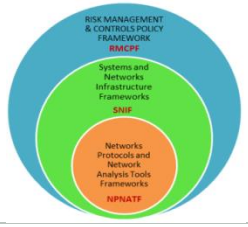
Keywords: *Cyber Risk Management, Cybersecurity and Penetration Testing, Computer Science Curricula, Professional Standards of Practice, Networks Protocols and Network Analysis, Systems and Networks Infrastructure, Risk Management & Controls Policy, Access to Technologies and Innovations, Innovative design and development Practices, Technology Innovations Impacting Engineering and Engineering Technology Education, STEM Education Developments.*



TOWARD INTEGRATED ENTERPRISE RISK MANAGEMENT, MODEL RISK MANAGEMENT, & CYBER-FINANCE RISK MANAGEMENT:

BRIDGING NETWORKS, SYSTEMS, AND, CONTROLS FRAMEWORKS FOR CYBERSECURITY CURRICULA & STANDARDS DEVELOPMENT

Yogi

Dr. Yogesh Malhotra

PhD, MSQF, MSCS, MSNCS, MSAcc, MBAEco, BE,
C.Eng., CCP/CDP, CISSP, CISA, CEH
Who's Who in America®, Who's Who in the World®,
Who's Who in Finance & Industry®,Who's Who in Science & Engineering®
Founder & Chief Research Scientist,
Global Risk Management Network, LLC

www.yogeshmalhotra.com dr.yogesh.malhotra@gmail.com

2015 NY Cyber Security & Engineering Technology Association Conference, Oct. 22, 2015
Rochester Institute of Technology, Rosica Hall, NTID, Rochester, New York

ABSTRACT

- Cybersecurity practices transitioning to Risk Management.
- Necessary to align Professional Standards & Curricula in sync.
- Current Standards & Curricula seem fragmented across:
  - **NPNATF** **Networks** Protocols & Network Analysis Tools Frameworks
  - **SNIF** **Systems** and Networks Infrastructure Frameworks
  - **RMCPF** Risk Management & **Controls** Policy Frameworks

Proposed Framework for aligning, integrating, and, streamlining Standards & Curricula across the **above three levels** to align them with needs of applied Risk Management practices.

BACKGROUND & FUTURE RESEARCH

- Following Risk Modeling for **Wall Street Banks**: **$1 Trillion AUM**
- **2,000-Hour Pen Testing** in NY-State & EC-Council DarkNets.
- Applied Tools: **Kali Linux, Metasploit, Nmap, Wireshark**, etc.
  - www.yogeshmalhotra.com/projects.html#Cybersecurity
- Applied Focus on Voice and Data Telecom Networks.
- 'Weakest Links' in underbelly of Global Banking & Finance.

Future Research: www.FutureOfFinance.org.

*2015 Princeton Quant Trading Conference: **C**yber-**F**inance*.

Future of Finance Beyond ***Flash Boys***: Post-HFT Cyber Risk Management.

Background: **E**nterprise **R**isk **M**anagement & **M**odel **R**isk **M**anagement

- www.yogeshmalhotra.com/blackswans.html

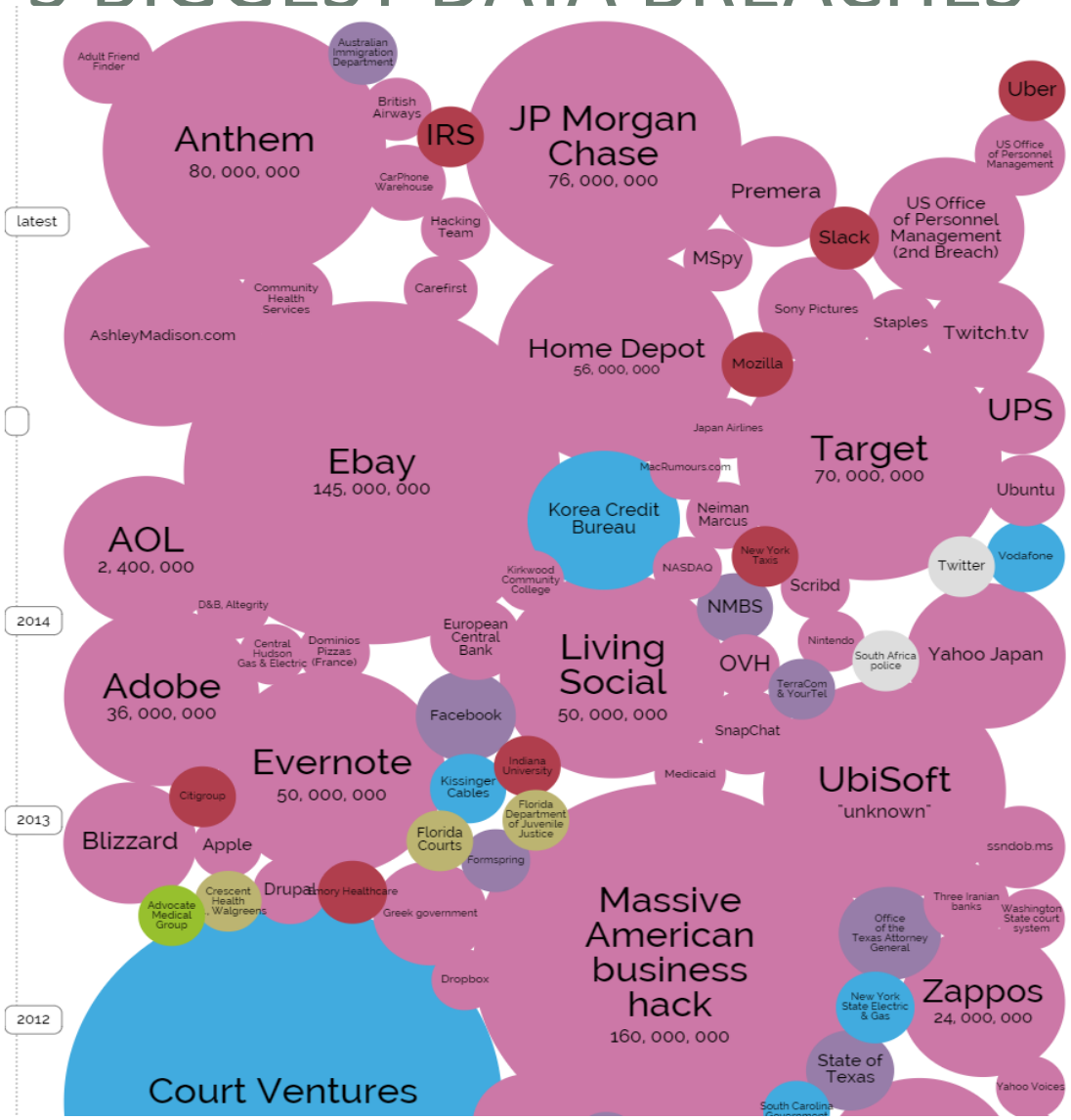
http://www.informationisbeautiful.net

WORLD'S BIGGEST DATA BREACHES

METHOD OF LEAK

- all
- accidentally published
- hacked
- inside job
- lost / stolen computer
- lost / stolen media
- poor security

No. of Records Stolen



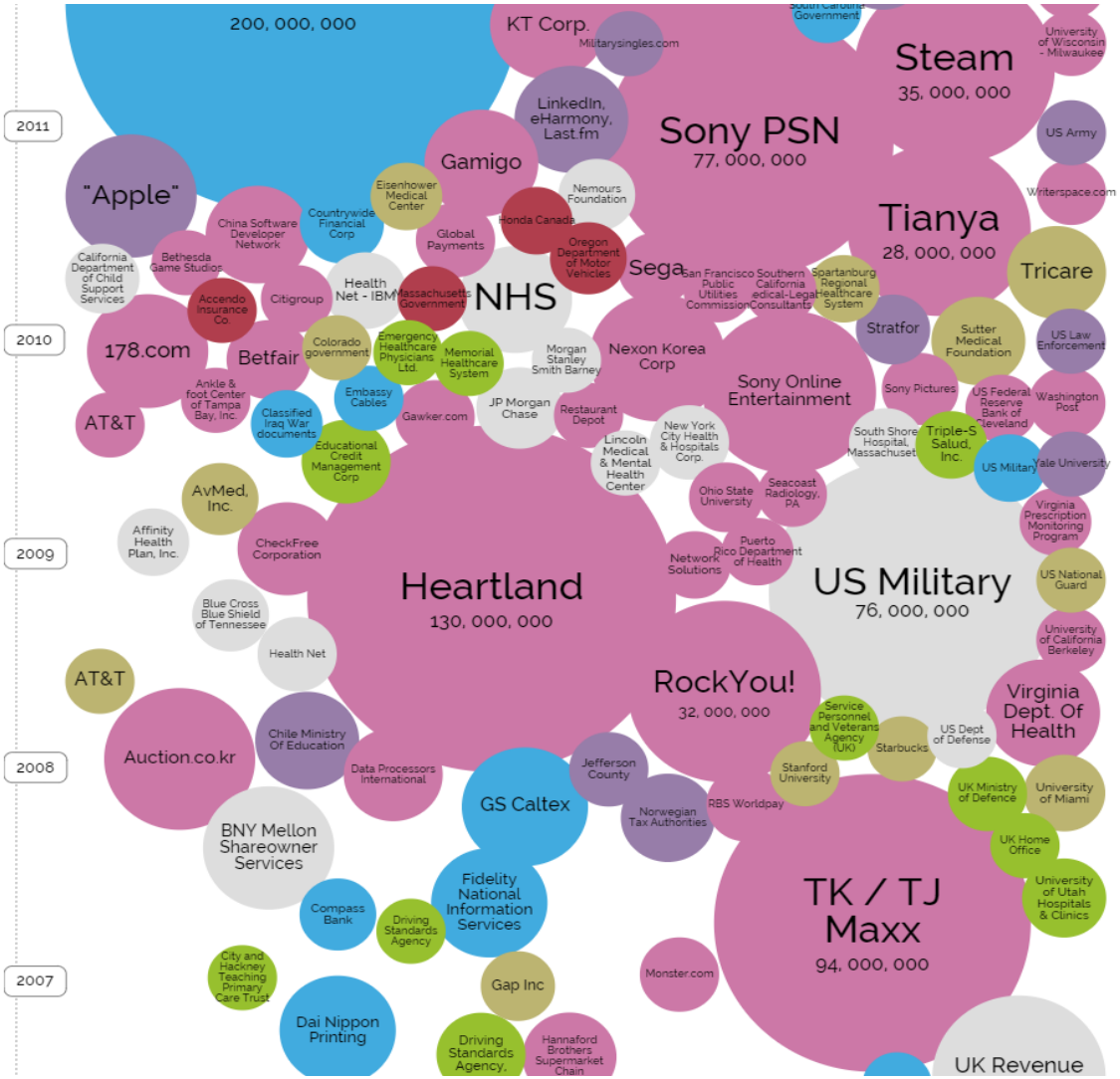
http://www.informationisbeautiful.net

WORLD'S BIGGEST DATA BREACHES

METHOD OF LEAK

- all
- accidentally published
- hacked
- inside job
- lost / stolen computer
- lost / stolen media
- poor security

No. of Records Stolen



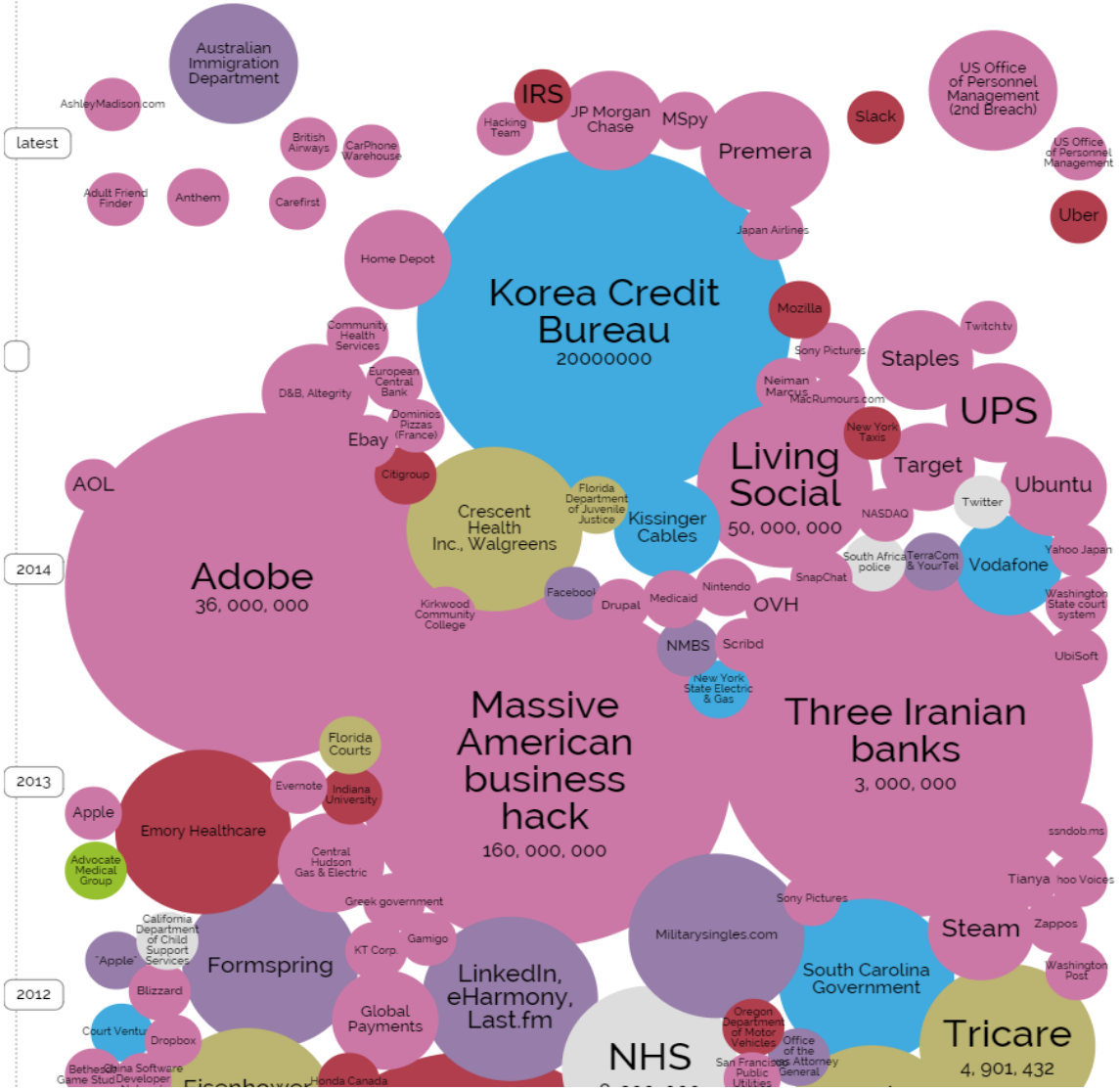
http://www.informationisbeautiful.net

WORLD'S BIGGEST DATA BREACHES

METHOD OF LEAK

- all
- accidentally published
- hacked
- inside job
- lost / stolen computer
- lost / stolen media
- poor security

Data Sensitivity



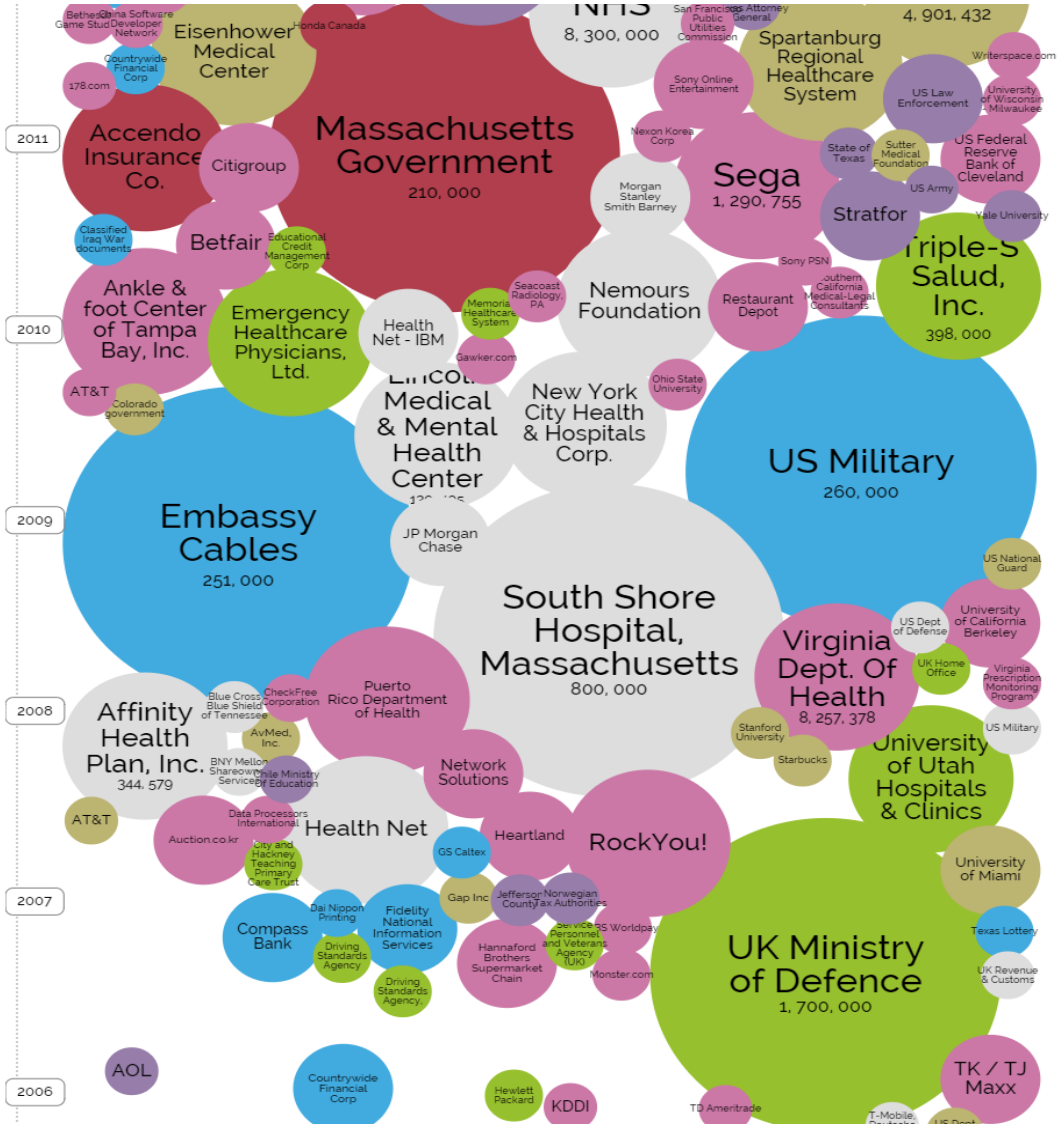
http://www.informationisbeautiful.net

WORLD'S BIGGEST DATA BREACHES

METHOD OF LEAK

- all
- accidentally published
- hacked
- inside job
- lost / stolen computer
- lost / stolen media
- poor security

Data Sensitivity



Threat of a Cryptoapocalyse 2015

Trust is at the breaking point:
The idea of a Cryptoapocapyse is far from science fiction. Heartbleed was just a taste of what this could look like. Could a website be trusted? How many keys were compromised? Could an organization be trusted online? The era of cloud computing, parallel processing, and GPUs are being used to test these attacks. The cost to compromise a MD5-signed digital certificate is now $0.65[17] in Amazon AWS, down from $200,000 in less than two years.[18]

MOST ALARMING THREATS
(IN ORDER OF CONCERN)

1. WEAK CRYPTOGRAPHIC EXPLOIT
2. MOBILE CERTIFICATE MISUSE
3. CODE-SIGNING CERTIFICATE MISUSE
4. MALICIOUS MITM CERTIFICATES
5. SSH KEY MISUSE
6. SERVER CERTIFICATE MISUSE

2015 Cost of Failed Trust Report: Trust Online is at the Breaking Point, Ponemon Institute, 2015.

NPNATF, SNIF, RMCPF

3 LEVELS OF FRAMEWORKS ANALYZED

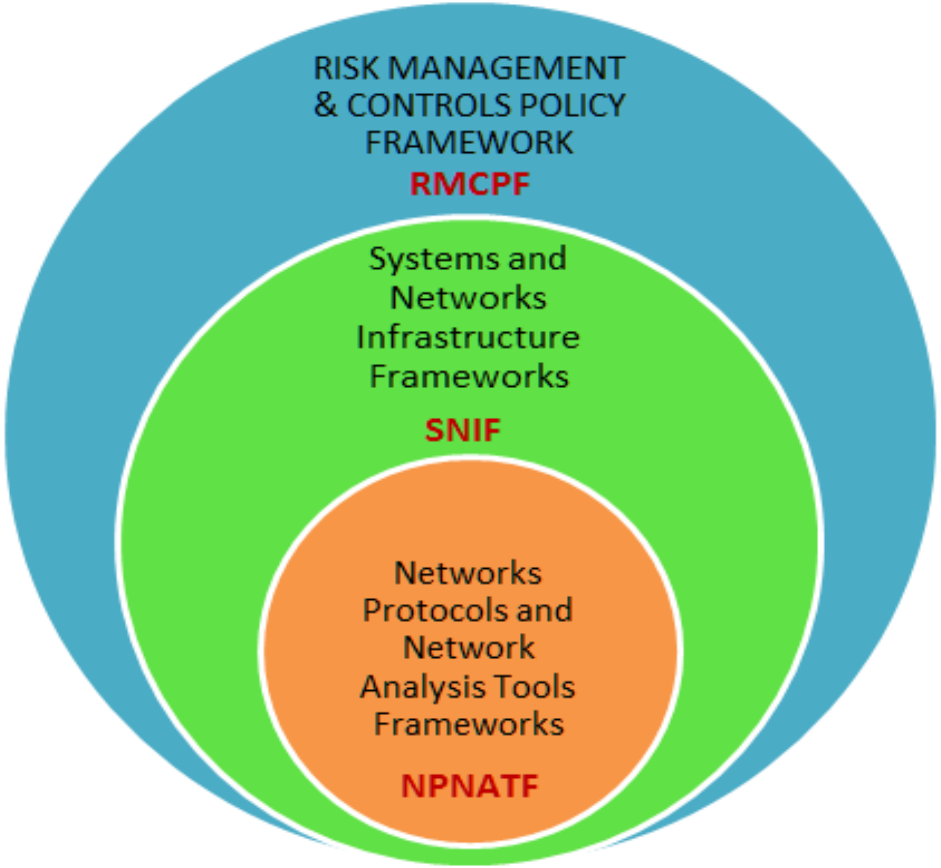
- Diverse frameworks have different levels and scopes
- **N**etworks **P**rotocols & **N**etwork **A**nalysis **T**ools **F**rameworks
  - Penetration Testing, Vulnerability Analysis & Auditing
    - Technically sophisticated Tool & Protocol Level
- **S**ystems & **N**etworks **I**nfrastructure **F**rameworks
  - Penetration Testing, Vulnerability Analysis & Auditing
    - Focus on Infrastructure, specifically Systems & Networks
- **R**isk **M**anagement & **C**ontrols **P**olicy **F**rameworks
  - Typically Policy Level and Strategy Level
    - Less specific to VoIP, Less granular in application to VoIP

INDUSTRY PRACTICES RESEARCH

What are the specific risks related issues that intersect across the 3 levels of analysis.

How the 3 levels relate to each other in various aspects in their focus on risks.

How the 3 levels need to address risks concerns spanning multiple levels.

