Indicator
① Internat.exe
RegNotifyChangeKeyValue
advapi32.dll
jh>PE
eFlv|gn
\LanguageProfile
SOFTWARE\Microsoft\CTF\TIP\
ntdll.dll
NtQueryInformationProcess
CoCreateInstance
```

Dynamic Analysis:

The screenshot shows the SNDBOX web interface. The main header says "SNDBOX" and the URL is "app.sndbox.com/sample/1080fa6b-dea2-473e-82bc-d187b6d5de2b/dynamic". The navigation bar includes "OVERVIEW", "STATIC ANALYSIS", "DYNAMIC ANALYSIS" (which is selected), and "NETWORK ANALYSIS". A search bar says "Search...". On the left, there's a "Recently uploaded" section with a circular icon showing "75% Malicious" and a "BEHAVIORAL INDICATORS" section. The main content area shows a file icon for "ctfmon.pe32" (2748). Below it, a detailed view for "ctfmon.pe32" shows tabs for "Info" and "Community". The "Info" tab displays "Overview", "Process", and "Indicators".

Fourth Malware:

The screenshot shows the SNDBOX web interface. The main header says "SNDBOX" and the URL is "app.sndbox.com/sample/000a5ba9-e33f-4e7f-94c9-4dc1472731d9/overview". The navigation bar includes "OVERVIEW" (selected), "STATIC ANALYSIS", "DYNAMIC ANALYSIS", and "NETWORK ANALYSIS". A search bar says "Search...". On the left, there's a "Recently uploaded" section with a circular icon showing "100% Malicious" and a "NAVIGATION" section with links to "General Information", "Signatures", and "Dynamic". The main content area shows a large red box containing the text "VERDICT: MALICIOUS". Below it, a "GENERAL INFORMATION" section shows "METADATA" details like File Name (svchost.exe), Tags (+), Upload Date (02/09/2020 10:55), File size (32.26 KB), MD5 (4e4bfbdb2f3cb7a7a96e2d24d64d0d468), SHA1 (7a9635061b1617f768bc50691b178e8f92a529ed), SHA256 (fa23f6e52c6e80c167940660a47f073b3c43a2adc49ae5e2758c9329d410c66), and File type (PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows). To the right, there are sections for "PRIVACY DISCLAIMER" (public analysis), "ENVIRONMENT SETUP SETTINGS" (with checkboxes for execution time, timebombs, command line, RPC monitoring, and ultrafast mode), and "TIMEBOMBS" (with checkboxes for mode calm and mode aggressive).

The screenshot shows the SNDBOX web application interface. The top navigation bar includes tabs for 'OVERVIEW', 'STATIC ANALYSIS', 'DYNAMIC ANALYSIS', and 'NETWORK ANALYSIS'. The 'OVERVIEW' tab is selected. On the left, a sidebar titled 'NAVIGATION' lists 'General Information', 'Signatures', and 'Dynamic'. The main content area displays a 'SIGNATURES' section with four detected behaviors:

- Startup Persistence**: Persistence. Generic persistency using the startup registry key. Source: Dynamic Execution. Detection: Sandbox Behavior Analyzer.
- File Dropped**: Dropper. Triggered when a process creates an executable. Source: Dynamic Execution. Detection: Sandbox Behavior Analyzer.
- Machine GUID**: Environment Check. Unique machine identifier. Source: Dynamic Execution. Detection: Sandbox Behavior Analyzer.
- Computer Name**: Environment Check. Obtain the hostname of the machine. Source: Dynamic Execution. Detection: Sandbox Behavior Analyzer.

A circular progress bar on the right indicates a 'Signatures sum' of 15, with a breakdown of 10 from 'Dynamic analysis' and 5 from 'Network analysis'.

Static Analysis:

The screenshot shows the SNDBOX web application interface with the 'STATIC ANALYSIS' tab selected. The left sidebar lists 'Sections', 'Import Table', and 'Strings'. The main content area displays the following sections:

Name	virtual Size	Virtual Address	Raw Size	Entropy
.text	0x00007514	0x00002000	0x00007600	5.65377362243594
.rsrc	0x00000240	0x0000a000	0x00000400	4.968771659524423
.reloc	0x0000000c	0x0000c000	0x00000200	0.08153941234324169

The 'IMPORT TABLE' section shows entries for 'mscoree.dll' with one function listed. The 'STRINGS' section contains the following text:

```
!This program cannot be run in DOS mode.
'.rsrc
@.reloc
@.sw
v2.0.50727
#Strings
<Module>
System.Runtime.CompilerServices
```

The screenshot shows the SNDBOX web application interface for static analysis. The main header reads "SNDBOX" and the URL is "app.sndbox.com/sample/000a5ba9-e33f-4e7f-94c9-4dc1472731d9/static". The navigation bar includes tabs for "OVERVIEW", "STATIC ANALYSIS" (which is selected), "DYNAMIC ANALYSIS", and "NETWORK ANALYSIS". A search bar at the top right contains the placeholder "Search...". Below the tabs, there are sub-tabs for "Library", "Functions", and "Address", with "mscoree.dll" selected and the count "1" displayed. The main content area is titled "STRINGS" and lists various memory addresses and their corresponding strings. One string, "Stub.exe", is highlighted with a red oval and a question mark icon, indicating it is a point of interest. Other strings listed include GetBytes, DeleteSubKey, System.IO.Compression, GZipStream, CompressionMode, set_Position, BitConverter,ToInt32, GetProcessById, get_MainWindowTitle, DateAndTime, get_Now, get_ProcName, Keyboard, get_Keyboard, get_ShiftKeyDown, get_CapsLock, Tolpper, StringBuilder, get_CtrKeyDown, Remove, STAThreadAttribute, avicap32.dll, and user32.dll.

Dynamic Analysis:

The screenshot shows the SNDBOX web application interface for dynamic analysis. The main header reads "SNDBOX" and the URL is "app.sndbox.com/sample/000a5ba9-e33f-4e7f-94c9-4dc1472731d9/dynamic". The navigation bar includes tabs for "OVERVIEW", "STATIC ANALYSIS", "DYNAMIC ANALYSIS" (which is selected), and "NETWORK ANALYSIS". A search bar at the top right contains the placeholder "Search...". Below the tabs, there are sub-tabs for "Process Relationship", "Environment Check", and "Persistency". The main content area displays a timeline of process creation events. It starts with "svchost.exe" (3736) creating "spoolsv.exe" (1392). This process then creates "netsh.exe" (3536). Each process is represented by a small icon and its name and PID. At the bottom left, there are links for "Insights", "API", and "API Statistics". At the bottom right, there is a "Community" section with tabs for "Info" and "Community". The "Info" tab is selected, showing an "Overview" table with three rows: "Process" (spoolsv.exe, svchost.exe, netsh.exe) and "Indicators" (4 indicators, 4 indicators, 3 indicators).