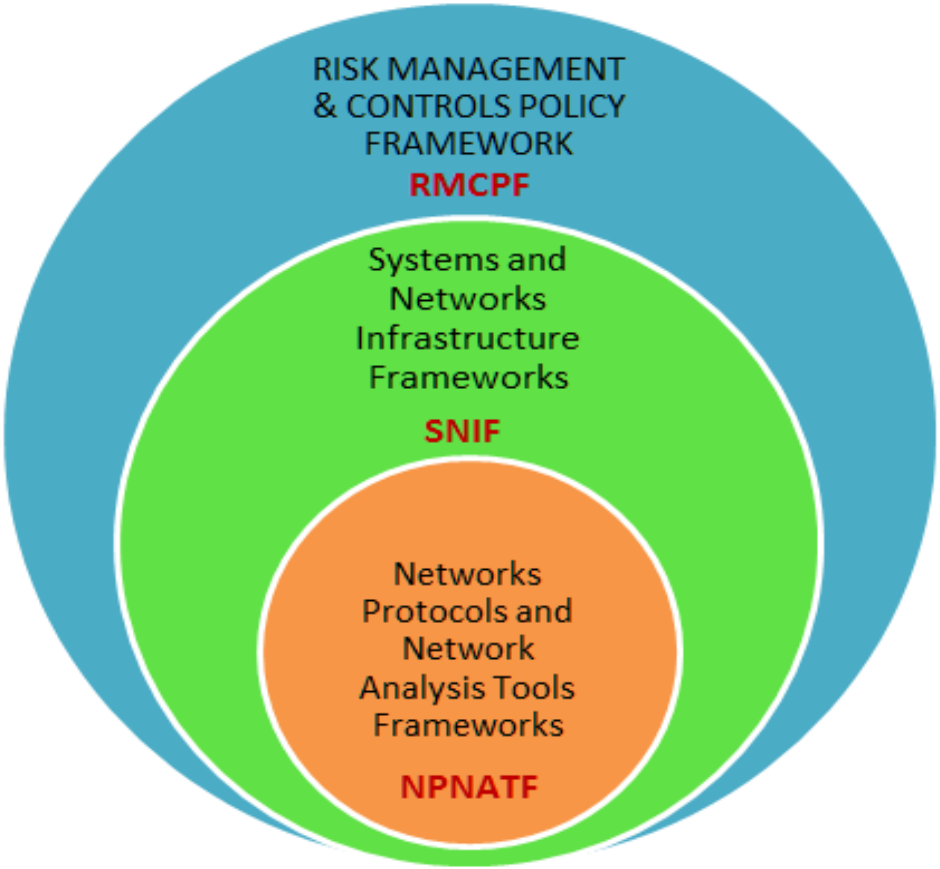


PROPOSED RISK MANAGEMENT FRAMEWORK

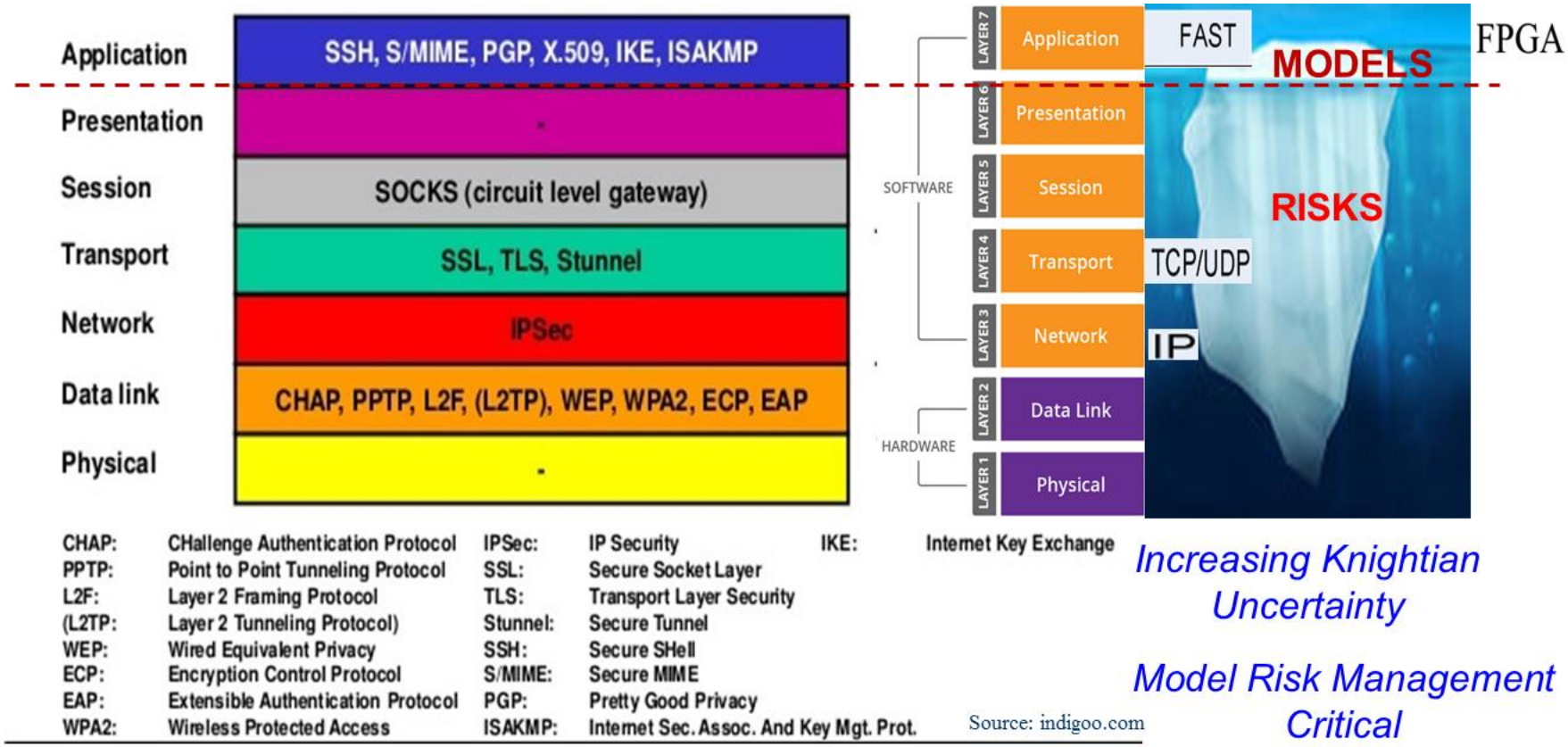
Enterprise Risk Management & Governance: ***ERM***

Systems & Networks Risk Management, Controls, Regulatory Compliance: ***MRM***

Cyber-Finance *Risk Management, Data at Rest, Data in Motion, Encryption:* ***C-FRM***



CYBER-FINANCE RISK MANAGEMENT



Source: 2015 Princeton Quant Trading Conference: www.FutureOfFinance.org

CYBER-FINANCE RISK MANAGEMENT

Related examples include **FIX (Financial Information eXchange)** and **FAST (FIX Adapted for STreaming)** protocols that form the backbone of buy- and sell-side trading or **SWIFT (Society for Worldwide Interbank Financial Telecommunication)** protocol that forms the backbone of worldwide banking transactions and messaging.

Regulated & Controlled Risks… Application Layer L7: Accounting & Auditing irregularities, Insider trading, Repo 105, LIBOR fixing, FOREX fixing, Credit ratings manipulations, Wash sales (High Frequency Trading), …

Unregulated & Uncontrolled Risks… Network Layers L3-6: Same or similar impacts on specific information but through ***cyber manipulations and cyber attacks***… at the Network Layer, Transport layer, related Security Protocols…

Such cyber risk 'losses' remain substantially unaccounted & unreported.

- SEC Corp Fin ***'materiality'*** criteria guidance for self-reporting by firms.

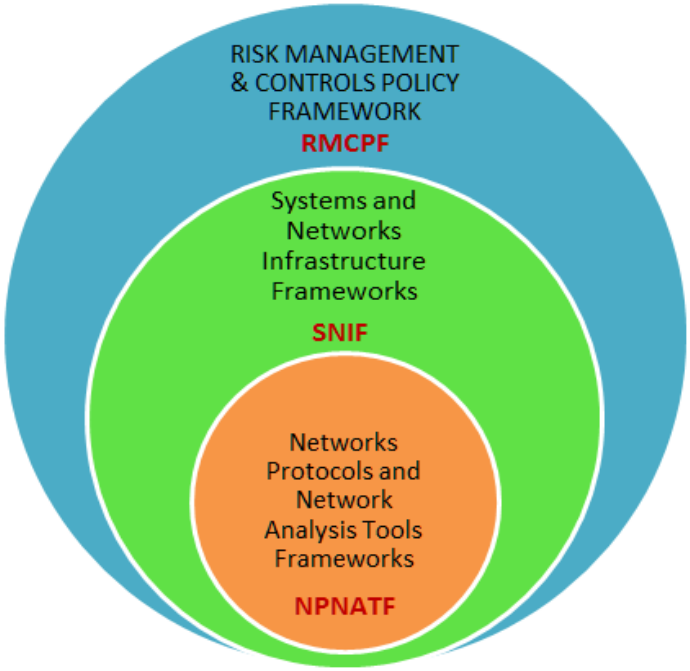
Source: 2015 Princeton Quant Trading Conference: www.FutureOfFinance.org

PROPOSED RISK MANAGEMENT FRAMEWORK

ERM

MRM

C-FRM



Connect Enterprise RM concerns to Pen Testing RM level concerns.

Align and Streamline Shared RM Goals and Outcomes at Top and all Other levels.

RM-Controls Policy Executives cognizant of how policy translates into actual execution.

Pen Testing within RM framework of importance and resource allocation.

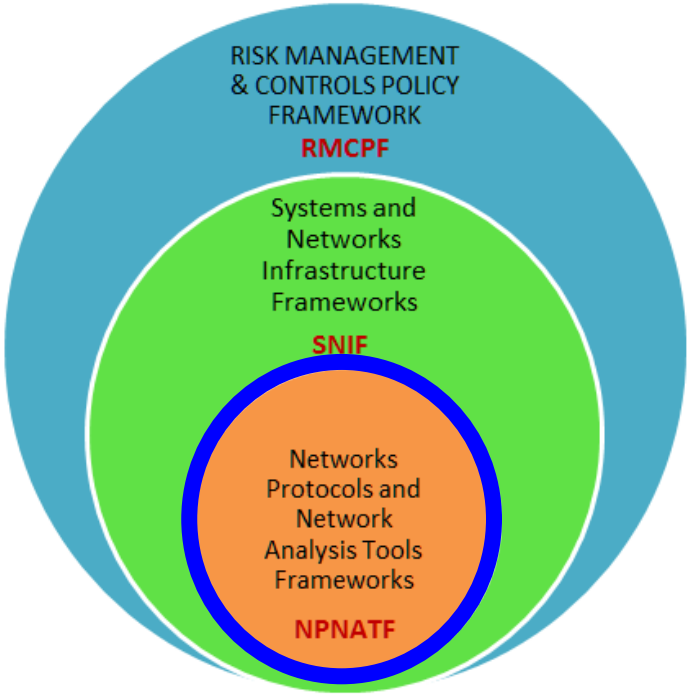
Pen Test team cognizant of contributions to value added at overall Enterprise Level.

NETWORKS PROTOCOLS & TOOLS FRAMEWORKS

ERM

MRM

C-FRM



Connect Enterprise RM concerns to Pen Testing RM level concerns.

Align and Streamline Shared RM Goals and Outcomes at Top and all Other levels.

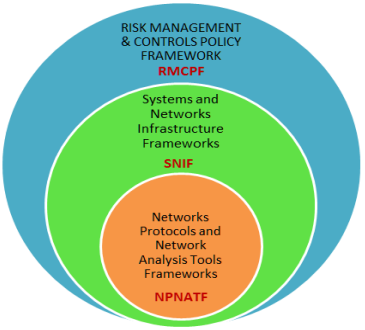
RM-Controls Policy Executives cognizant of how policy translates into actual execution.

Pen Testing within RM framework of importance and resource allocation.

Pen Test team cognizant of contributions to value added at overall Enterprise Level.

This is the level of network protocols, such as the above security protocols, where most critical threats and vulnerabilities exist and where real countermeasures need to be devised.

NETWORKS PROTOCOLS & TOOLS FRAMEWORKS

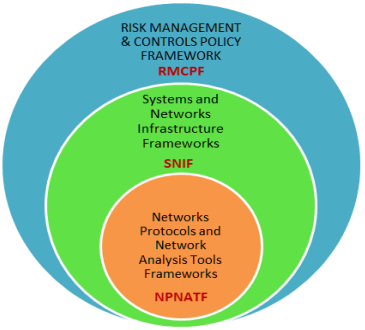


Is "pen testing" worth it?

If it is, then how to ensure that it is done right?

"It's going to be expensive, and you'll get a thick report when the testing is done... And that's the real problem. You really don't want a thick report documenting all the ways your network is insecure. You don't have the budget to fix them all, so the document will sit around waiting to make someone look bad. Or, even worse, it'll be discovered in a breach lawsuit. And if you're not going to fix all the uncovered vulnerabilities, there's no point uncovering them."

NETWORKS PROTOCOLS & TOOLS FRAMEWORKS

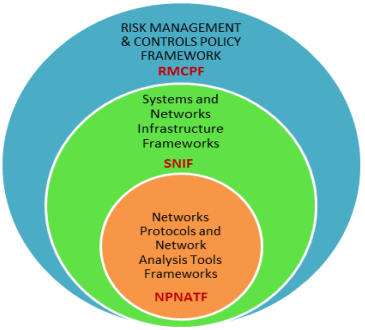


Is "pen testing" worth it?
If it is, then how to ensure that it is done right?

"One, you want to know whether certain vulnerability is present because you're going to fix it if it is. And two, you need a big, scary report to persuade your boss to spend more money."

Actual hands-on and / or automated pen testing process level wherein specific network analysis tools are used for various network analysis activities related to both vulnerability assessment *and* penetration testing.

NETWORKS PROTOCOLS & TOOLS FRAMEWORKS



NASA
Ames Research Center

Vulnerability Assessment:

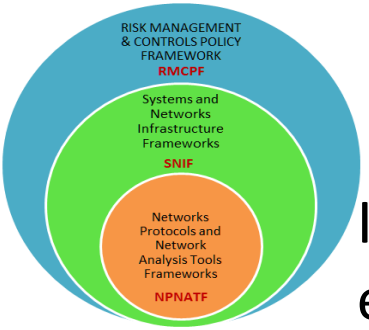
- Typically is general in scope and includes a large assessment.
- Predictable. (I know when those darn Security guys scan us.)
- Unreliable at times and high rate of false positives. (I've got a banner)
- Vulnerability assessment invites debate among System Admins.
- Produces a report with mitigation guidelines and action items.

Penetration Testing:

- Focused in scope and may include targeted attempts to exploit specific vectors (Both IT and Physical)
- Unpredictable by the recipient. (Don't know the "how?" and "when?")
- Highly accurate and reliable. (I've got root!)
- Penetration Testing = Proof of Concept against vulnerabilities.
- Produces a binary result: Either the team owned you, or they didn't.

Network Vulnerability Testing
Web Vulnerability Testing
Wireless War Driving / Walking
Phone Network Testing
Social Engineering Testing
Walk-throughs and Dumpster Diving
Physical Security Auditing

NETWORKS PROTOCOLS & TOOLS FRAMEWORKS



A penetration test simulates the actual attack from a malicious attacker which could be *anyone*.

In reality, such attacks from anyone out there are what enterprises *must* need to prepare for even if they like the phrase vulnerability assessment over penetration testing.

"When it comes to security, *the best defense is offense*; *you need to test the effectiveness of your own security practices before a real intruder does it for you.*"

metasploit®

"You must test your software before someone else does."

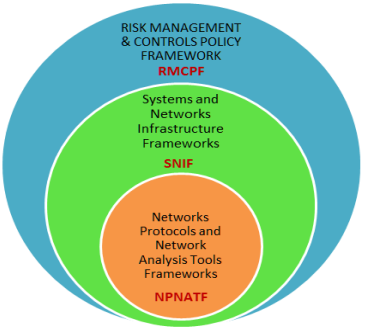
CODENOMICON

NASA

ERNST & YOUNG

pwc

NETWORKS PROTOCOLS & TOOLS FRAMEWORKS

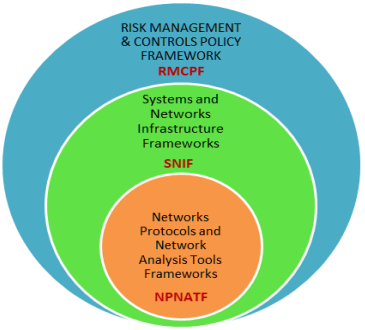


Two different types of frameworks

Overall scheme within which various ***phases*** of actual penetration testing, vulnerability analysis, stress testing, security auditing, etc. are conducted.

Swiss-knife like **tool kits** that are actually deployed to execute the technical ethical hacking and pen testing procedures within specific phases of penetration testing and vulnerability analysis with aid of **specific tools and techniques** for identifying and exploiting vulnerabilities.

NETWORKS PROTOCOLS & TOOLS FRAMEWORKS



- Pre-engagement Interactions
- Intelligence Gathering
- Threat Modeling
- Vulnerability Analysis
- Exploitation
- Post Exploitation
- Reporting

LOG IN

Navigation
- Main page
- PTES Technical Guideline
- In the Media
- FAQ

Search

Search

Go Search

Tools
- What links here
- Related changes
- Special pages
- Printable version
- Permanent link
- Page information

page view source history

High Level Organization of the Standard

The penetration testing execution standard consists of seven (7) main sections. These cover everything rela the scenes in order to get a better understanding of the tested organization, through vulnerability research, e reporting, which captures the entire process, in a manner that makes sense to the customer and provides th

This version can be considered a v1.0 as the core elements of the standard are solidified, and have been "ro a penetration test can be performed at. As no pentest is like another, and testing will range from the more m and enable the tester to step up the intensity on those areas where the organization needs them the most. S

Following are the main sections defined by the standard as the basis for penetration testing execution:

- Pre-engagement Interactions
- Intelligence Gathering
- Threat Modeling
- Vulnerability Analysis
- Exploitation
- Post Exploitation
- Reporting

PENETRATION TESTING EXECUTION STANDARD PTES Technical Guidelines

As the standard does not provide any technical guidelines as far as how to execute an actual pentest, we ha

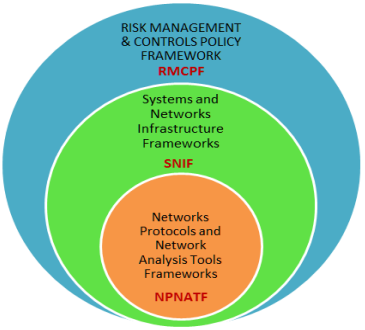
- Technical Guidelines

For more information on what this standard is, please visit:

- The Penetration Testing Execution Standard: FAQ

www.pentest-standard.org

NETWORKS PROTOCOLS & TOOLS FRAMEWORKS



Information Security Risk Rating Scale

Extreme 13-15	• Extreme risk of security controls being compromised with the possibility of catastrophic financial losses occurring as a result
High 10-12	• High risk of security controls being compromised with the potential for significant financial losses occurring as a result
Elevated 7-9	• Elevated risk of security controls being compromised with the potential for material financial losses occurring as a result
Moderate 4-6	• Moderate risk of security controls being compromised with the possibility of limited financial losses occurring as a result
Low 1-3	• Low risk of security controls being compromised with measurable negative impacts as a result

PENETRATION TESTING EXECUTION STANDARD
PTES
Technical Guidelines

www.pentest-standard.org

Completed at the time of this assessment

Tasks

Identify internal security point of contact

- Identify current resources to dedicate the task of resolving security concerns within the environment. The remediation process should be owned and supported by senior staff in order to effectively manage its completion.
- Secure appropriate funding for initial program review and 3rd party assessment

Identify Current Security State of security

- This task will be performed at an executive level. CLIENT will identify the proper ownership and executive support channel to champion this effort. In addition, CLIENT will need to take inventory of the "Security Management Chain of Command", Policy, Procedure, and Compliance tracking sophistication.

One (1) to Three (3) Months

Tasks

Create Remediation Strategy

- Leverage results found within the Penetration Test to create a full remediation strategy
- This assessment report will provide the basis for this action. It must now be formalized and approved by the CLIENT Security Team.

Create Information Security Council/Task Force

- To gain better traction in the remediation and security onboarding process, CLIENT should create a specific ISEC council to aid in remediation and adequately involve each individual team.
- The council should consist of Management of each individual business unit
- ....

Begin Security Project planning

- Assign Executive owners of security for CLIENT
- ...

Prioritize Remediation Events

- Leverage results found within Penetration Test to gain understanding of the tasks needed to be performed in order to resolve the risks identified.
- Assign priority listing to remediation tasks that will provide the highest level of impact and largest reduction of identified risk.
- Start process with server patching to gain quick increases in environment security.

Patch Services

- **Specific things to be fixed/how...**
- ...

Harden Servers

- ...
- ...

Three (3) to Twelve (12) Months

Tasks

Security Self Assessment

Adequate security of information and the systems that process it is a fundamental management responsibility. CLIENT officials must understand the current status of their information security program and controls in order to make informed judgments and investments that appropriately mitigate risks to an acceptable level. Self-assessments provide a method for CLIENT officials to determine the current status of their information security programs and, where necessary, establish a target for improvement. A good guide for this is **NIST SP 800-53a**: found at http://csrc.nist.gov/publications/PubsDrafts.html Another approach would be to run the **Microsoft Security Assessment Tool** : found at http://www.microsoft.com/technet/security/tools/msat/default.mspx

Twelve (12) Months+

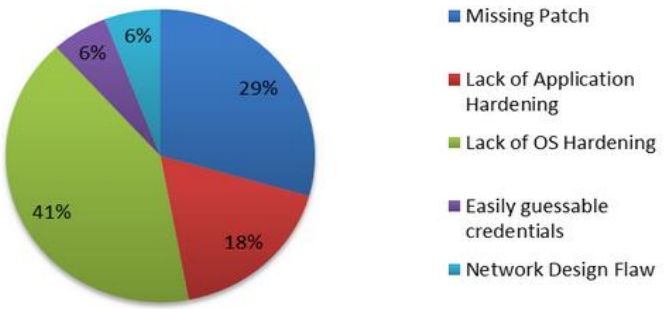
Tasks

Perform 3rd Party Assessment of Information Security and Compliance with 27001/2 (or any other compliance control set chosen).

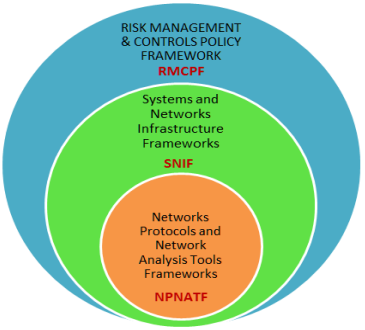
- Perform a Corporate wide assessment of CLIENT's ability to defend against targeted & generic attacks
- Identify the root cause of compliance gaps
- Identify strategy for using the output of the assessment to facilitate a security baseline

Begin remediation planning/budgeting

Security Risk Origin/Category

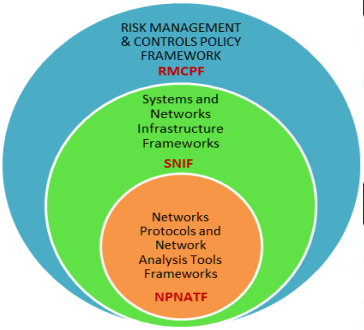


NETWORKS PROTOCOLS & TOOLS FRAMEWORKS



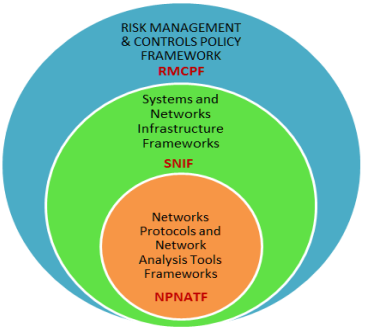
www.kali.org

NETWORKS PROTOCOLS & TOOLS FRAMEWORKS

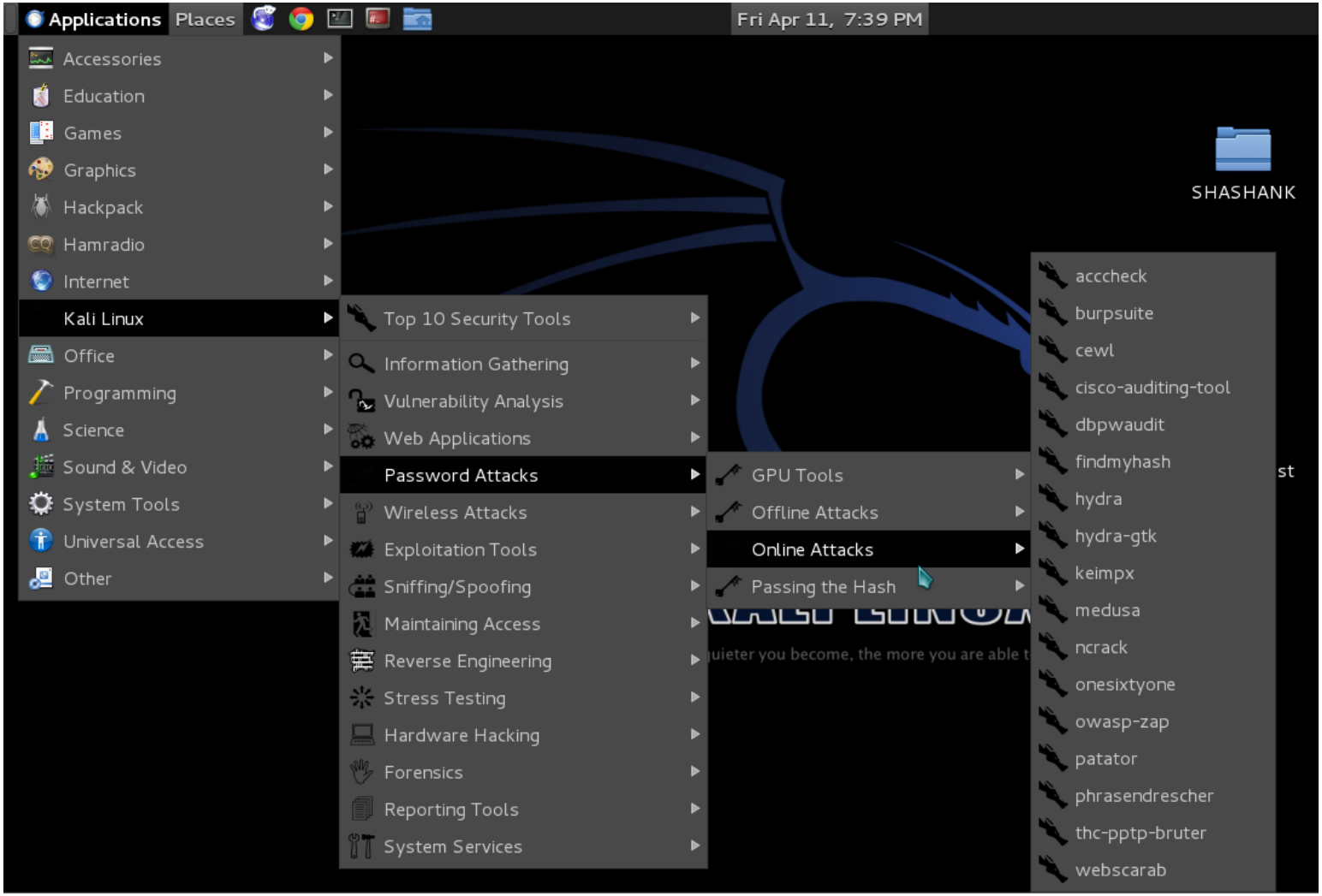


www.kali.org

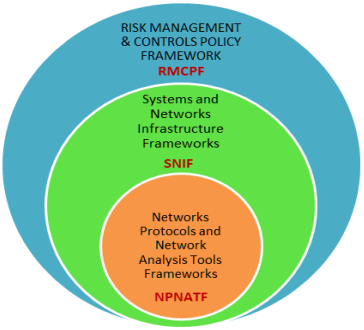
NETWORKS PROTOCOLS & TOOLS FRAMEWORKS



www.kali.org



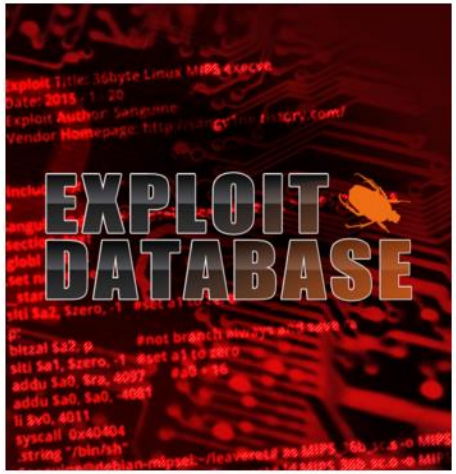
NETWORKS PROTOCOLS & TOOLS FRAMEWORKS



Kali Linux

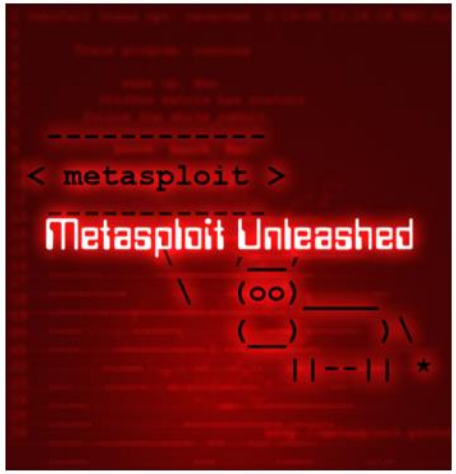
Kali Linux is the highest-rated and most popular Linux security distribution available. Kali Linux is a robust, enterprise ready penetration testing Linux distribution and is the successor of the popular and highly-rated BackTrack Linux. Kali Linux is used by penetration testers and IT professionals around the world to test the security of their networks.

The Exploit Database



The Exploit Database is the ultimate archive of public exploits and corresponding vulnerable software, developed for use by penetration testers and vulnerability researchers. Its aim is to serve as the most comprehensive collection of exploits gathered from various sources.

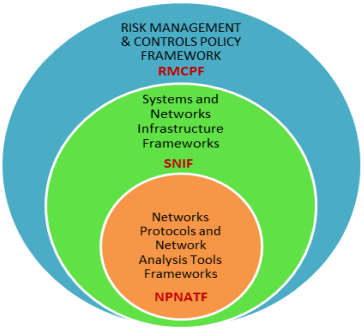
Metasploit Unleashed



The Metasploit Unleashed free online security training course was created to fill a gap in quality documentation on the practical usage of the popular and versatile Metasploit Framework. In keeping with the open-source nature of Metasploit, this resource is provided at no charge.

www.offensive-security.com/community-projects/

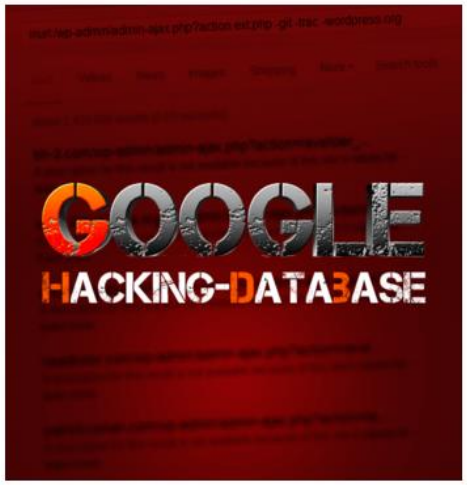
NETWORKS PROTOCOLS & TOOLS FRAMEWORKS



Kali Nethunter

Kali NetHunter is a Android penetration testing platform for Nexus and OnePlus devices built on top of Kali Linux, which includes some special and unique features such as HID Keyboard attacks, BADUSB attacks, as well as support for booting ISOs and images such as Konboot as well as a full Kali Linux Tools.

Google Hacking Database



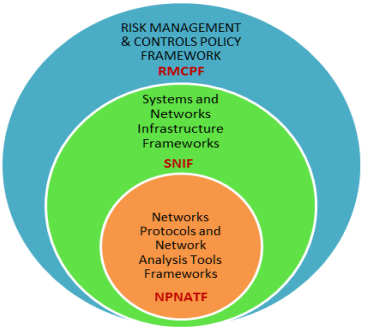
The Google Hacking Database (GHDB) is the authoritative source for querying the ever-widening reach of the Google search engine. In the GHDB, you will find search terms for files containing usernames, vulnerable servers, and even files containing passwords.

BackTrack Linux

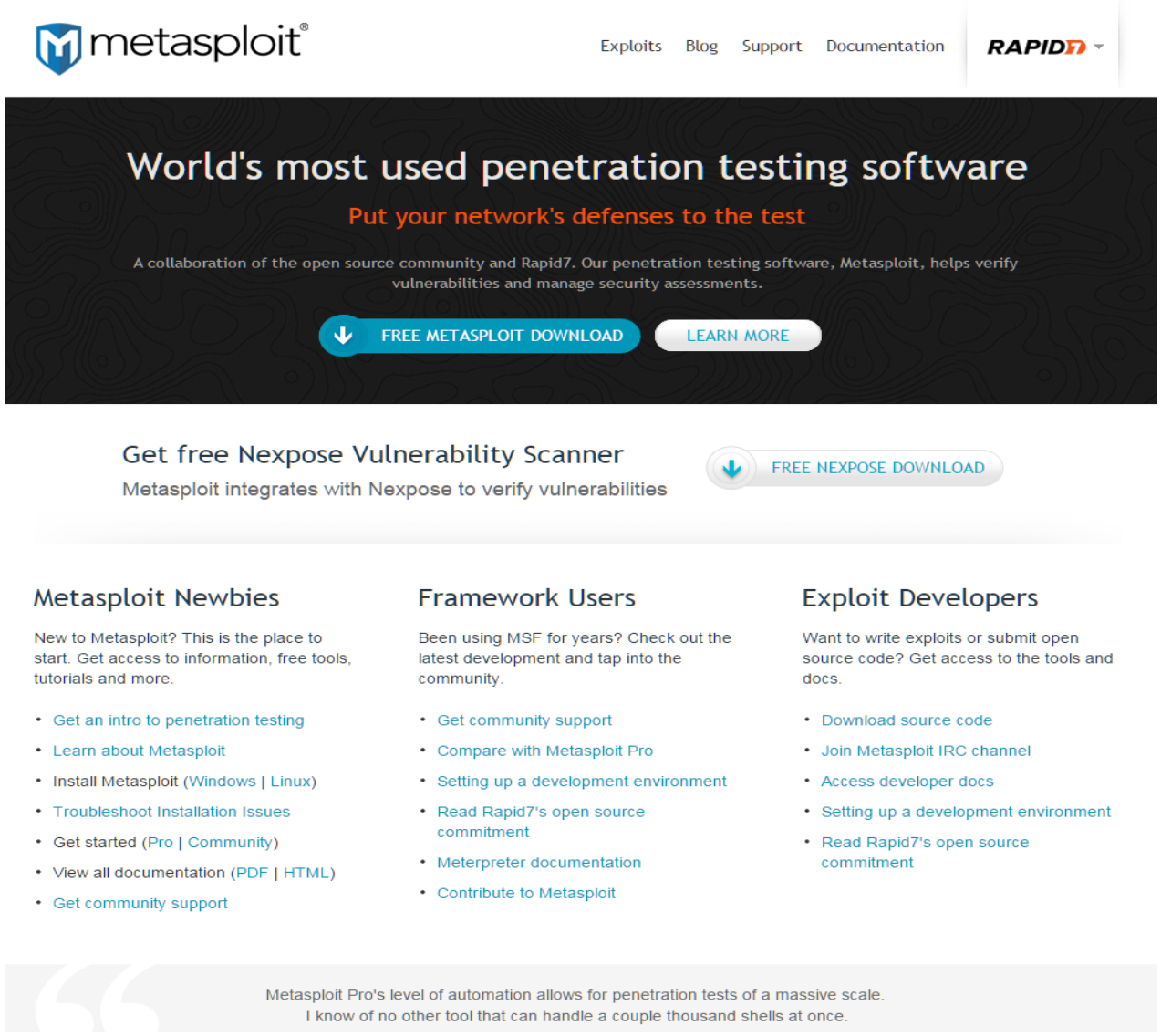
Prior to the release of Kali Linux, its predecessor, BackTrack Linux was the highest-rated and most popular Linux security distribution available. BackTrack is a Linux-based penetration testing arsenal that aids security professionals in their ability to perform assessments in a purely native dedicated environment.

www.offensive-security.com/community-projects/

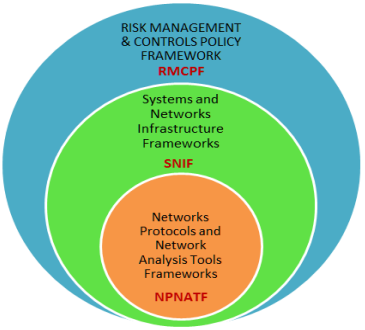
NETWORKS PROTOCOLS & TOOLS FRAMEWORKS

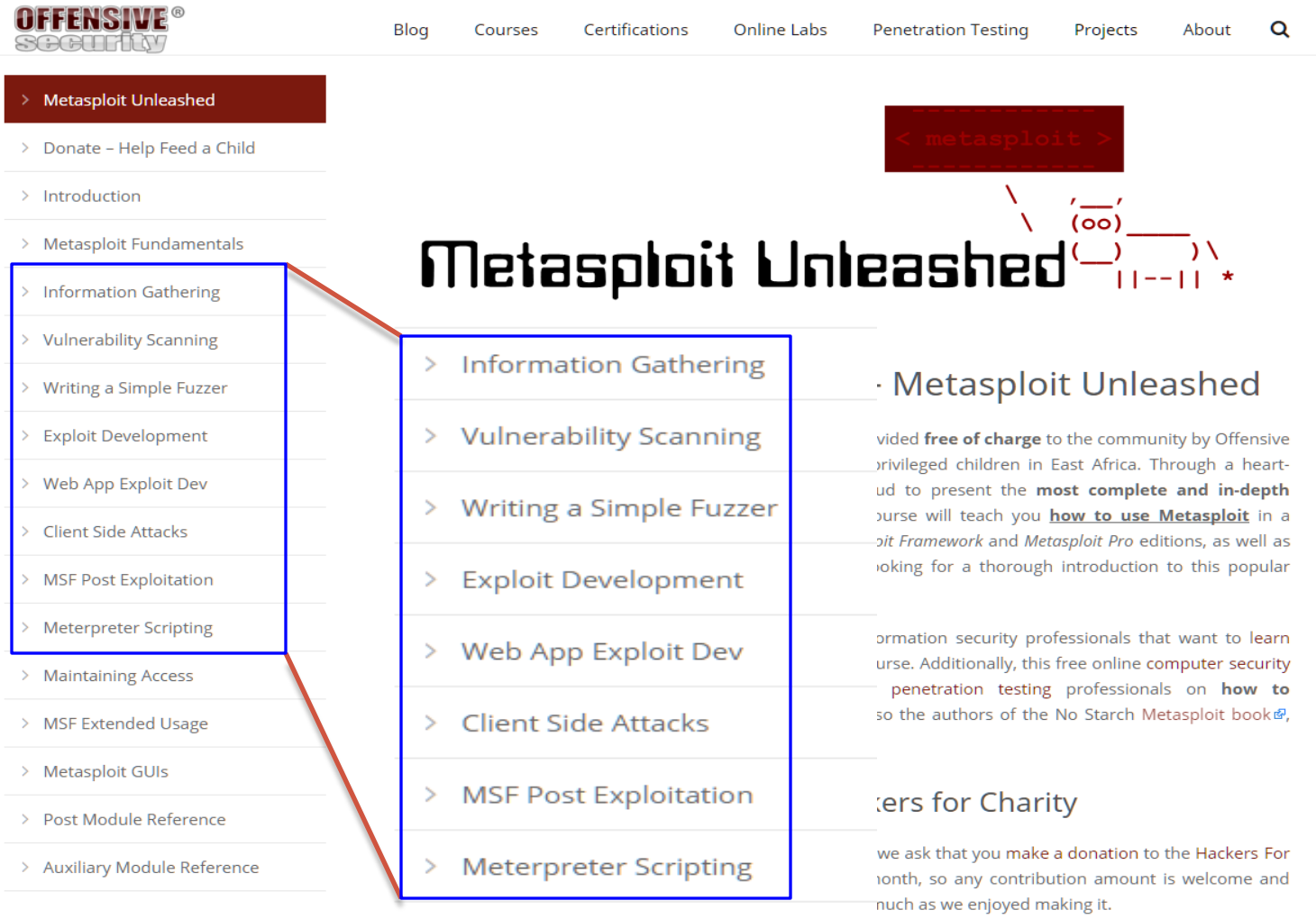


www.metasploit.com



NETWORKS PROTOCOLS & TOOLS FRAMEWORKS





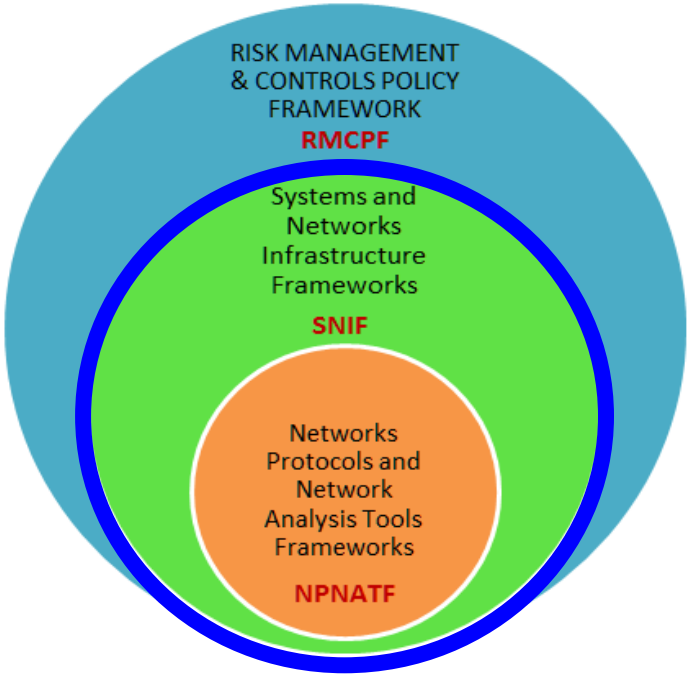
www.offensive-security.com/metasploit-unleashed/

SYSTEMS AND NETWORKS LEVEL FRAMEWORKS

ERM

MRM

C-FRM



Connect Enterprise RM concerns to Pen Testing RM level concerns.

Align and Streamline Shared RM Goals and Outcomes at Top and all Other levels.

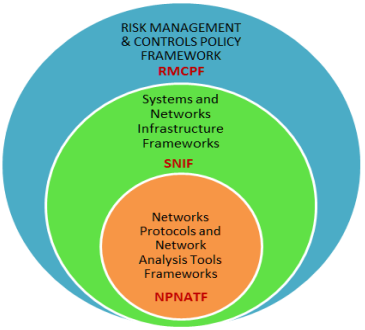
RM-Controls Policy Executives cognizant of how policy translates into actual execution.

Pen Testing within RM framework of importance and resource allocation.

Pen Test team cognizant of contributions to value added at overall Enterprise Level.

At this specific level the focus of most procedures and techniques is at the systems and networks level rather than at the more granular level of telecom network protocols.

SYSTEMS AND NETWORKS LEVEL FRAMEWORKS



Home
About OWASP
Acknowledgements
Advertising
AppSec Events
Books
Brand Resources
Chapters
Donate to OWASP
Downloads
Funding
Governance
Initiatives
Mailing Lists
Membership
Merchandise
News
Community portal
Presentations
Press
Projects
Video
Volunteer

Reference
Activities
Attacks
Code Snippets

Page | Discussion | Read | View source | V

The OWASP Testing Framework

OWASP Testing Guide v3 Table of Contents

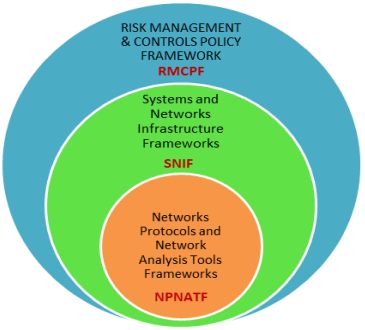
This article is part of the OWASP Testing Guide v3. The entire OWASP Testing Guide v3 can be downloaded here.

OWASP at the moment is working at the OWASP Testing Guide v4: you can browse the Guide here

[hide]

www.owasp.org/index.php/The_OWASP_Testing_Framework

SYSTEMS AND NETWORKS LEVEL FRAMEWORKS



ıge Discussion Read Viev

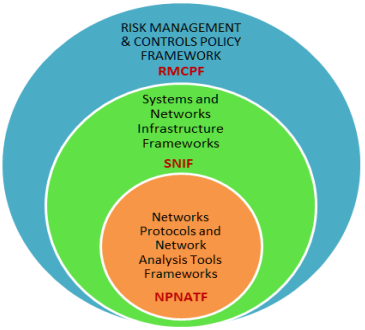
OWASP Top 10/Mapping to WHID

Here is a mapping of the [| OWASP Top 10 - 2013] to example real world entries in the OWASP/WASC Web Hacking Incident Database (WHID):

- A1: Injection - http://www.google.com/fusiontables/DataSource?snapid=S2086702IR5
- A2: Broken Authentication and Session Management - https://www.google.com/fusiontables/DataSource?snapid=S1536601kboC
- A3: Cross-site Scripting - https://www.google.com/fusiontables/DataSource?snapid=S856202bP-1
- A4: Insecure Direct Object Reference - http://www.google.com/fusiontables/DataSource?snapid=S208914Efwz
- A5: Security Misconfiguration - http://www.google.com/fusiontables/DataSource?snapid=S208909HtmA
- A6: Sensitive Data Exposure - http://www.google.com/fusiontables/DataSource?snapid=S2089112yxM
- A7: Missing Function Level Access Control - http://www.google.com/fusiontables/DataSource?snapid=S208910u7mt
- A8: Cross-site Request Forgery - https://www.google.com/fusiontables/DataSource?snapid=S856204sdBi
- A9: Using Components with Known Vulnerabilities - https://www.google.com/fusiontables/DataSource?snapid=S1536701c0JG
- A10: Unvalidated Redirects and Forwards - http://www.google.com/fusiontables/DataSource?snapid=S2089124qF5

https://www.owasp.org/index.php/OWASP_Top_10/Mapping_to_WHID

SYSTEMS AND NETWORKS LEVEL FRAMEWORKS



OWASP/WASC Web Hacking Incident Database (WHID)

File View Edit Visualize Merge Labs

SIGN IN

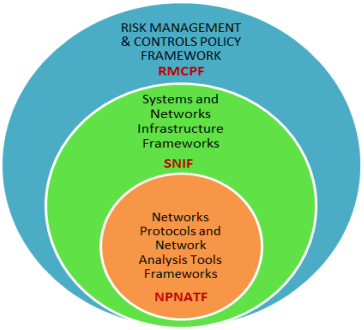
Switch to new look | Get link | Share

Showing 'Attack Method' CONTAINS 'Injection' options

1 - 100 of many Next »

WHID ID	Entry Title	Incident Description	Reference	Date Occurred	Attack Meth	Application	Outcome	Attacked Entity Field	Attacked En	Mass Attack	Mass Attack
2015-090	WHID 2015-090: RubyGems.org hacked, interrupting Heroku services and putting sites using Rails at risk	A user uploaded a malicious gem that contained a malicious gem manifest (YAML file). The manifest contained embedded Ruby with this payload. This is the only known incident involving this vulnerability, but the vulnerability involved is a remote code execution exploit, so the usual rules apply.	http://venturebeat.com/2013/01/30/rubygems-org-hacked-interrupting-heroku-services-and-putting-millions-of-sites-using-rails-at-risk/	1/30/2015	Code Injection	Improper Input Handling	Leakage of Information	Technology			
2015-086	WHID 2015-086: Buy Way Hit by Extortionist Rex Mundi Hackers	Hacker group Rex Mundi, which recently attempted to extort $15,000 from AmeriCash Advance and $50,000 from Drake International, now claim to have breached the servers of Belgian company Buy Way	http://www.esecurityplanet.com/hackers/buy-way-hit-by-extortionist-rex-mundi-hackers.html	1/25/2015	SQL Injection	Improper Input Handling	Leakage of Information	Retail			
2015-071	WHID 2015-071: PhonCert Hacked	DB Dump	http://siph0n.net/exploits.php?id=3676	1/31/2015	SQL Injection	Improper Input Handling	Leakage of Information	Entertainment			
2015-068	WHID 2015-068: Higher Education Commission Pakistan Hacked	DB Dump	http://siph0n.net/exploits.php?id=3670	1/29/2015	SQL Injection	Improper Input Handling	Leakage of Information	Education			
2015-064	WHID 2015-064: Rex Mundi dumps more data after another entity doesn?t pay extortion demands	Last week, we hacked the servers of Temporis, allegedly France?s largest network of franchised temp work agencies (www.temporis-franchise.fr).	http://www.databreaches.net/rex-mundi-dumps-more-data-after-another-entity-doesnt-pay-extortion-demands/	1/27/2015	SQL Injection	Improper Input Handling	Leakage of Information	Recruiting			
2015-063	WHID 2015-063: Victor Valley College hit by computer security breach	The entire Victor Valley College Information Technology Department has been placed on paid administrative leave while campus police and an outside company investigate a breach in security protocol, President Roger Wagner said Thursday.	http://www.databreaches.net/ca-victor-valley-college-hit-by-computer-security-breach-entire-it-dept-put-on-leave/	1/31/2015	SQL Injection	Improper Input Handling	Leakage of Information	Education			
2015-062	WHID 2015-062: oklahomacounty.c hacked	DB Dump on PasteBin	http://pastebin.com/0ekAGZWs	1/25/2015	SQL Injection	Improper Input Handling	Leakage of Information	Government			
2015-060	WHID 2015-060: ValidDumps.RU Full User Database Dump	DB Dump	http://siph0n.net/exploits.php?id=3668	1/22/2015	SQL Injection	Improper Input Handling	Leakage of Information	Hacker Site			
2015-059	WHID 2015-059: FreshFiction DB Dumped	DB Dump on PasteBin	http://pastebin.com/ZGfRR7mL	1/24/2015	SQL Injection	Improper Input Handling	Leakage of Information	Media			
	WHID 2015-057										

SYSTEMS AND NETWORKS LEVEL FRAMEWORKS



IBM

IBM developerWorks® Technical topics Evaluation software Community Events

developerWorks > Technical topics > Security > Technical library >

OWASP top 10 vulnerabilities

Look at the top 10 web application security risks worldwide as determined by the Open Web Application Security Project. Then discover how IBM Security AppScan helps website administrators find, correct, and avoid these and other web security threats.

PDF (119 KB) | 0 Comments

Share:

developerWorks security editors, developerWorks, IBM

20 April 2015

→ Try IBM Security AppScan

+ Table of contents

OWASP

The Open Web Application Security Project (OWASP) is an international organization dedicated to enhancing the security of web applications. As part of its mission, OWASP sponsors numerous security-related projects, one of the most popular being the Top 10 Project. This project publishes a list of what it considers the current top 10 web application security risks worldwide. The list describes each vulnerability, provides examples, and offers suggestions on how to avoid it. The most recent version of the top 10 list, officially published in June 2013, updated the 2010 list. The 2013 Top 10 list is based on data from seven application security firms, spanning over 500,000 vulnerabilities across hundreds of organizations. OWASP prioritized the top 10 according to their prevalence and their relative exploitability, detectability, and impact.

Free trial of AppScan Standard

IBM Security AppScan Standard helps you detect and correct many of the types of security issues found in the OWASP top 10 list. You can download a trial version of AppScan Standard and test it out for yourself.

As a further aid in understanding some of these vulnerabilities, the IBM Security Systems Ethical Hacking team has prepared the following videos.

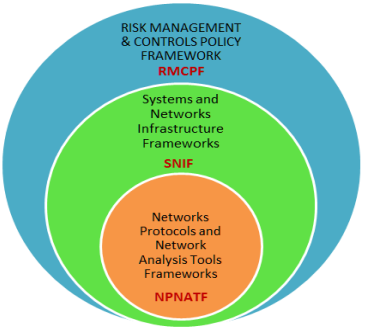
#1 Injection

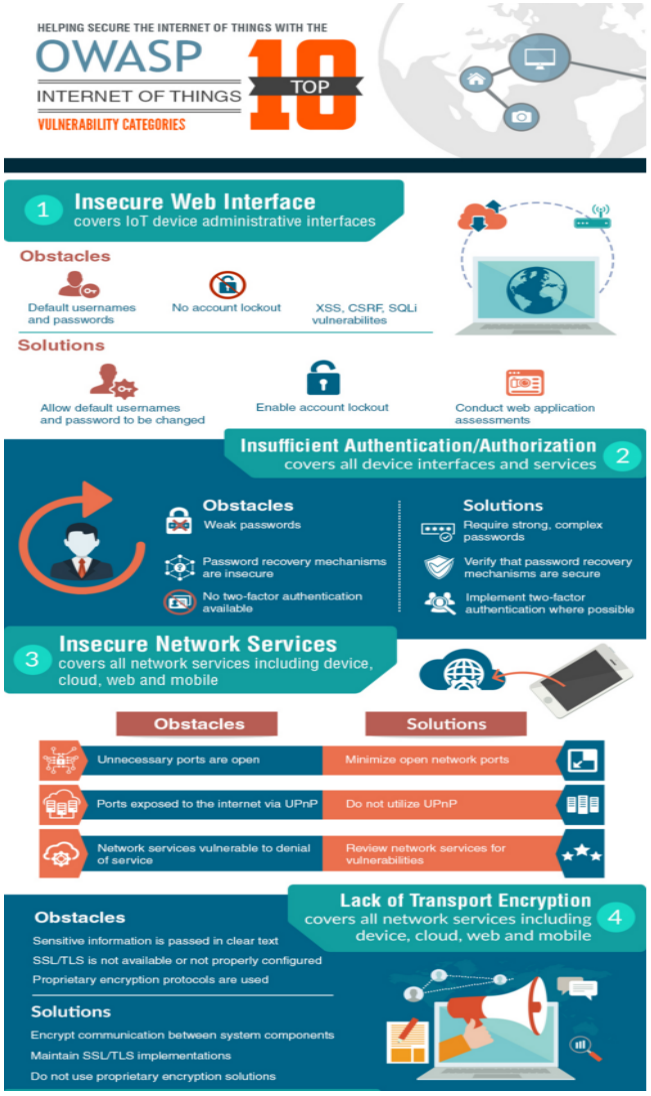
Warren Moynihan defines injection and lists a few of the many examples of it. He then provides a detailed example of how injection techniques might be used by a hacker to gain access to otherwise protected data. Finally, he illustrates how you can use IBM Security AppScan to find and eliminate this vulnerability.

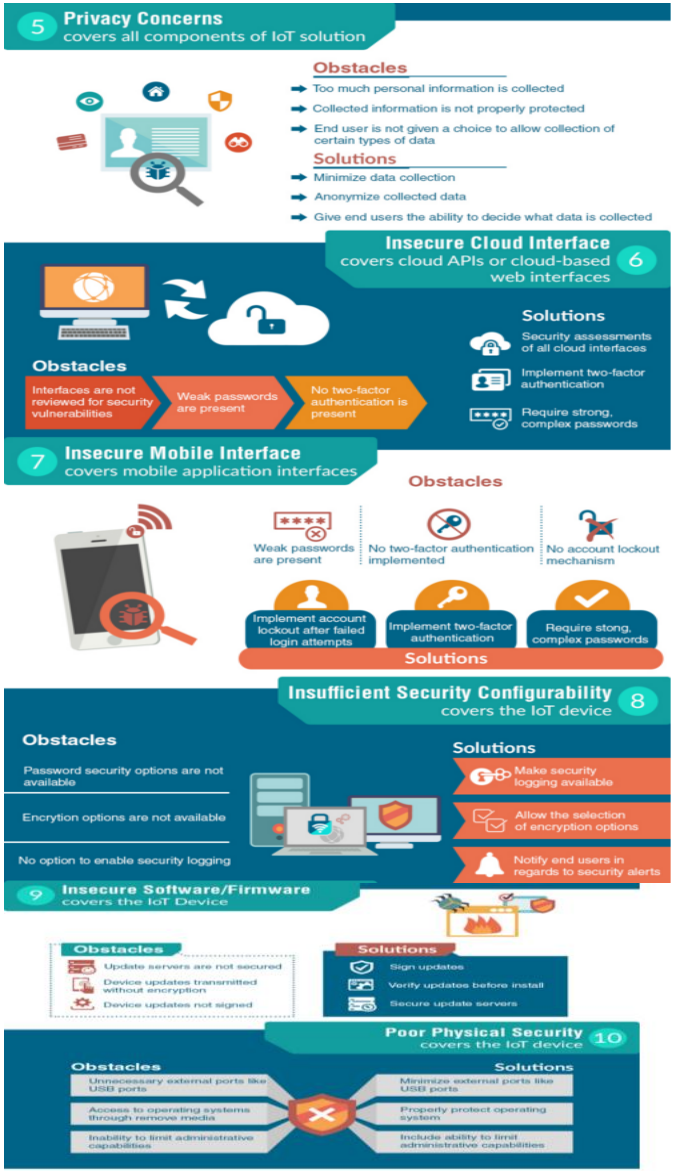
#1 Injection

http://www.ibm.com/developerworks/library/se-owasptop10/index.html

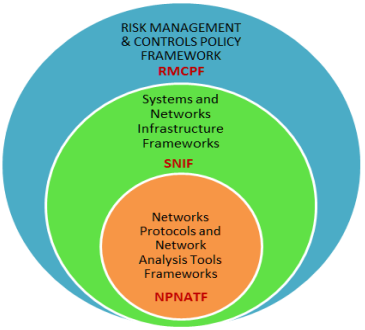
SYSTEMS AND NETWORKS LEVEL FRAMEWORKS







SYSTEMS AND NETWORKS LEVEL FRAMEWORKS



ERNST & YOUNG

Internal A&P Testing:

- After being given a physical connection to a point on the client's network, attempt to gain a privileged level of access to systems/data on that network
- Performed from network point(s) on the client site

External A&P Testing:

- Attempt to penetrate the client's network security perimeter in order to access client systems/data from the Internet
- May include techniques such as social engineering and 'trophy' gathering

External Vulnerability Scanning:

- Use commercially available software tools to perform vulnerability scanning of the client's business critical servers and network devices
- No attempt to exploit potential vulnerabilities identified
- No investigation of false positives from the scanning tool(s)

Corporate Desktop / Laptop Build Assessment:

- Assess the security of your Standard Build

Physical Security Testing:

- Attempt to gain unauthorised physical access to the client's office / site, followed by an attempt to plug a laptop/device into the client's network undetected
- No attempt to penetrate the client's internal network

Web / Application Testing:

- Attempt to circumvent the programming logic of a web site to gain unauthorised access to data or underlying systems.
- Can be done anonymously and/or with suitable credentials.

Social Engineering:

- Impersonation/deception techniques directed at targeted individuals in an attempt to obtain information that could be used to further other attacks

Remote Access / Wardialling:

- Dialling telephone number ranges allocated to the client in order to identify possible modems

Wireless Testing:

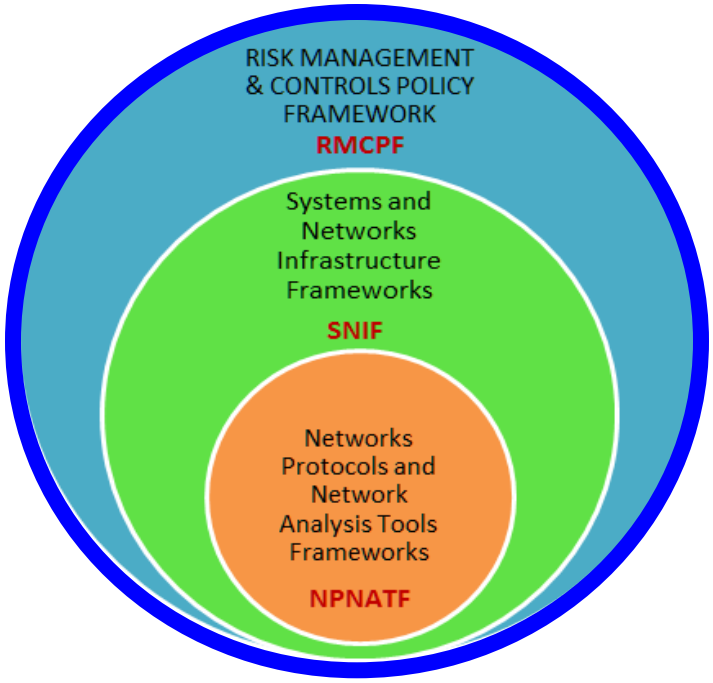
- Scanning for Wireless networks or devices, within your premises which could potentially allow access to be gained to your internal network

RISK MANAGEMENT CONTROLS FRAMEWORKS

ERM

MRM

C-FRM



Connect Enterprise RM concerns to Pen Testing RM level concerns.

Align and Streamline Shared RM Goals and Outcomes at Top and all Other levels.

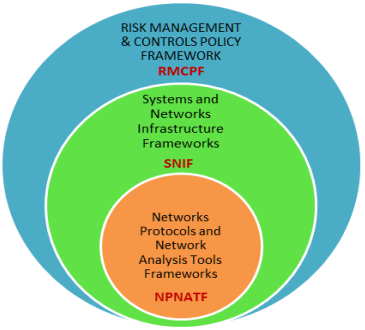
RM-Controls Policy Executives cognizant of how policy translates into actual execution.

Pen Testing within RM framework of importance and resource allocation.

Pen Test team cognizant of contributions to value added at overall Enterprise Level.

However, for either of SNIF and NPNATF to have real teeth and real resources for them to have the needed effect, they need to be effectively linked and related to the top level RMCPF.

RISK MANAGEMENT CONTROLS FRAMEWORKS



Three types of regulatory frameworks visible to C-suite

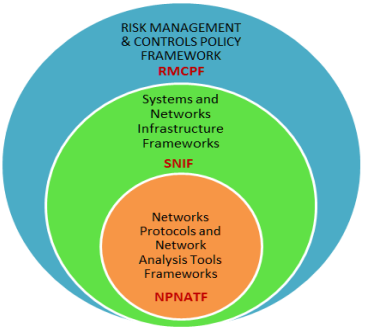
Payment Card Industry Data Security Standards (PCI DSS) (www.pcisecuritystandards.org)

IT Systems Banking Audit & Control Frameworks

- ISACA Controls Framework: COSO, COBIT (www.isaca.org)

SANS Financial Services Regulatory Frameworks (www.sans.org)

RISK MANAGEMENT CONTROLS FRAMEWORKS



Requirements and Security Assessment Procedures

Version 3.1
April 2015

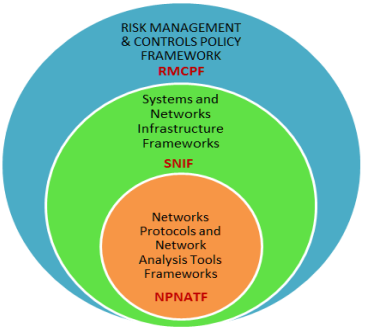
PCI Security Standards Council

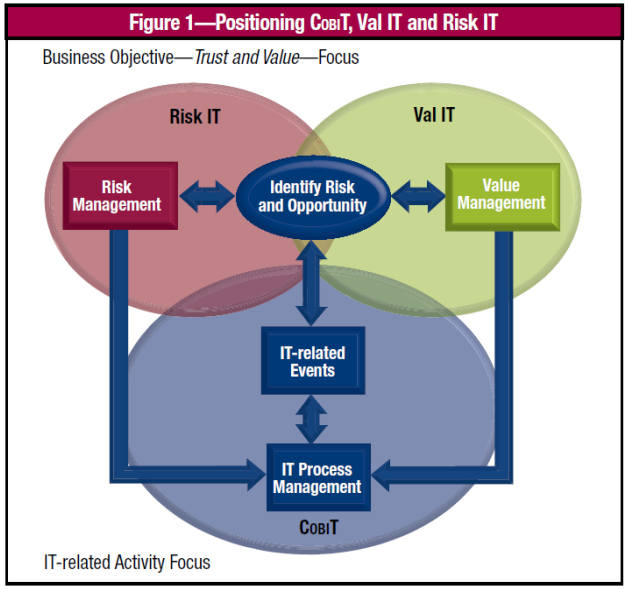
PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

www.pcisecuritystandards.org

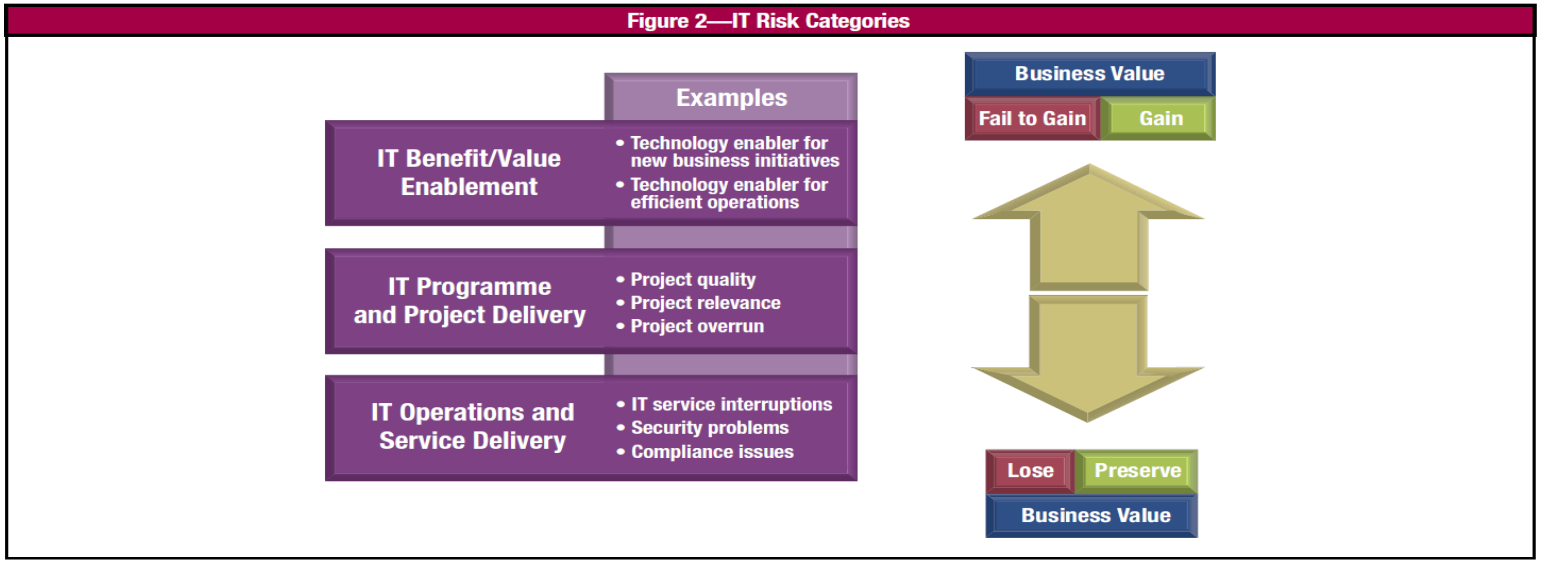
RISK MANAGEMENT CONTROLS FRAMEWORKS



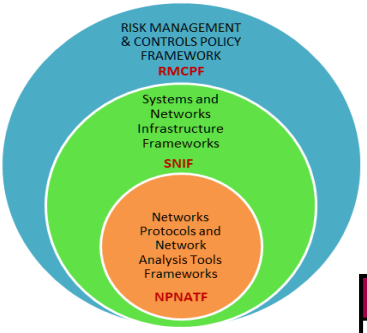


ISACA
Trust in, and value from, information systems

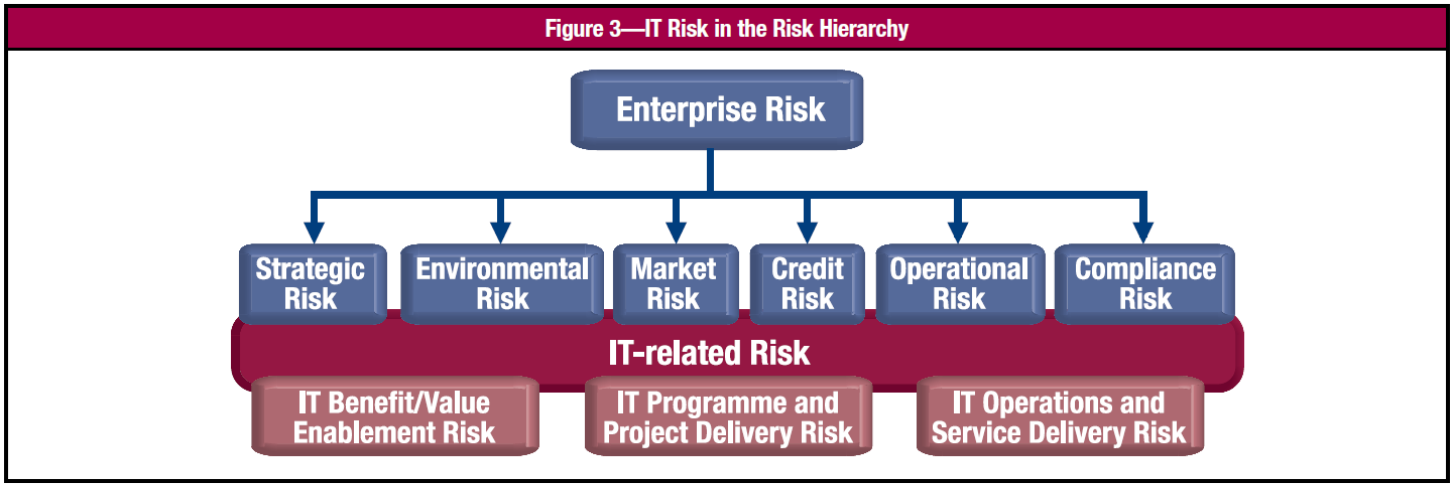
www.isaca.org



RISK MANAGEMENT CONTROLS FRAMEWORKS

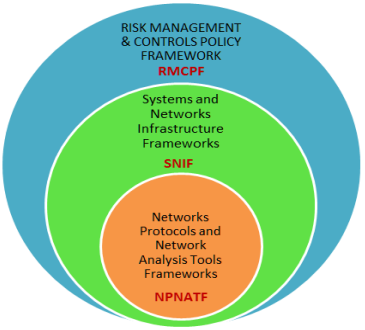


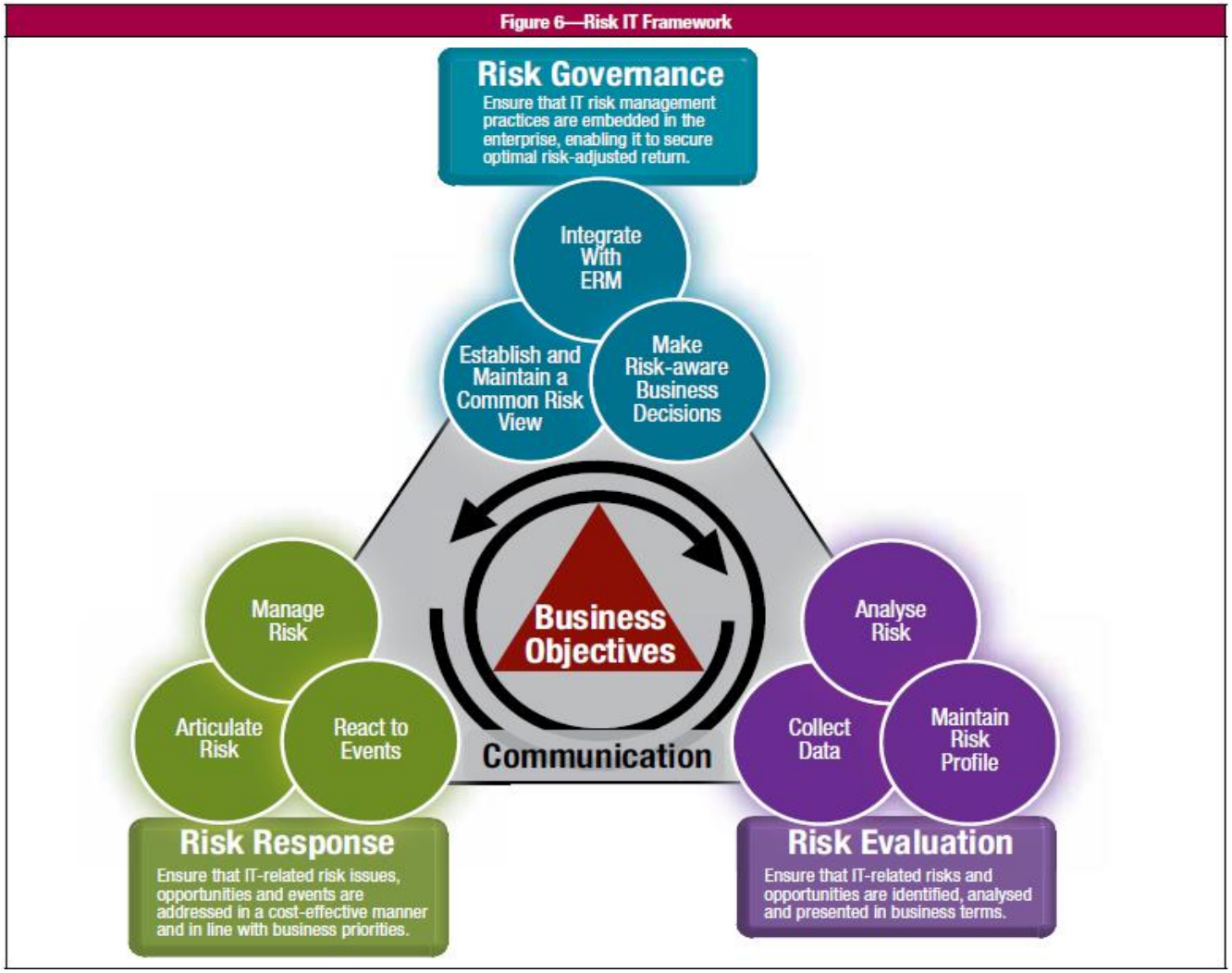
ISACA
Trust in, and value from, information systems



www.isaca.org

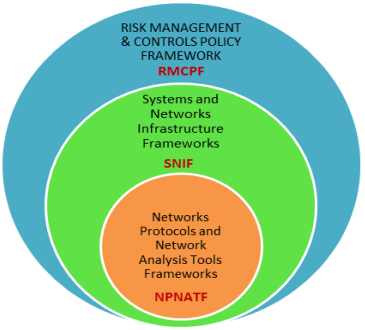
RISK MANAGEMENT CONTROLS FRAMEWORKS



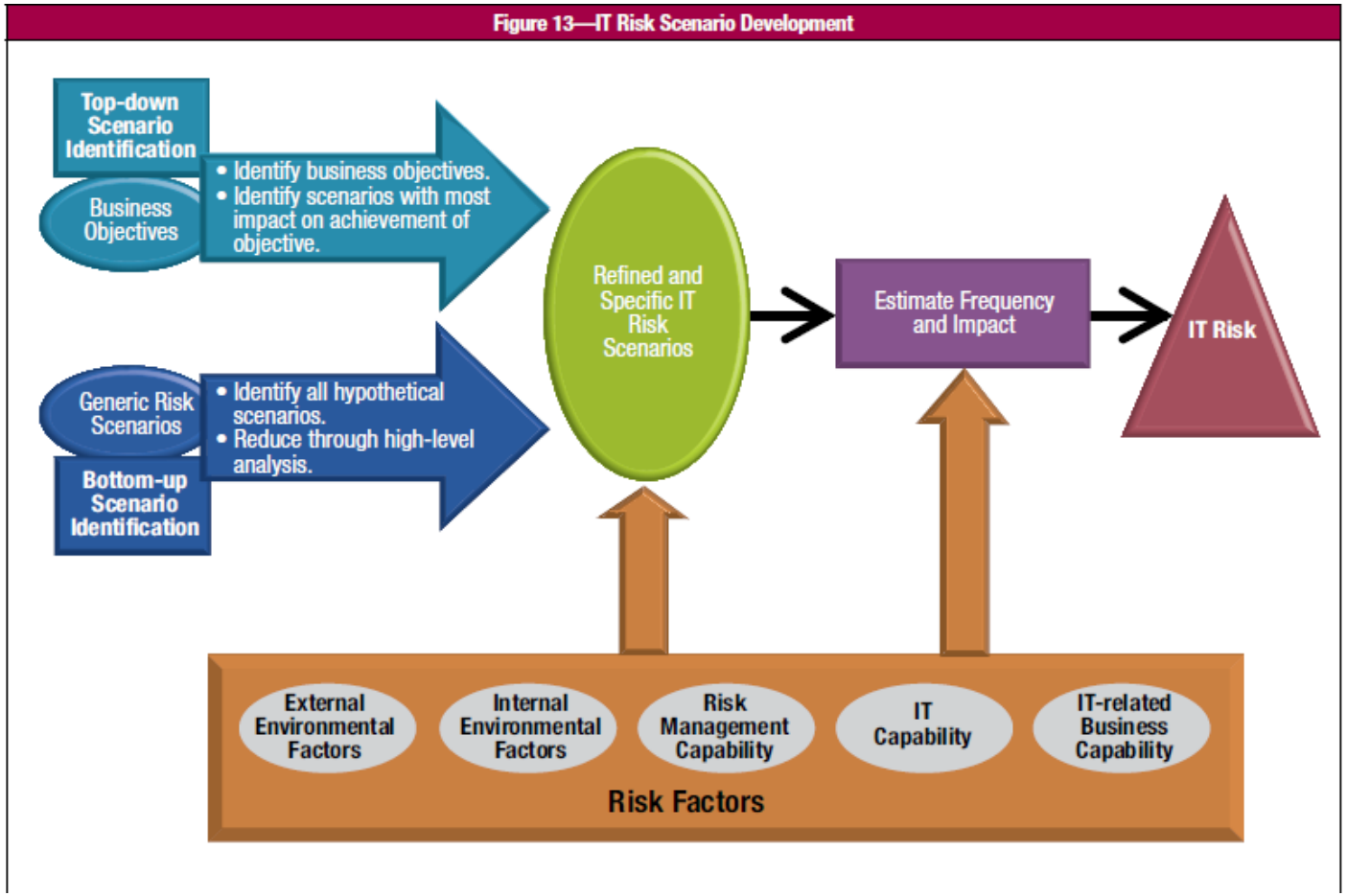


www.isaca.org

RISK MANAGEMENT CONTROLS FRAMEWORKS

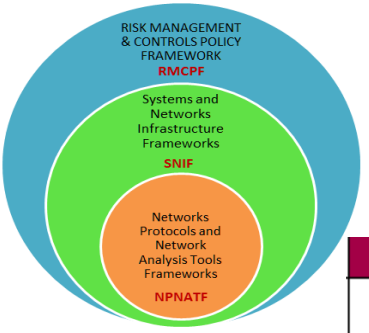


ISACA
Trust in, and value from, information systems



www.isaca.org

RISK MANAGEMENT CONTROLS FRAMEWORKS

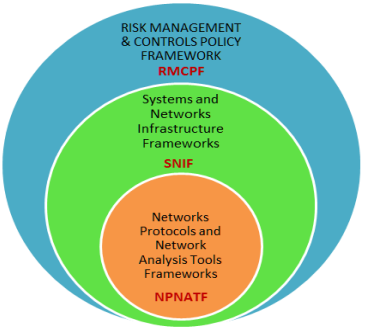


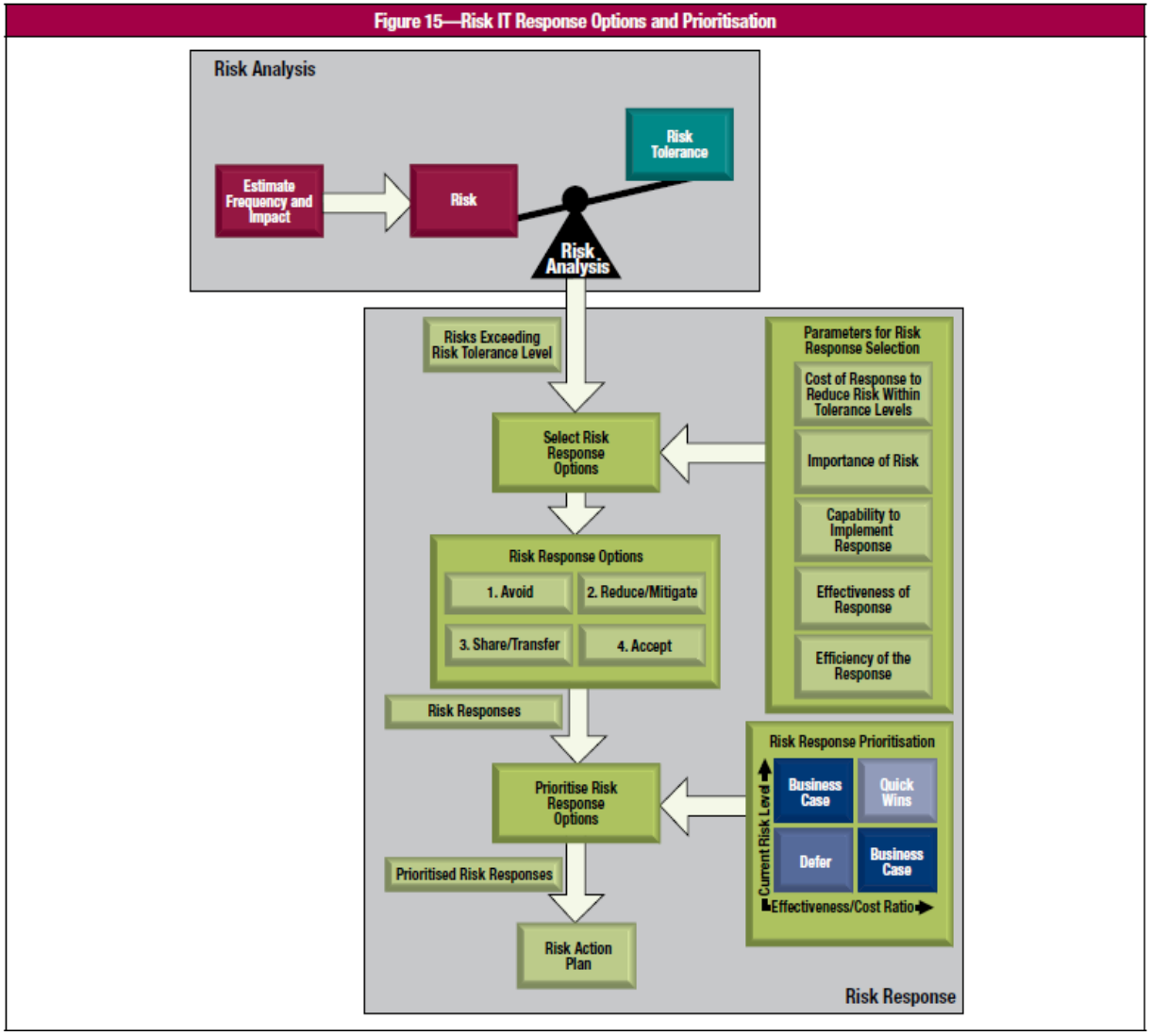
ISACA
Trust in, and value from, information systems

Figure 14—IT Risk Scenario Components

www.isaca.org

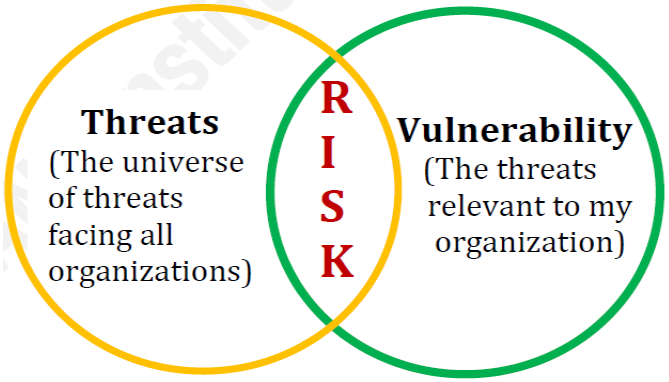
RISK MANAGEMENT CONTROLS FRAMEWORKS





www.isaca.org

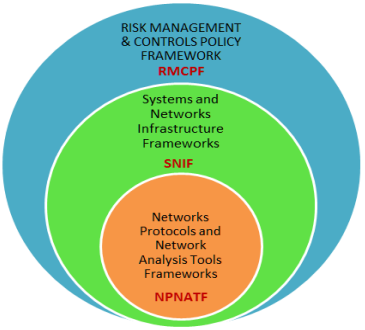
RISK MANAGEMENT CONTROLS FRAMEWORKS



Penetration Testing in the Financial Services Industry

Platform	OS	Version	Example Applications						Risk Rating	Vuln. Status	Vuln. Rating	Pen-Test Priority
			e-Mail	*Wireless*	*VoIP*	*G/L*	*Citrix*	*SSH*				
Unix/Linux	AIX	5.6						yes	4	patched 13-02-10	2	8
Unix/Linux	SuSE	5.5				yes		yes	5	patched 06-27-09	4	20
Midrange	iSeries	v6r1				yes			3	patched 06-27-09	4	12
Midrange	iSeries	v5r4				yes			3	patched 13-02-10	3	9
Mainframe	OS/390	R6				yes			2	patched 13-02-10	3	6
Mainframe	z/OS	V1.9				yes			2	patched 13-02-10	3	6
Windows	Win 2008		yes		yes				4	patched 13-02-10	2	8
Windows	Win 7						yes		3	patched 13-02-10	2	6
Network	IOS	12.4		yes				yes	3	patched 13-02-10	3	9
Network	IOS	12.3			yes			yes	4	patched 06-20-09	4	16

PROPOSED RISK MANAGEMENT FRAMEWORK



How can pen testing and vulnerability analysis effectively contribute to the execution of enterprise level risk management, controls, and compliance policies?

How can enterprise level risk management, controls, and compliance policies ensure that pen testing and vulnerability are accountable to enterprise risk management execution?

While bridging the disconnects between the three levels – *risk management policy*, *systems and network infrastructure controls*, and *vulnerability analysis and threat assessment* such as at the level of specific protocols – the proposed framework resolves the pen testing dilemmas.

APPLYING THE FRAMEWORK TO VOIP

3 LEVELS OF FRAMEWORKS ANALYZED

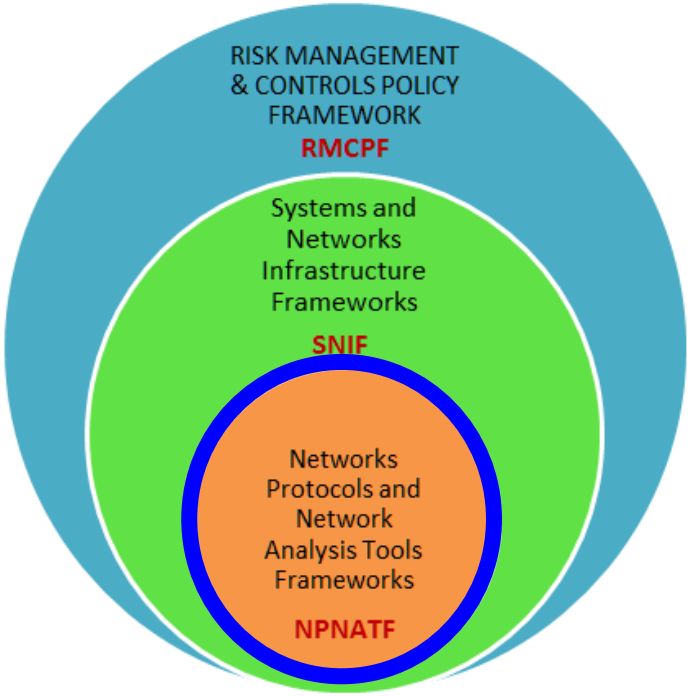
- Diverse frameworks have different levels and scopes
- **N**etworks **P**rotocols & **N**etwork **A**nalysis **T**ools **F**rameworks
  - Penetration Testing, Vulnerability Analysis & Auditing
    - Technically sophisticated Tool & Protocol Level
- **S**ystems & **N**etworks **I**nfrastructure **F**rameworks
  - Penetration Testing, Vulnerability Analysis & Auditing
    - Focus on Infrastructure, specifically Systems & Networks
- **R**isk **M**anagement & **C**ontrols **P**olicy **F**rameworks
  - Typically Policy Level and Strategy Level
    - Less specific to VoIP, Less granular in application to VoIP

NETWORKS PROTOCOLS & TOOLS FRAMEWORKS

ERM

MRM

C-FRM



Connect Enterprise RM concerns to Pen Testing RM level concerns.

Align and Streamline Shared RM Goals and Outcomes at Top and all Other levels.

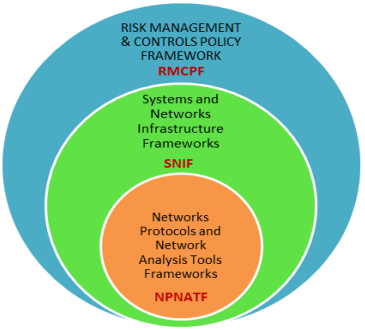
RM-Controls Policy Executives cognizant of how policy translates into actual execution.

Pen Testing within RM framework of importance and resource allocation.

Pen Test team cognizant of contributions to value added at overall Enterprise Level.

This is the level of network protocols, such as the above security protocols, where most critical threats and vulnerabilities exist and where real countermeasures need to be devised.

NETWORKS PROTOCOLS & TOOLS FRAMEWORKS



- Pre-engagement Interactions
- Intelligence Gathering
- Threat Modeling
- Vulnerability Analysis
- Exploitation
- Post Exploitation
- Reporting

LOG IN

Navigation

- Main page
- PTES Technical Guideline
- In the Media
- FAQ

Search

Search

Go Search

Tools

- What links here
- Related changes
- Special pages
- Printable version
- Permanent link
- Page information

page view source history

High Level Organization of the Standard

The penetration testing execution standard consists of seven (7) main sections. These cover everything rela the scenes in order to get a better understanding of the tested organization, through vulnerability research, e reporting, which captures the entire process, in a manner that makes sense to the customer and provides th

This version can be considered a v1.0 as the core elements of the standard are solidified, and have been "ro a penetration test can be performed at. As no pentest is like another, and testing will range from the more m and enable the tester to step up the intensity on those areas where the organization needs them the most. S

Following are the main sections defined by the standard as the basis for penetration testing execution:

- Pre-engagement Interactions
- Intelligence Gathering
- Threat Modeling
- Vulnerability Analysis
- Exploitation
- Post Exploitation
- Reporting

PENETRATION TESTING EXECUTION STANDARD PTES Technical Guidelines

As the standard does not provide any technical guidelines as far as how to execute an actual pentest, we ha

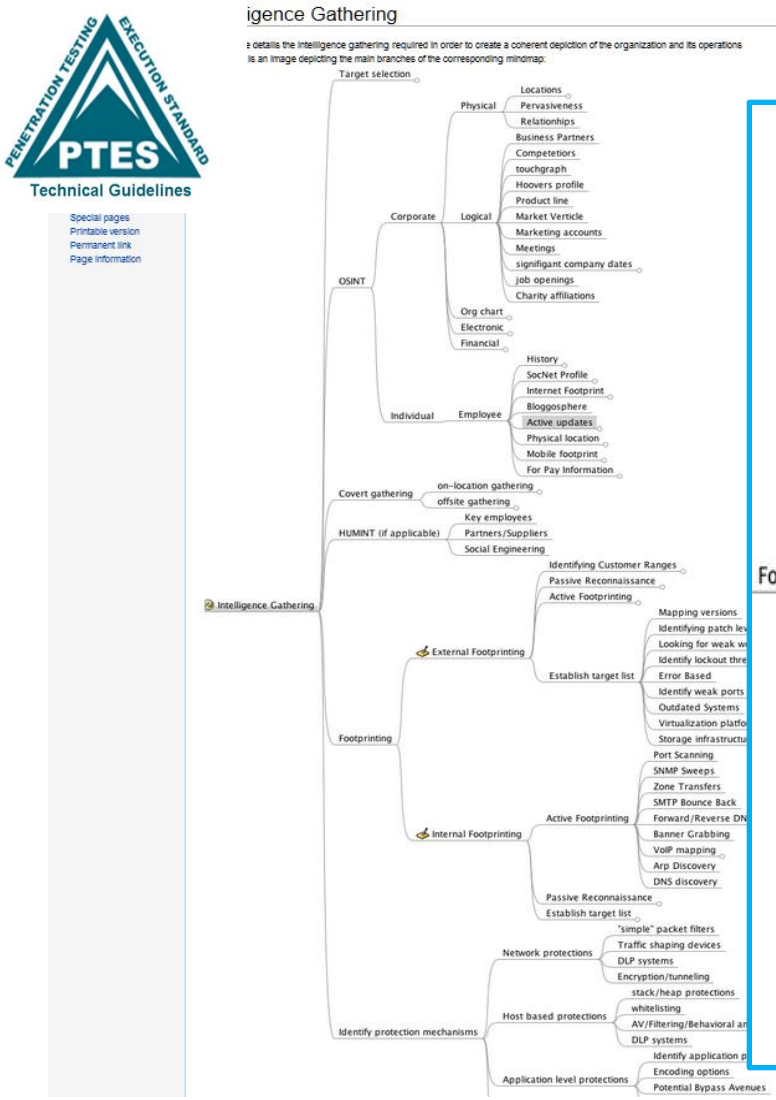
- Technical Guidelines

For more information on what this standard is, please visit:

- The Penetration Testing Execution Standard: FAQ

www.pentest-standard.org

EXISTING FRAMEWORKS OF PENTESTING

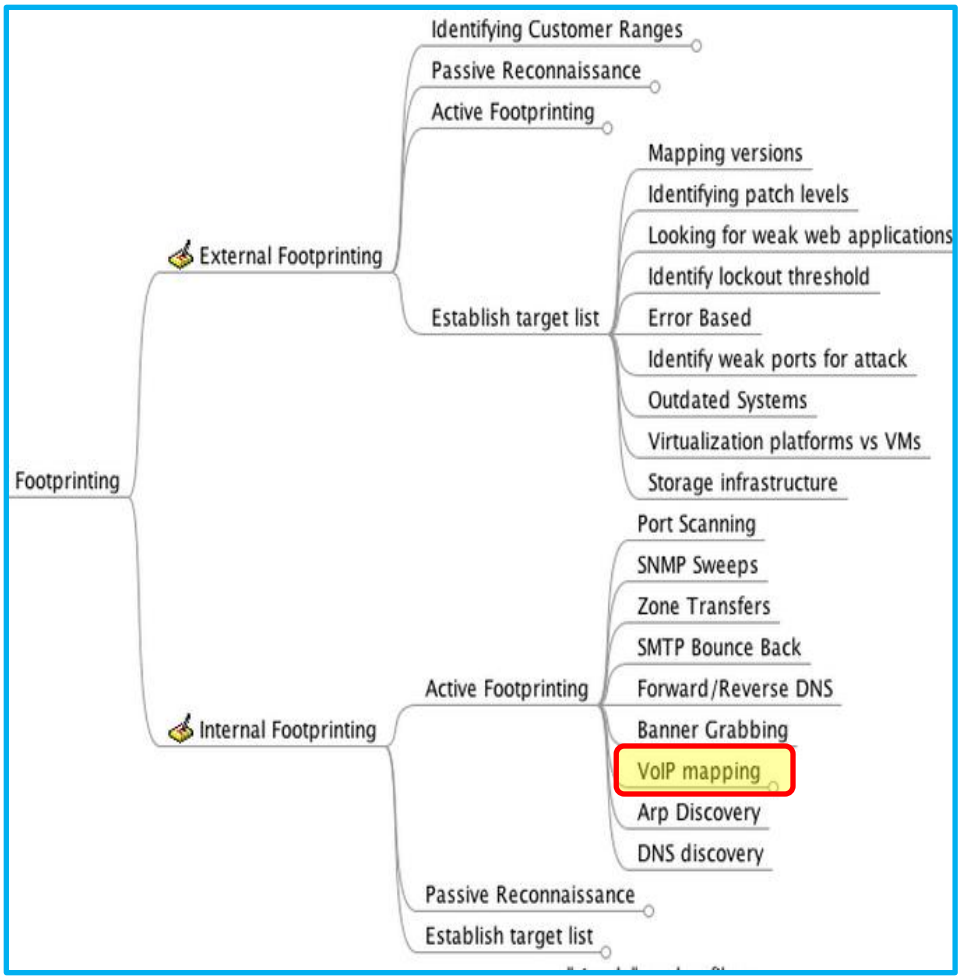


EXISTING FRAMEWORKS OF PENTESTING

2.5 External Footprinting
- 2.5.1 I
- 2.
- 2.
- 2.5.2 A
- 2.5.3 Passive Reconnaissance
- 2.5.4 Active Footprinting
  - 2.5.4.1 Zone Transfers
    - 2.5.4.1.1 Host
    - 2.5.4.1.2 Dig
  - 2.5.4.2 Reverse DNS
  - 2.5.4.3 DNS Bruting
    - 2.5.4.3.1 Fierce2 (Linux)
    - 2.5.4.3.2 DNSEnum (Linux)
    - 2.5.4.3.3 Dnsdict6 (Linux)
  - 2.5.4.4 Port Scanning
    - 2.5.4.4.1 Nmap (Windows/Linux)
  - 2.5.4.5 SNMP Sweeps
    - 2.5.4.5.1 SNMPEnum (Linux)
  - 2.5.4.6 SMTP Bounce Back
  - 2.5.4.7 Banner Grabbing
    - 2.5.4.7.1 HTTP

2.6 Internal Footprinting
- 2.6.1 Active Footprinting
  - 2.6.1.1 Ping Sweeps
    - 2.6.1.1.1 Nmap (Windows/Linux)
    - 2.6.1.1.2 Alive6 (Linux)
  - 2.6.1.2 Port Scanning
    - 2.6.1.2.1 Nmap (Windows/Linux)
  - 2.6.1.3 SNMP Sweeps
    - 2.6.1.3.1 SNMPEnum (Linux)
  - 2.6.1.4 Metasploit
  - 2.6.1.5 Zone Transfers
    - 2.6.1.5.1 Host
    - 2.6.1.5.2 Dig
  - 2.6.1.6 SMTP Bounce Back
  - 2.6.1.7 Reverse DNS
  - 2.6.1.8 Banner Grabbing
    - 2.6.1.8.1 HTTP
    - 2.6.1.8.2 httprint
  - 2.6.1.9 VoIP mapping
    - 2.6.1.9.1 Extensions
    - 2.6.1.9.2 Svwar
    - 2.6.1.9.3 enumIAX
  - 2.6.1.10 Passive Reconnaissance
    - 2.6.1.10.1 Packet Sniffing

PTES Technical Guidelines



EXISTING FRAMEWORKS OF PENTESTING

PTES Technical Guidelines

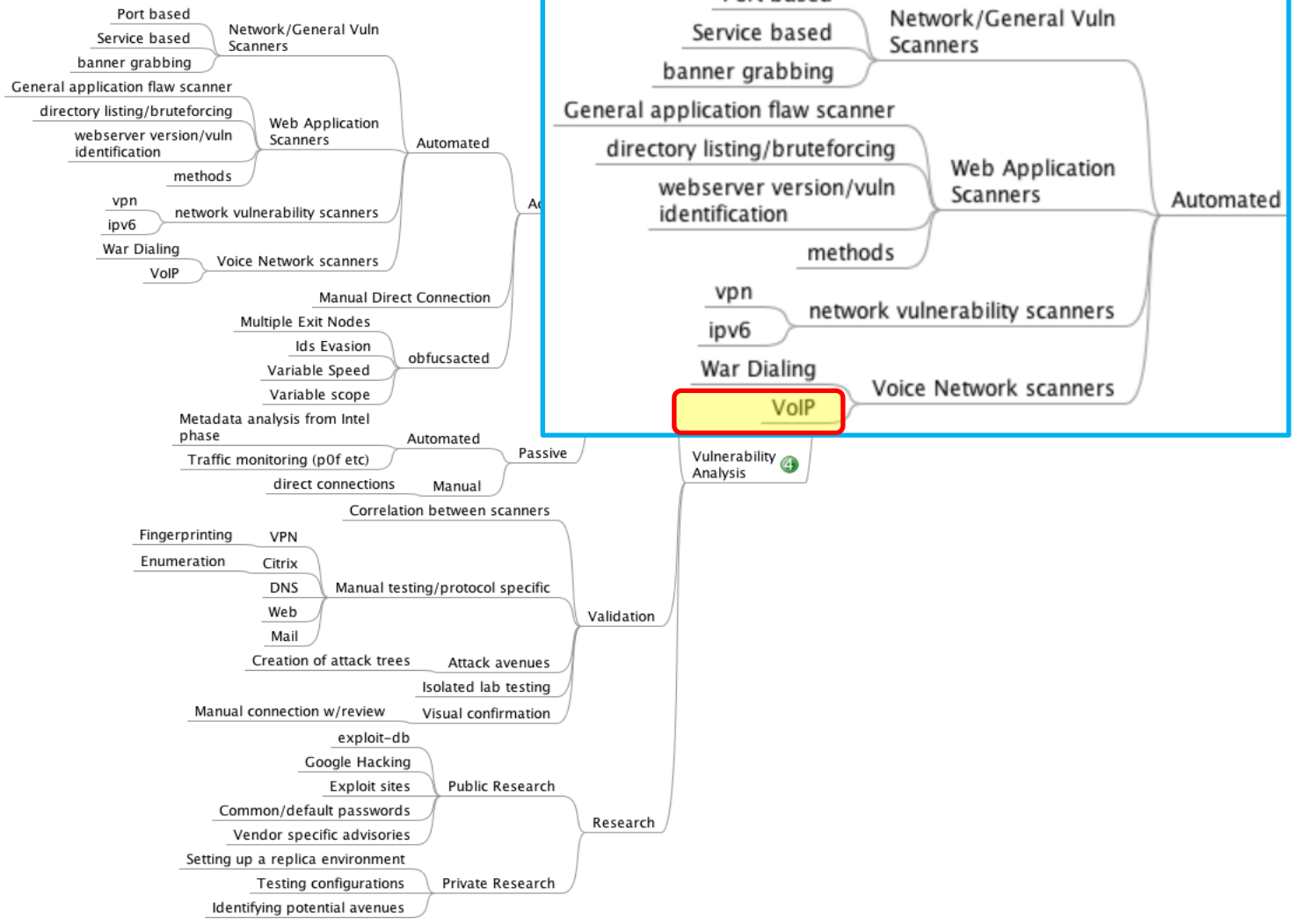
In the Media
FAQ

Tools

What links here
Related changes
Special pages
Printable version
Permanent link
Page information

Vulnerability Analysis

This phase describes the main topics that the vulnerability analysis should cover. This is of course dependent of the previous phases deliverables.
Following is an image depicting the main branches of the corresponding mindmap:



Vulnerability Analysis
Port based
Service based
banner grabbing
Network/General Vuln Scanners
General application flaw scanner
directory listing/bruteforcing
webserver version/vuln identification
methods
Web Application Scanners
Automated
vpn
ipv6
network vulnerability scanners
War Dialing
VoIP
Voice Network scanners

EXISTING FRAMEWORKS OF PENTESTING

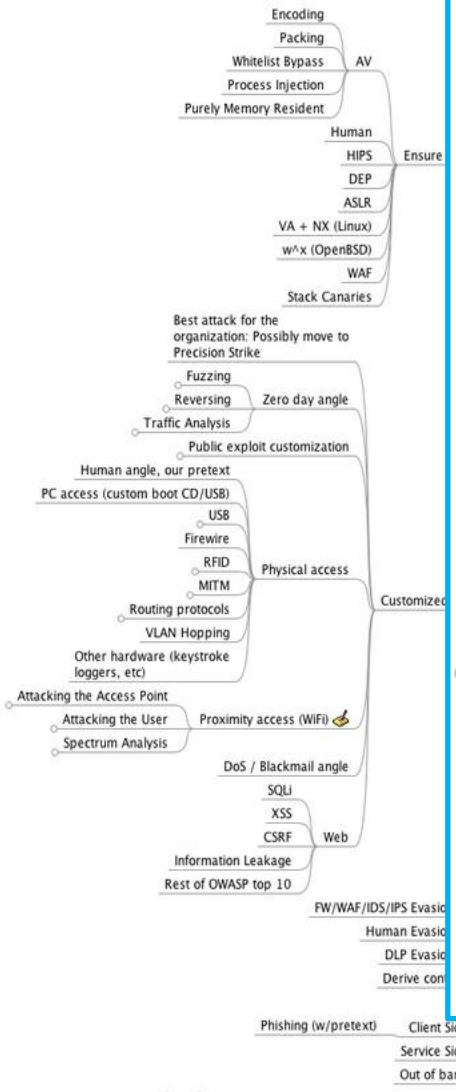
PTES Technical Guidelines

Tools

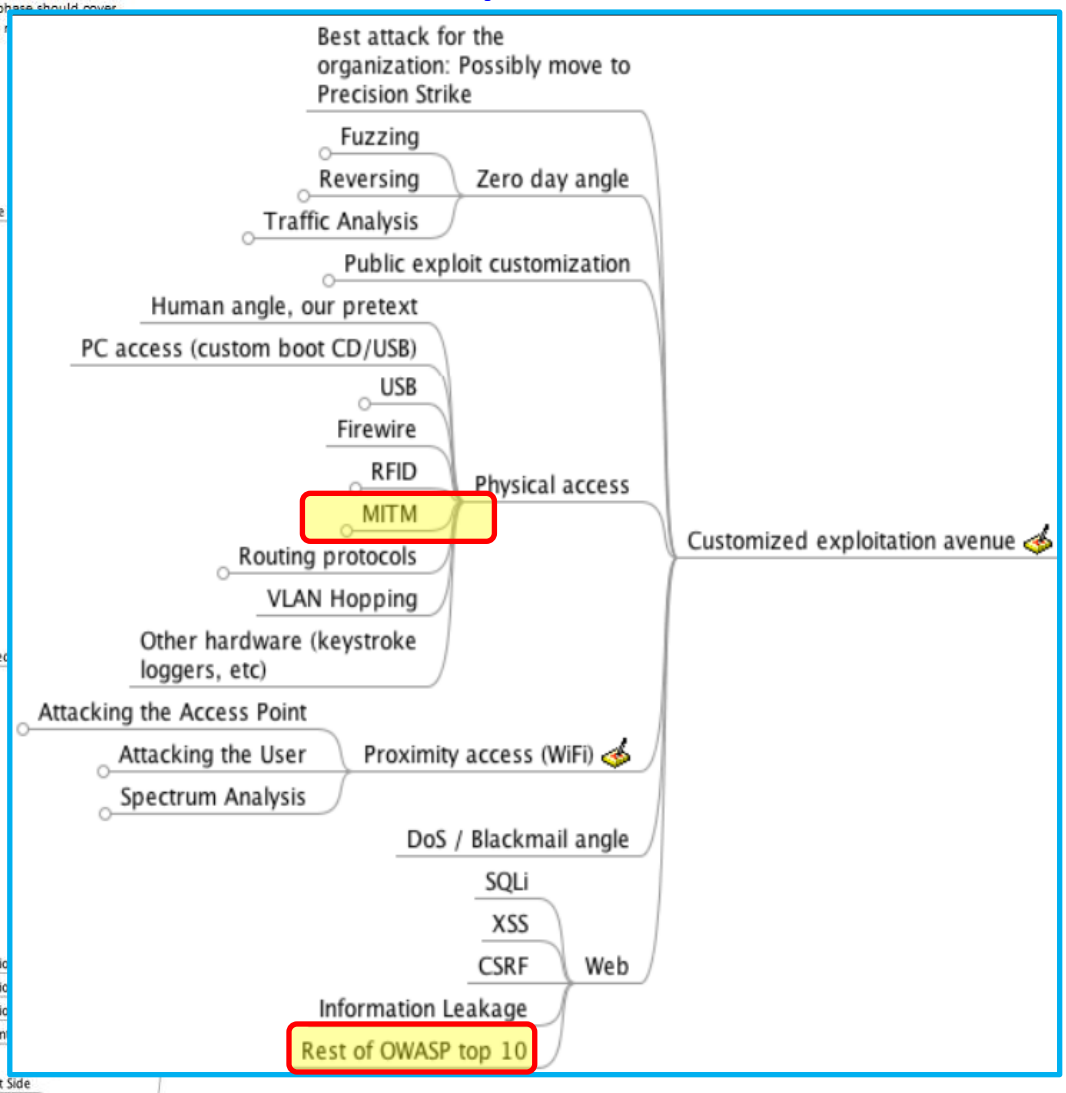
What links here
Related changes
Special pages
Printable version
Permanent link
Page information

Exploitation

This section describes the methodology and issues that the exploitation phase should cover.
Following is an image depicting the main branches of the corresponding



Exploitation



EXISTING FRAMEWORKS OF PENTESTING

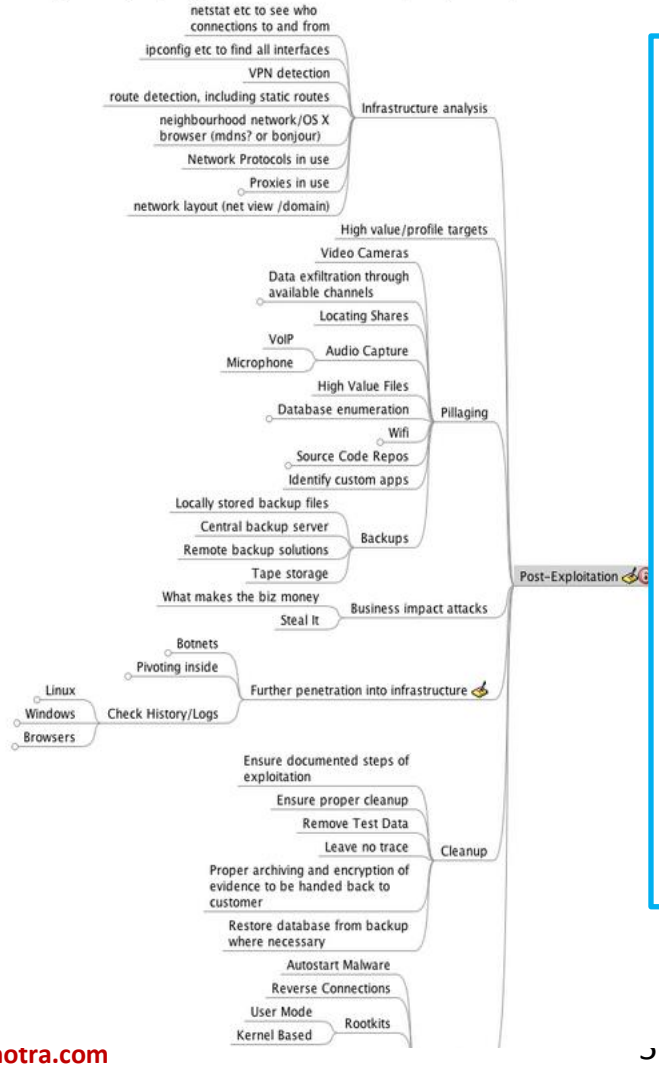
PTES Technical Guidelines

FAQ

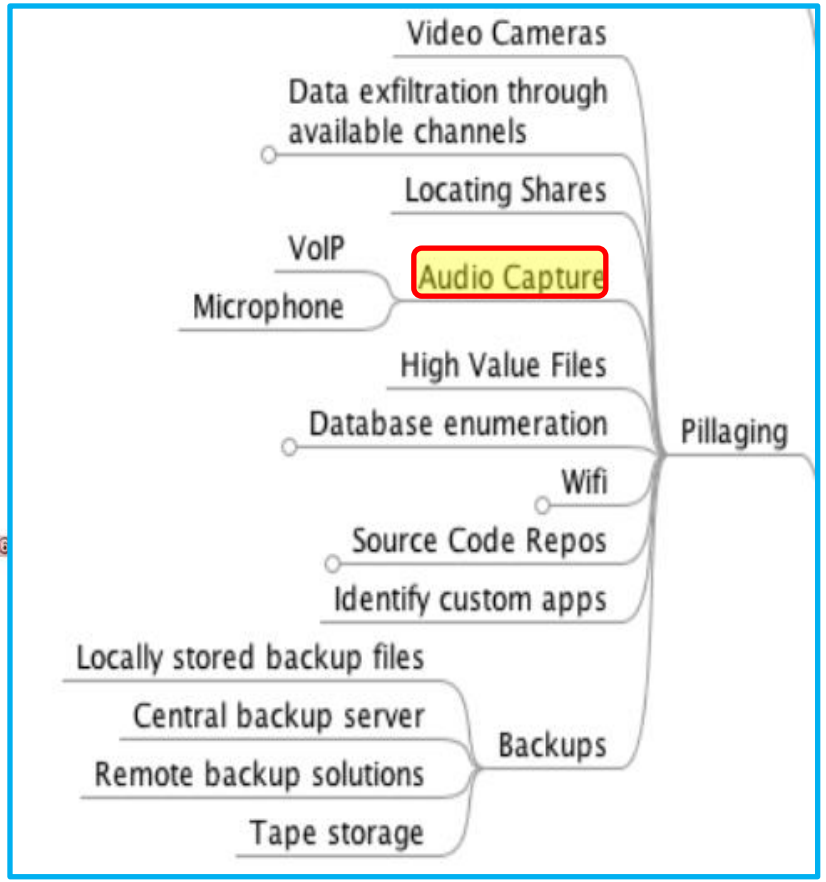
What links here
Related changes
Special pages
Printable version
Permanent link
Page information

Post Exploitation

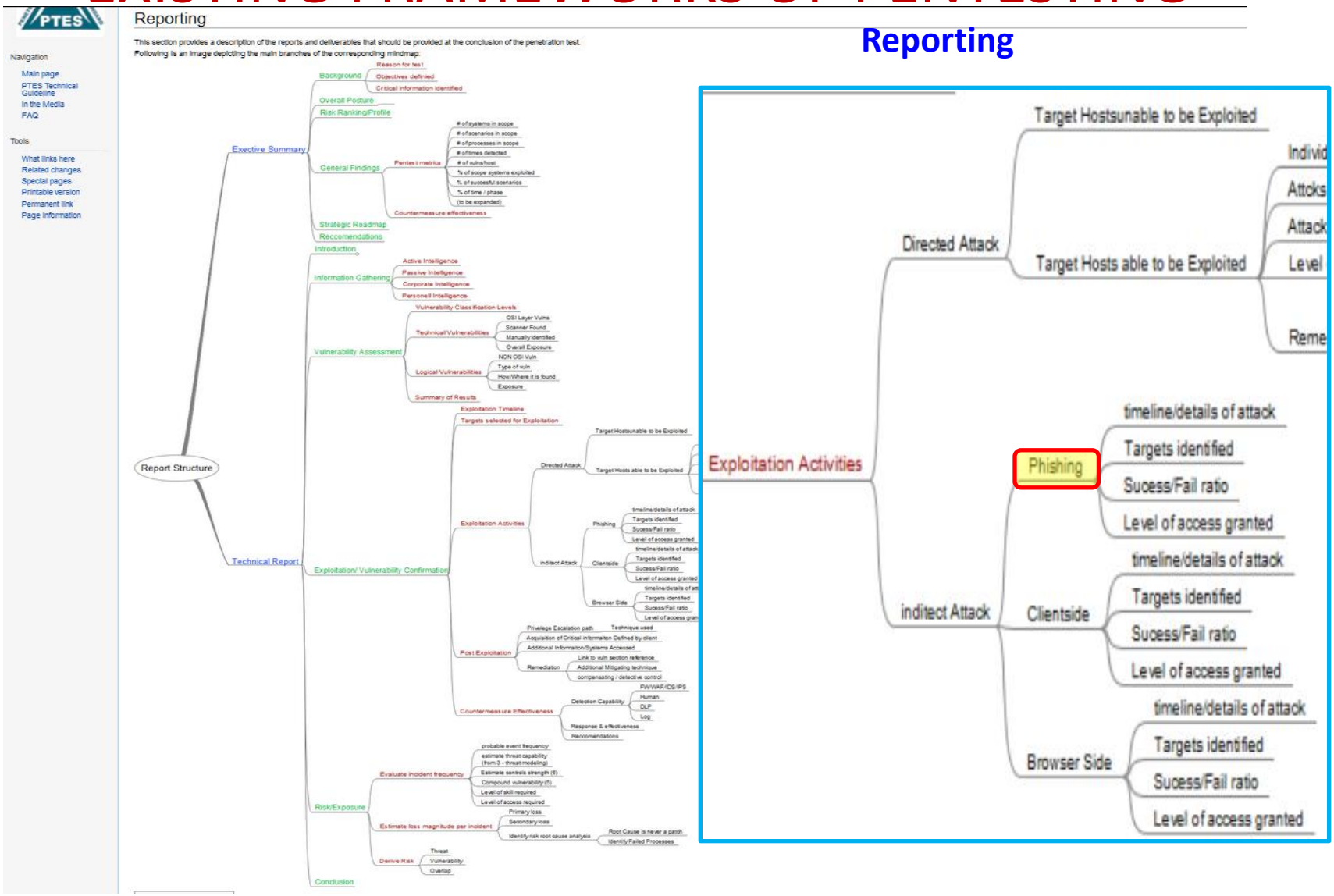
This section details the post-exploitation elements that should be addressed in a penetration test.
Following is an image depicting the main branches of the corresponding mindmap:



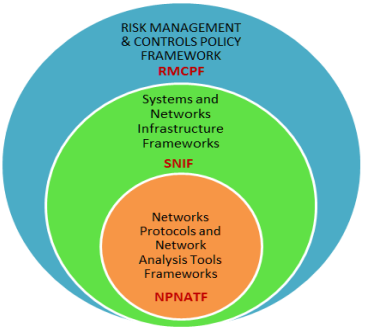
Post Exploitation



EXISTING FRAMEWORKS OF PENTESTING



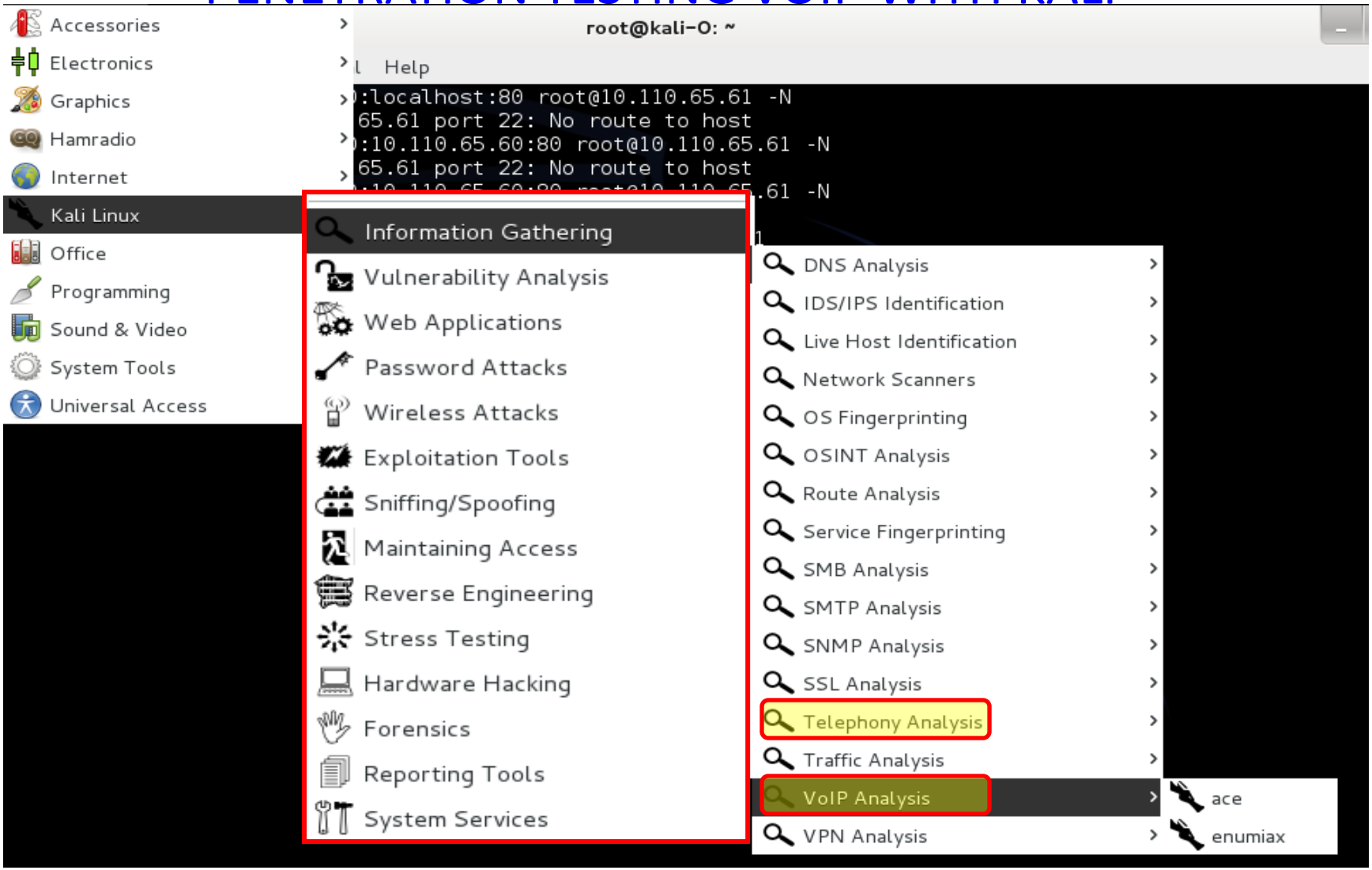
NETWORKS PROTOCOLS & TOOLS FRAMEWORKS



www.kali.org

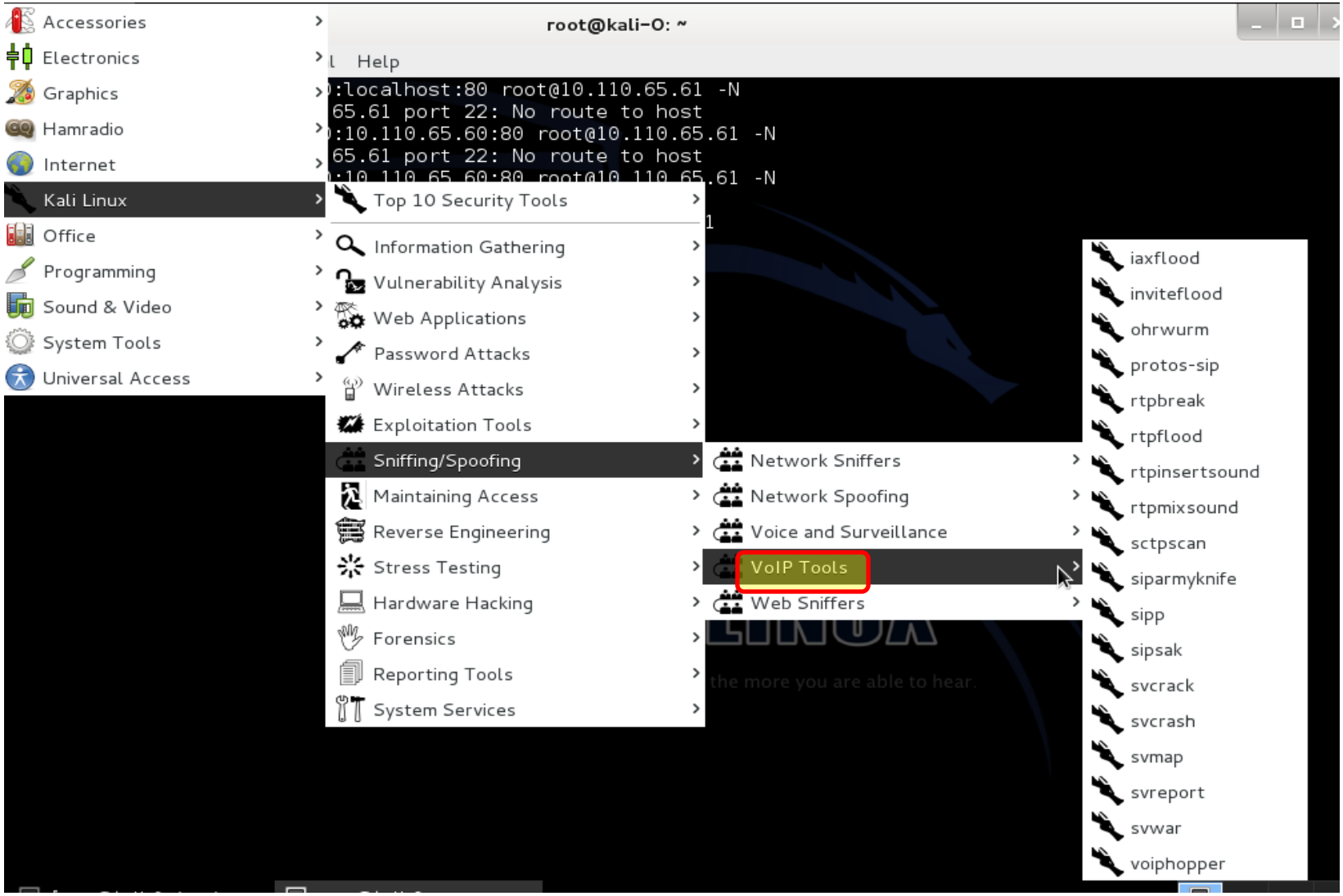
EXISTING FRAMEWORKS OF VOIP PENTESTING

PENETRATION TESTING VOIP WITH KALI



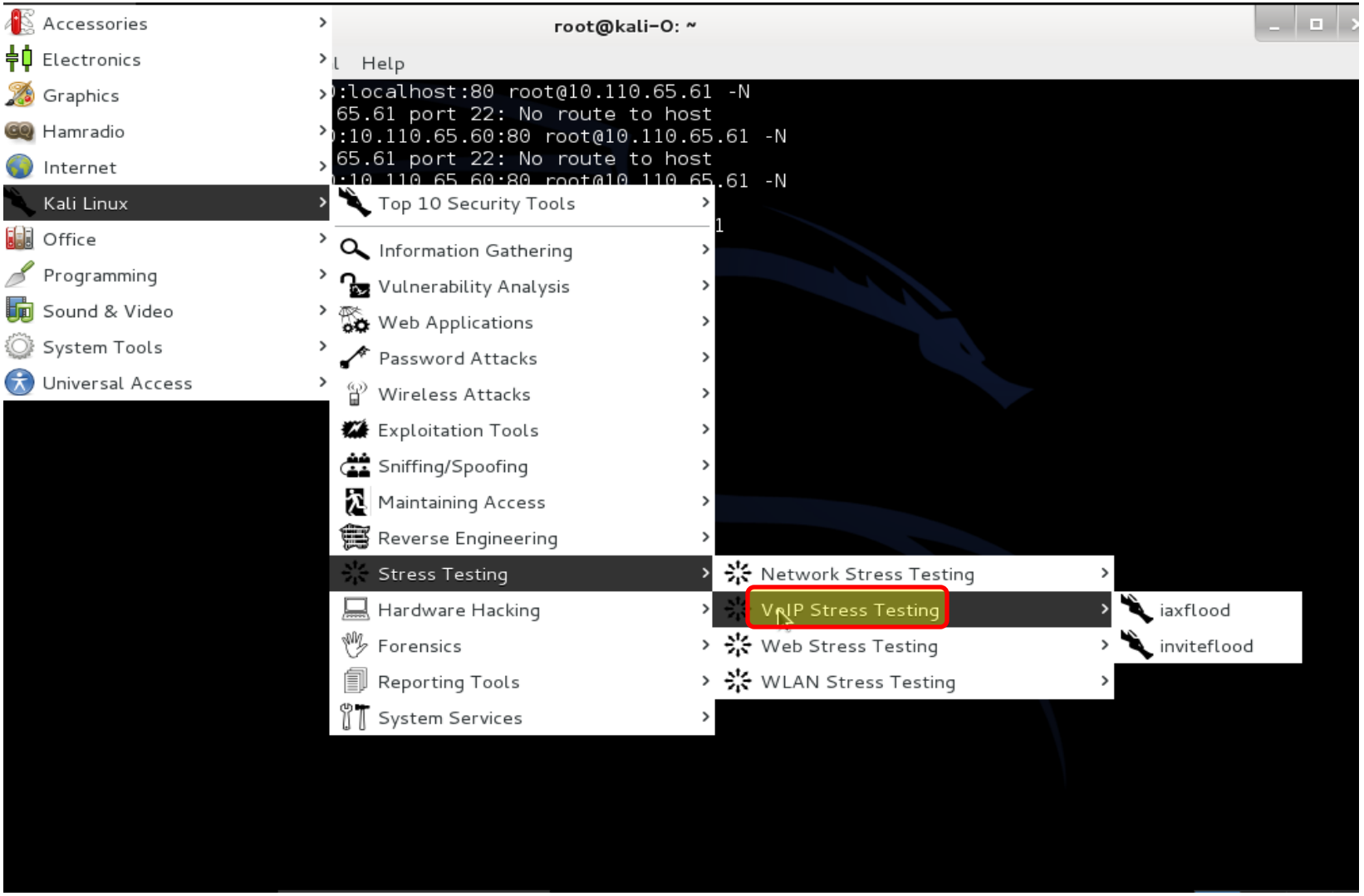
EXISTING FRAMEWORKS OF VOIP PENTESTING

PENETRATION TESTING VOIP WITH KALI



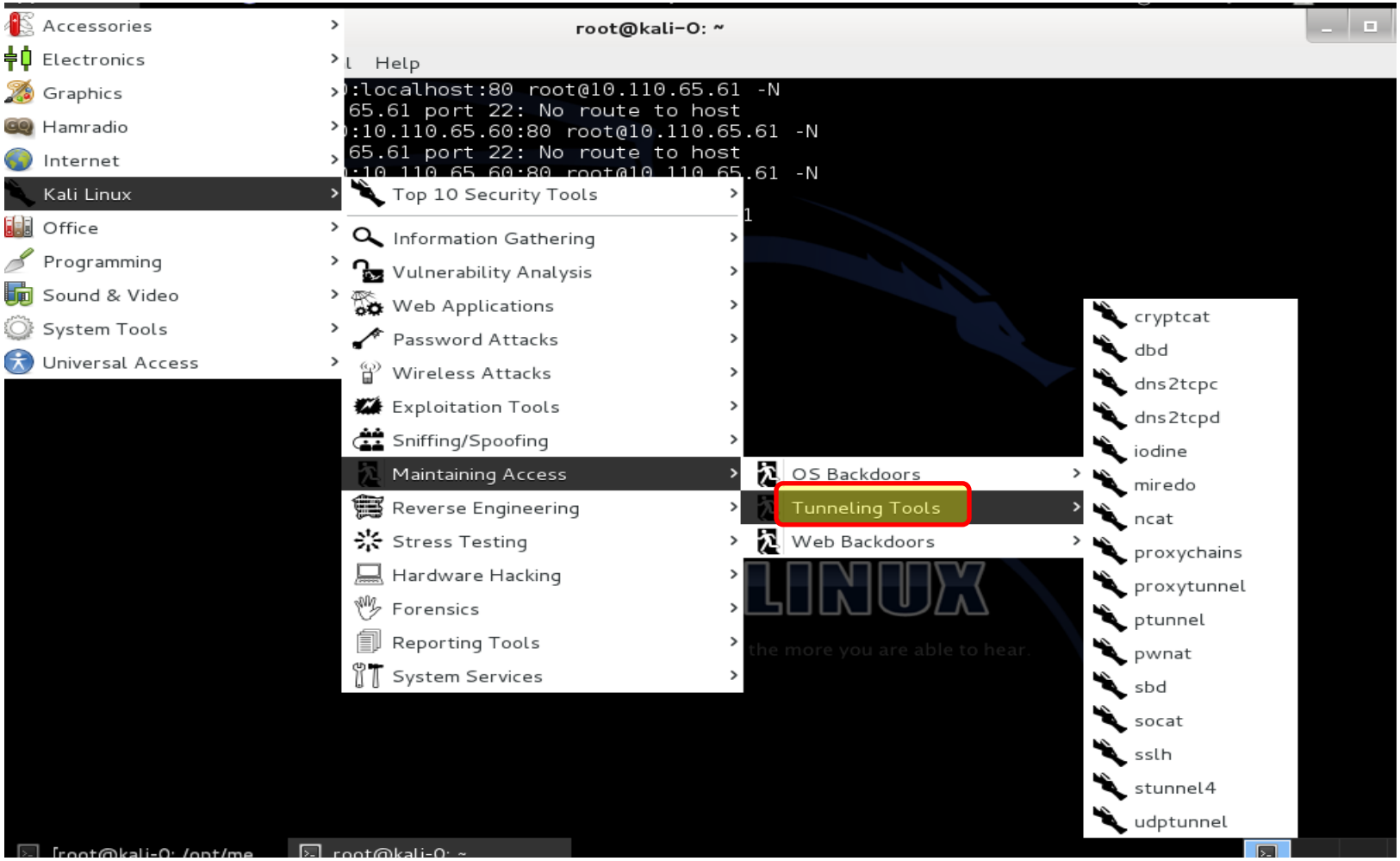
EXISTING FRAMEWORKS OF VOIP PENTESTING

PENETRATION TESTING VOIP WITH KALI



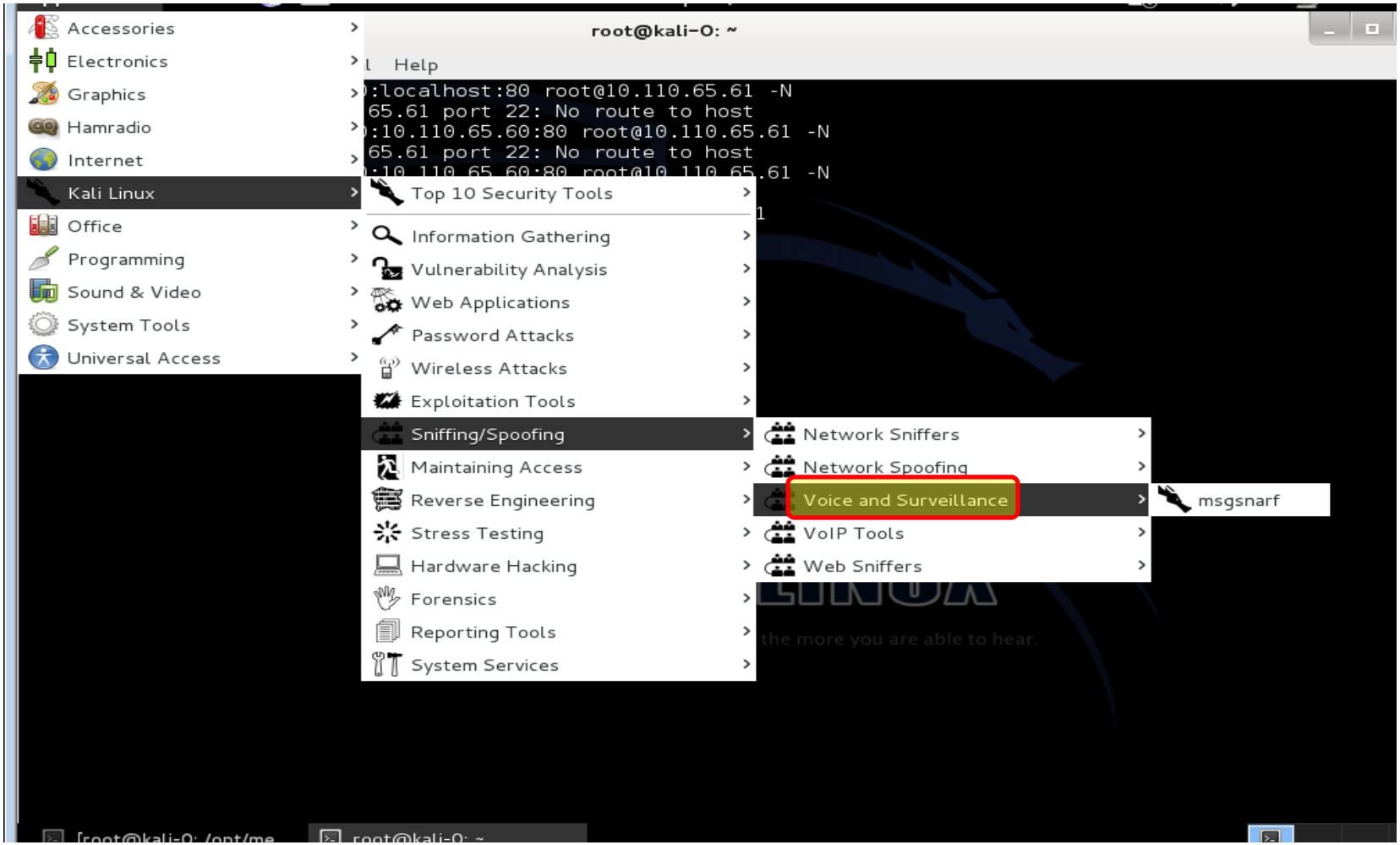
EXISTING FRAMEWORKS OF VOIP PENTESTING

PENETRATION TESTING VOIP WITH KALI



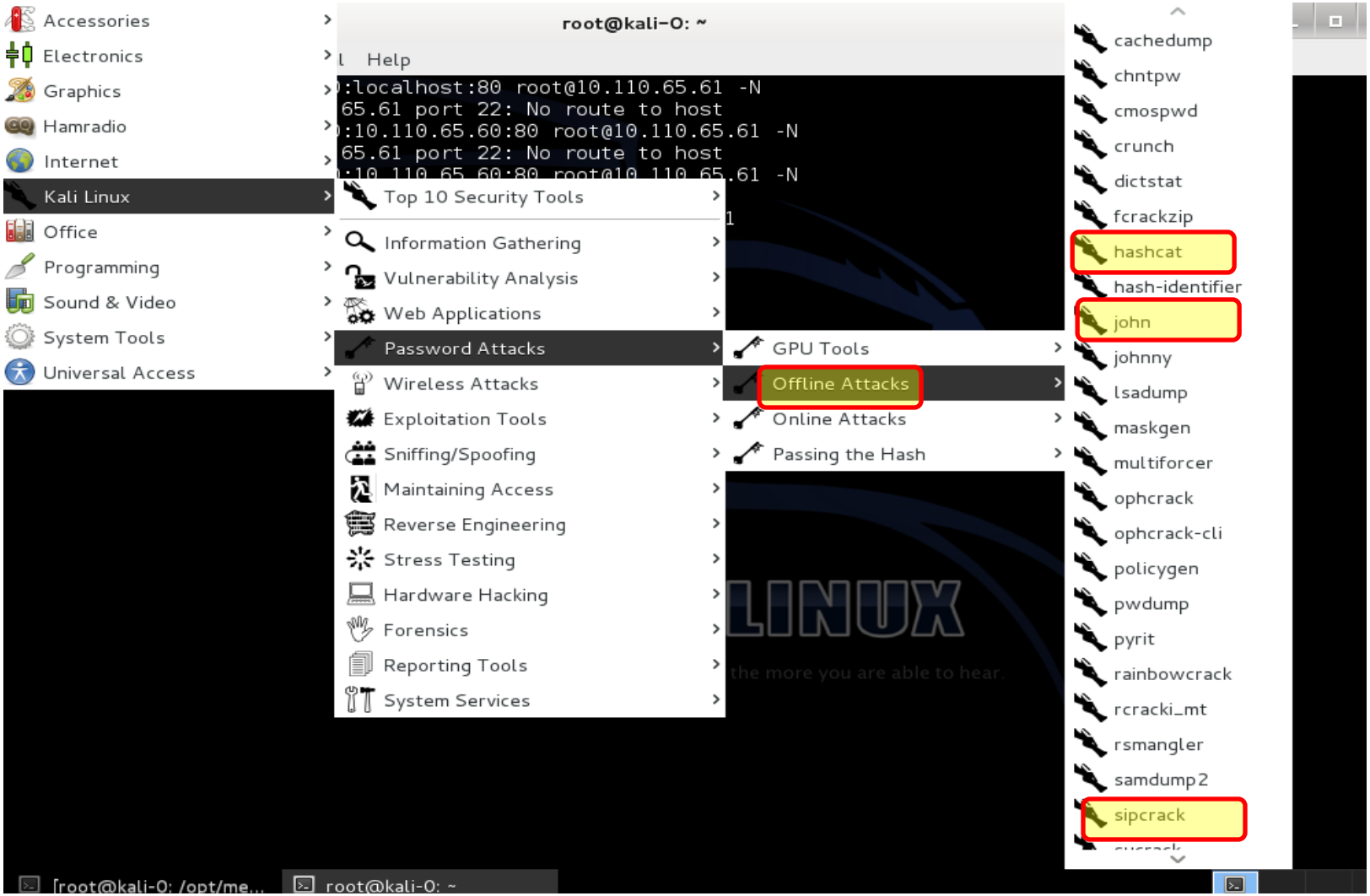
EXISTING FRAMEWORKS OF VOIP PENTESTING

PENETRATION TESTING VOIP WITH KALI



EXISTING FRAMEWORKS OF VOIP PENTESTING

PENETRATION TESTING VOIP WITH KALI



EXISTING FRAMEWORKS OF VOIP PENTESTING

PENETRATION TESTING WITH 'HACKING VOIP'

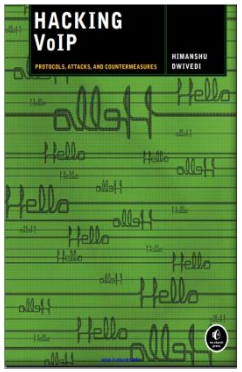
VOIP PROTOCOLS

SIGNALING: SIP SECURITY

SIP Basics .....
SIP Messages .....
Making a VoIP Call with SIP Methods .....
- Registration .....
- The INVITE Request .....

Enumeration and Registration .....
- Enumerating SIP Devices on a Network .....
- Registering with Identified SIP Devices .....
- Authentication .....
- Encryption .....

SIP Security Attacks .....
- Username Enumeration .....
- SIP Password Retrieval .....
- Man-in-the-Middle Attack .....
- Registration Hijacking .....
- Spoofing SIP Proxy Servers and Registrars .
- Denial of Service via BYE Message .....
- Denial of Service via REGISTER .....
- Denial of Service via Un-register .....
- Fuzzing SIP .....



SIGNALING: H.323 SECURITY

H.323 Security Basics .....
- Enumeration .....
- Authentication .....
- Authorization .....

H.323 Security Attacks .....
- Username Enumeration (H.323 ID) .....
- H.323 Password Retrieval .....
- H.323 Replay Attack .....
- H.323 Endpoint Spoofing (E.164 Alias) .....
- E.164 Alias Enumeration .....
- E.164 Hopping Attacks .....
- Denial of Service via NTP .....
- Denial of Service via UDP (H.225 Registration Reject)
- Denial of Service via Host Unreachable Packets .....
- Denial of Service via H.225 nonStandardMessage ..

MEDIA: RTP SECURITY

RTP Basics .....
RTP Security Attacks .....
- Passive Eavesdropping
- Active Eavesdropping ..
- Denial of Service .....

EXISTING FRAMEWORKS OF VOIP PENTESTING

PENETRATION TESTING WITH 'HACKING VOIP'

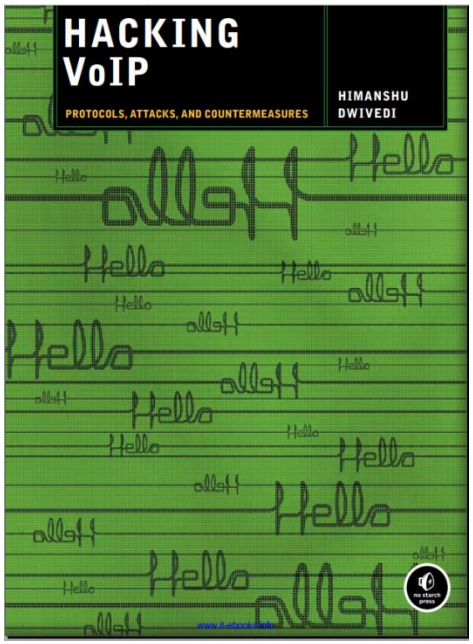
VOIP PROTOCOLS

MEDIA: RTP SECURITY

RTP Basics .....
RTP Security Attacks .....
- Passive Eavesdropping
- Active Eavesdropping ..
- Denial of Service .....

SIGNALING AND MEDIA: IAX SECURITY

IAX Authentication .....
IAX Security Attacks .....
- Username Enumeration .....
- Offline Dictionary Attack .....
- Active Dictionary Attack .....
- IAX Man-in-the-Middle Attack .....
- MD5-to-Plaintext Downgrade Attack .....
- Denial of Service Attacks .....



EXISTING FRAMEWORKS OF VOIP PENTESTING

PENETRATION TESTING WITH 'HACKING VOIP'

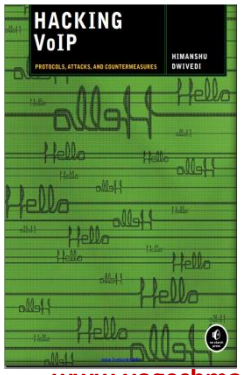
VOIP SECURITY THREATS

ATTACKING VOIP INFRASTRUCTURE

Vendor-Specific VoIP Sniffing .....
Hard Phones .....
- Compromising the Phone's Configuration File .....
- Uploading a Malicious Configuration File .....
- Exploiting Weaknesses of SNMP .....

Cisco CallManager and Avaya Call Center .....
- Using Nmap to Scan VoIP Devices .....
- Scanning Web Management Interfaces with Nikto
- Discovering Vulnerable Services with Nessus .....

Modular Messaging Voicemail System .....
Infrastructure Server Impersonation .....
- Spoofing SIP Proxies and Registrars .....
- Redirecting H.323 Gatekeepers .....



UNCONVENTIONAL VOIP SECURITY THREATS

VoIP Phishing .....
- Spreading the Message .....
- Receiving the Calls .....

Making Free Calls .....
Caller ID Spoofing .....
- Example 1 .....
- Example 2 .....
- Example 3 .....
- Example 4 .....

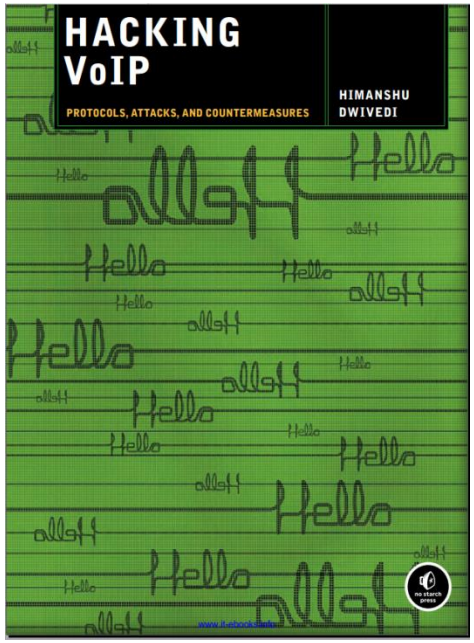
Anonymous Eavesdropping and Call Redirection .....
Spam Over Internet Telephony .....
- SPIT and the City .....
- Lightweight SPIT with Skype/Google Talk .....

EXISTING FRAMEWORKS OF VOIP PENTESTING

PENETRATION TESTING WITH 'HACKING VOIP'

SECURING VOIP

AUDITING VOIP FOR SECURITY BEST PRACTICES



EXISTING FRAMEWORKS OF VOIP PENTESTING

AUDITING VOIP FOR SECURITY WITH 'HACKING VOIP'

SIP authentication

SIPS, or SIP wrapped in a TLS tunnel, should be used for session layer protection when using SIP.

SIP register

SIP User Agent should authenticate `REGISTER` and `INVITE` requests.

H.225 authentication

H.225 wrapped in a TLS tunnel should be used for session layer protections using H.323.

H.225 MD5 authentication time

To limit replay attacks, low NTP thresholds should be used with H.225 MD5 authentication.

IAX authentication

IAX wrapped in a TLS tunnel should be used for session layer protection when using IAX.

Concurrent SIP/IAX/H.323 se

Do not allow concurrent sessions with a single username and password (one session per account).

Session layer unregistration

Session protocols, such as SIP, H.323, and IAX, should require authentication to unregister an endpoint or User Agent.

LDAP over SSL

If H.323 endpoints or SIP User Agents use an LDAP store for authentication, ensure that LDAP over SSL is enabled to protect authentication credentials.

Media encryption

Voice communication should be encrypted if it contains private, sensitive, or confidential information.

SRTP key exchange

When SRTP is used, the key exchange should not traverse the network in cleartext. Hence, TLS should be used at all times with SIP or H.323 when SRTP is enabled (otherwise, any security enabled with SRTP is negated).

RTP entropy

RTP packets need to contain an adequate level of entropy to help prevent RTP injection attacks. Ensure that the full 64-bits of the SSRC, sequence number, and timestamp use random values rather than sequential values.

IAX media communication

Voice communication should be encrypted if it contains private, sensitive, or confidential information.

E.164 aliases

E.164 aliases should be unique and difficult to spoof or enumerate.

Duplicate E.164 alias handlin

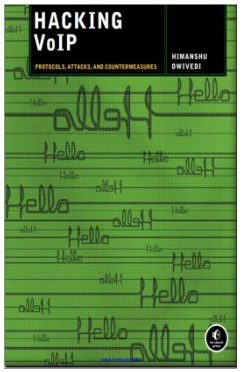
A gatekeeper's registration conflict policy should be set to `Reject`, which will prevent spoofed E.164 aliases from overwriting legitimate endpoints. It should be noted that with this setting, an attacker can perform a Denial of Service attack on a legitimate endpoint, register with the gatekeeper, and prevent the legitimate endpoint from registering when it comes back online (because of the `Reject` policy). Ensure that DoS attacks on endpoints are mitigated before setting the policy.

Authentication/authorization

A compromised E.164 alias should be useless without the corresponding authentication information.

E.164 duplicate errors

Vague error messages for duplicate E.164 aliases should be used.



EXISTING FRAMEWORKS OF VOIP PENTESTING

AUDITING VOIP FOR SECURITY WITH 'HACKING VOIP'

802.1x

802.1x-compliant devices, including endpoints and User Agents, should be used on VoIP networks.

VLAN usage

VLANs are good for segmentation but should not be used as a security control because an attacker can simply unplug a VoIP hard phone from the closest Ethernet jack and plug into the VoIP network with his or her PC. 802.1x can be used to ensure that unauthorized systems are not connected to the VoIP VLAN.

ARP monitoring

Enable ARP monitoring on all video conference networks to detect ARP pollution/ poisoning attacks.

Network segmentation

While not a security control, VoIP networks should be separated from data networks.

In-band/out-of-band manageme

Management methods for VoIP devices should be out-of-band and managed from a secure and trusted management network. VoIP devices should not be managed from in-band data connections.

VoIP management filtering

VoIP device management should be limited to authorized machines using IP address and hostname filters.

VoIP management protocols

Password authentication for management purposes should use encrypted protocols.

SNMP

The use of SNMPv1 is strongly discouraged. If it is a business requirement, use difficult-to-guess community strings and restrict access via a firewall or router access control lists.

Timestamp/date

Date and timestamp information should be current in order to ensure the integrity of all log files.

Logging

All VoIP devices should log important activity to the management software. Logs should be reviewed regularly.

Hard phone PINs

PINs for hard phones should be unique and consist of more than four characters.

Hard phone boot process

Hard phones should use HTTPS for boot files over the network.

Toll fraud and abuse

On VoIP devices, enable server-side controls that help prevent the abuse of the phone system. For example, create explicit permissions on who can make calls outbound, join conferences, and make international outbound calls.

AutoDiscovery

Gatekeepers, Border Controllers, and endpoints should have static IP addresses listed on them.

SSL certificates

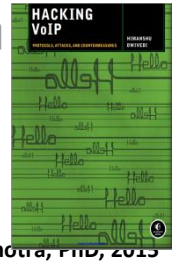
Devices using SSL for authentication or media communication should use strong SSL certificates.

SSL certificates checking

Incorrect, CName mismatch, or example SSL certificates to and from VoIP devices are automatically disabled.

DHCP/DNS servers

Supporting VoIP infrastructure services, such as DHCP and DNS, should use dedicated resources that are not shared with user and data networks.



EXISTING FRAMEWORKS OF VOIP PENTESTING

PENETRATION TESTING & SECURITY WITH 'SECURING VOIP'

VoIP Architectures and Protocols

Architectures
VoIP Network Components
Signaling Protocols
Media Transport Protocols
Other IP Protocols Used in VoIP
Summary

Threats and Attacks

Definitions of Threats and Attacks
Threats in VoIP
Service Disruption
Attacks Related to Telephony Services
Denial of Service
Annoyance (That Is, SPIT)
Unauthorized Access
Eavesdropping
Masquerading
Fraud

VoIP Vulnerabilities

Categories of Vulnerabilities
Configuration Management Vulnerabilities in VoIP
Approaches to Vulnerability Analysis
Human Behavior Vulnerabilities

Signaling Protection Mechanisms

SIP Protection Mechanisms
Transport Layer Security
Datagram Transport Layer Security
S/MIME
IPSec
H.323 Protection Mechanisms
MGCP Protection Mechanisms

Media Protection Mechanisms

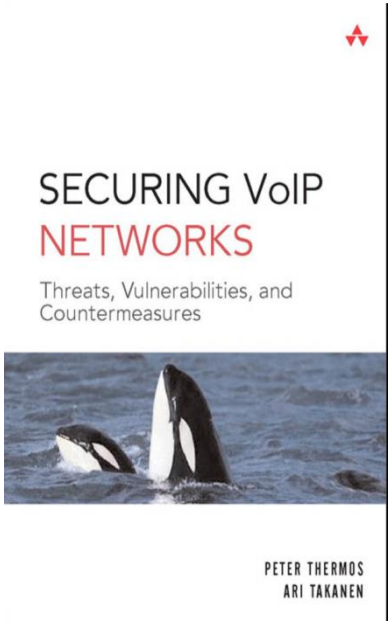
SRTP
SRTCP

Key Management Mechanisms

MIKEY
SRTP Security Descriptions
ZRTP

VoIP and Network Security Controls

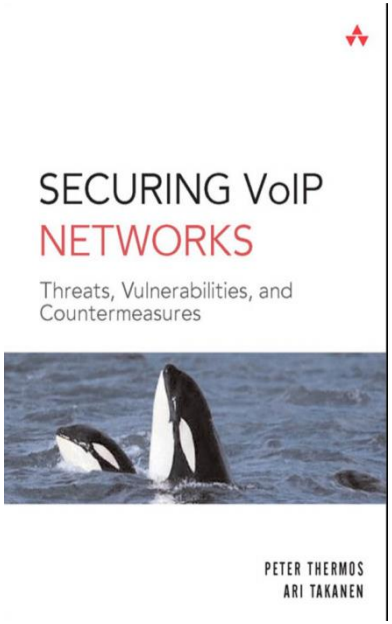
Architectural Considerations
Authentication, Authorization, and Auditing: Diameter
User-Authorization-Request Command
VoIP Firewalls and NAT
Session Border Controllers
Intrusion Detection and VoIP



EXISTING FRAMEWORKS OF VOIP PENTESTING

PENETRATION TESTING & SECURITY WITH 'SECURING VOIP'

A Security Framework for Enterprise VoIP Networks

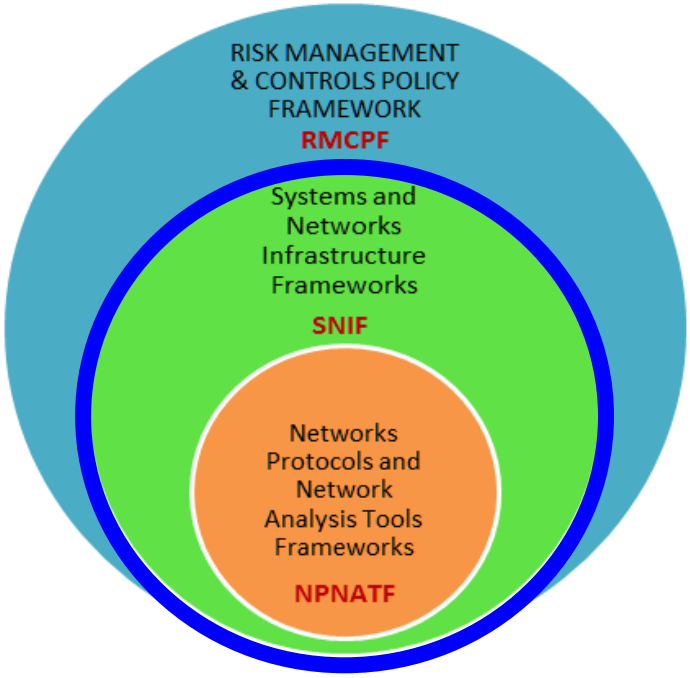


SYSTEMS AND NETWORKS LEVEL FRAMEWORKS

ERM

MRM

C-FRM



Connect Enterprise RM concerns to Pen Testing RM level concerns.

Align and Streamline Shared RM Goals and Outcomes at Top and all Other levels.

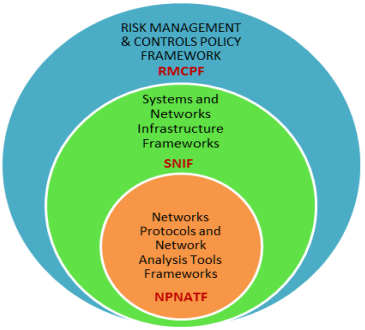
RM-Controls Policy Executives cognizant of how policy translates into actual execution.

Pen Testing within RM framework of importance and resource allocation.

Pen Test team cognizant of contributions to value added at overall Enterprise Level.

At this specific level the focus of most procedures and techniques is at the systems and networks level rather than at the more granular level of telecom network protocols.

SYSTEMS AND NETWORKS LEVEL FRAMEWORKS



Home
About OWASP
Acknowledgements
Advertising
AppSec Events
Books
Brand Resources
Chapters
Donate to OWASP
Downloads
Funding
Governance
Initiatives
Mailing Lists
Membership
Merchandise
News
Community portal
Presentations
Press
Projects
Video
Volunteer

Reference
Activities
Attacks
Code Snippets

Page | Discussion | Read | View source | V

The OWASP Testing Framework

OWASP Testing Guide v3 Table of Contents

This article is part of the OWASP Testing Guide v3. The entire OWASP Testing Guide v3 can be downloaded here.

OWASP at the moment is working at the OWASP Testing Guide v4: you can browse the Guide here

[hide]

www.owasp.org/index.php/The_OWASP_Testing_Framework

EXISTING FRAMEWORKS OF VOIP PENTESTING

Page Discussion Read View sc

Web Application Penetration Testing

Footprinting

Scanning

Enumeration

Infrastructure Denial of Service

- DNS Auditing tool
- Internetwork Routing Protocol Attack Suite
- UDP Flooder
- Wireshark

Eavesdropping

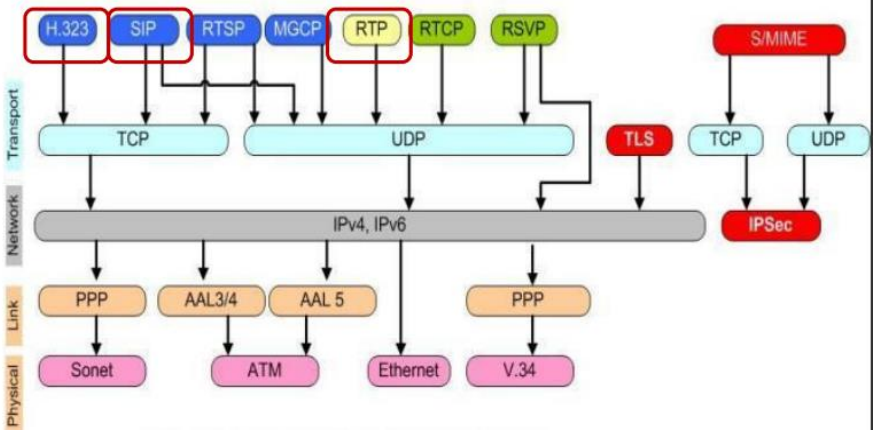
- Cain and Abel
- dsniff
- VoIPong
- vomit

Network and Application Interception

- arpwatch
- Cain and Abel
- Dsniff
- Ettercap
- siprogue

Fuzzing

- ohrwurm RTP fuzzer
- PROTOS SIP fuzzing suite
- TCPView



EXISTING FRAMEWORKS OF PENTESTING

ERNST & YOUNG

Uses various tools and techniques to identify, & try to exploit security vulnerabilities to gain access to data and systems.

- May not produce a comprehensive list of all vulnerabilities within a client's IT infrastructure, due to time limits and customer limitations.
- Because of this, risk management is imperative.

The Causes - VoIP

- Lack of segmentation from IP data networks
  - Very common to see 802.1q VLAN tagging
- VOIP solutions built on common hacking targets
  - Cisco Call Manager & Microsoft Windows 2000, Microsoft SQL Server
- Encryption usually supported, but not enabled
  - Commonly due to performance issues, or lack of manageability

Solutions - VoIP

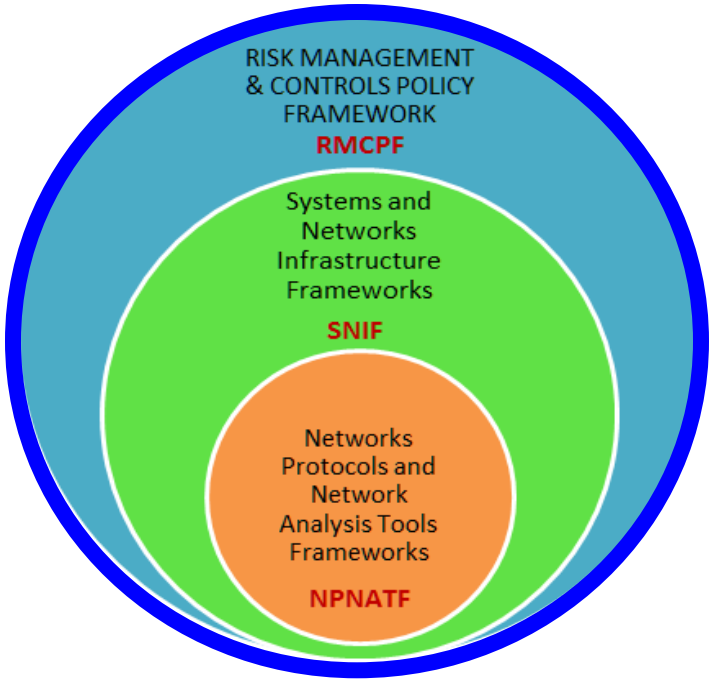
- Firewalls and segregation controls
  - Separate voice from data traffic
- Consider enabling encryption
  - Consider what voice traffic may be more sensitive than others
- Hardening VoIP devices
  - Install the latest patches, restrict connecting devices, authenticate devices
- Monitoring VoIP related logs
  - Consider review of system logs, application logs, security logs

RISK MANAGEMENT CONTROLS FRAMEWORKS

ERM

MRM

C-FRM



Connect Enterprise RM concerns to Pen Testing RM level concerns.

Align and Streamline Shared RM Goals and Outcomes at Top and all Other levels.

RM-Controls Policy Executives cognizant of how policy translates into actual execution.

Pen Testing within RM framework of importance and resource allocation.

Pen Test team cognizant of contributions to value added at overall Enterprise Level.

However, for either of SNIF and NPNATF to have real teeth and real resources for them to have the needed effect, they need to be effectively linked and related to the top level RMCPF.

BANKING & FINANCE INDUSTRY VOIP STANDARDS

"Use of VoIP has become a primary component of enterprise electronic communications. As such, it is the conduit for all multimedia electronic communications, including voice, short message service (SMS) texts and video."

"Many organizations have embraced several frameworks at an enterprise level, including the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Internal Control Framework. The importance of the control framework has been enhanced due to regulatory requirements by the US Securities and Exchange Commission (SEC) as directed by the US Sarbanes-Oxley Act of 2002 and similar legislation in other countries. Enterprises seek to integrate control framework elements used by the general audit/assurance team into the IT audit and assurance framework. Since COSO is widely used, it has been selected for inclusion in this audit/assurance program."

"Since VoIP uses the IP protocol, it is vulnerable to the usual attacks by hackers, malware, etc. In addition, failure to enforce adequate separation between voice and data circuits implies that if either one were to be compromised, the enterprise would be exposed to the partial or complete loss of both critical functions."

BANKING & FINANCE INDUSTRY VOIP STANDARDS

VoIP Threat Taxonomy

Type of Risk	Threats
Disruption of VoIP Data and Service	VoIP Control Packet Flood
	VoIP Call Data Flood
	TCP/UDP/ICMP Packet Flood
	VoIP Implementation DoS Exploit
	OS/Protocol Implementation DoS Exploit
	VoIP Protocol DoS Exploit
	Wireless DoS Attack
	Network Service DoS Attacks
	VoIP Application DoS Attacks
	VoIP Endpoint PIN Change
	VoIP Packet Replay
	VoIP Packet Injection
	VoIP Packet Modification
	QoS Modification
	VLAN Modification
VoIP Data and Service Theft	VoIP Social Engineering
	Rogue VoIP Device Connection
	ARP Cache Poisoning
	VoIP Call Hijacking
	Network Eavesdropping
	VoIP Application Data Theft
	Address Spoofing
	VoIP Call Eavesdropping
	VoIP Control Eavesdropping
	VoIP Toll Fraud
	VoIP Voice Mail Hacks

BANKING & FINANCE INDUSTRY VOIP STANDARDS

ISACA Controls Framework

As described in the following Executive Summary, VoIP server is an architecture that supports and drives business processes.

The primary COBIT processes associated with an implementation of VoIP server are as follows:

- PO2 *Define the Information Architecture*—Defined data classification scheme used to establish content security requirements
- PO6 *Communicate Management Aims and Direction*—Once governance and policies are established communicating same to the users
- AI1 *Identify Automated Solutions*—Business requirements necessary to define and implement business processes
- AI3 *Acquire and Maintain Technology Infrastructure*—Technology architecture required to support the VoIP server environment and ensure alignment with the enterprise architecture
- DS5 *Ensure Systems Security*—Security configuration and processes required to secure the VoIP server contents
- DS9 *Manage the Configuration*—Configuration settings of the various servers which support the infrastructure of VoIP server.
- DS11 *Manage Data*—Data management classification, storage, and retention
- ME2 *Monitor and Evaluate Internal Control*—The decentralized nature of VoIP server installations requires the monitoring of internal control by as a part of the management structure
- ME3 *Ensure Compliance with External Requirements*—Compliance with regulatory and legal entities associated with the VoIP server content
- ME4 *Provide IT Governance*—Decentralized VoIP server environments, managed by users requires policies and processes to assure adherence to internal controls, effective and efficient data management, and accompanying management oversight

BANKING & FINANCE INDUSTRY VOIP STANDARDS

ISACA VoIP Audit/Assurance Program

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
1. PLANNING AND SCOPING THE AUDIT									
1.1 Define the audit/assurance objectives. The audit/assurance objectives are high-level and describe the overall audit goals.									
1.1.1 Review the audit/assurance objectives in the introduction to this audit/assurance program.									
1.1.2 Modify the audit/assurance objectives to align with the audit/assurance universe, annual plan and charter.									
1.2 Define audit assignment success. The success factors need to be identified. Communication among the IT audit/assurance team, other assurance teams and the enterprise is essential.									
1.2.1 Identify the drivers for a successful review. (This should exist in the assurance function's standards and procedures.)									
1.2.2 Communicate success attributes to the process owner or stakeholder, and obtain agreement.									
1.3 Define the boundaries of the review. The review must have a defined scope. Understand the functions and application requirements for the VoIP servers within the scope.									
1.3.1 Obtain a list of VoIP servers and, for each, the relevant manufacturer, supplier and software versions.									
1.3.2 Identify the criteria for selecting VoIP servers for inclusion or exclusion in the current audit/review.									
1.4 Identify and document audit risk. The risk assessment is necessary to evaluate where audit resources should be focused. In most enterprises, audit resources are not available for all processes. The risk-based approach assures utilization of audit resources in the most effective manner.									
1.4.1 Identify the business risk associated with the use of VoIP under consideration for audit/review.									

BANKING & FINANCE INDUSTRY VOIP STANDARDS

ISACA VoIP Audit/Assurance Program

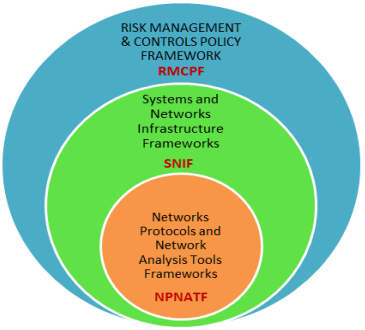
Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
3.2.2.1.4 Review the VoIP policies and standards document, and review it as noted in the following steps.									
3.2.2.1.4.1 Architecture standards include the points indicated in the following steps.									
3.2.2.1.4.1.1 All VoIP phones must be on a virtual LAN (VLAN) separate from any data VLAN and must use RFC 1918 nonroutable addresses.[3]									
3.2.2.1.4.1.2 Voice LANs and VLANs must be firewalled off from any data VLANs/LANs.									
3.2.2.1.4.1.3 Appropriate mechanisms, such as access control lists (ACLs), are required to prevent any communication across VLANs.									
3.2.2.1.4.1.4 Review the ACLs to ensure they provide the appropriate isolation between VoIP VLAN and data/other VLANs.									
3.2.2.1.4.1.5 Connections from VoIP components to the Internet are expressly forbidden.									
3.2.2.1.4.1.6 In the case of any exceptions to the above policy, determine that the risk has been documented and appropriate countermeasures implemented (e.g., additional VoIP-aware firewalls).									
3.2.2.1.4.1.7 If telecommuters are permitted to access the VoIP PBX over the Internet, they must enter via an encrypted VPN tunnel with strong user authentication.									
3.2.2.1.4.1.8 An intrusion detection system (IDS) or intrusion prevention system (IPS) is deployed to protect									

BANKING & FINANCE INDUSTRY VOIP STANDARDS

ISACA VoIP Audit/Assurance Program

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
against external Denial of Service (DoS) attacks.									
3.2.2.1.4.1.9 VoIP-enabled phones must authenticate when connecting to the PBX by a challenge-response process.									
3.2.2.1.4.1.10 In a high-security environment, VoIP phones must be encrypted to deter internal attacks (e.g., where a "rogue" PC is connected to a VoIP network to intercept voice packets.)[4]									
3.2.2.1.4.1.11 If encryption is deployed, it must be enforced to/from all phones and between the gateway and the external PSTN.									
3.2.2.1.4.1.12 If encryption is deployed, an industry-standard encryption algorithm such as AES or 3DES, is required. No proprietary algorithms, vendor-supplied or otherwise should ever be used, due to their unknown effectiveness.									
3.2.2.1.4.1.13 If wireless connectivity is deployed (i.e., to/from cell phones), a strong encryption protocol, such as WPA2, is used, not WEP or other weak encryption.									
3.2.2.1.4.1.14 In a regulated environment, Skype is not permitted due to the ease of user impersonation and lack of HTTPS (encryption) protection.									
3.2.2.1.4.1.15 Where feasible, the option of MAC-binding should be implemented to ensure no unauthorized devices connect to the VoIP VLAN.									
3.2.2.1.4.2 Operations									
3.2.2.1.4.2.1 Verify that all VoIP-related administrative									

PROPOSED RISK MANAGEMENT FRAMEWORK

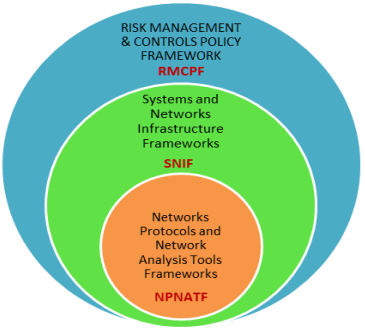


Given above context of risk management, controls, and compliance frameworks, compliance can benefit from adapting the proposed framework to institution's specific needs.

Integration across the 3 levels of vulnerability analysis and penetration testing embedded within overall systems and networks controls and overarching risk management frameworks can facilitate such context-sensitive adaptation.

e.g. From perspective of the ISACA framework, vulnerability assessment and penetration testing can be embedded within IT audit framework of assessment of adequacy of internal controls for effective risk management and compliance.

PROPOSED RISK MANAGEMENT FRAMEWORK

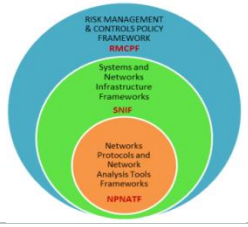


By adopting and integrating the 3 levels of specific frameworks discussed herein, a financial institution can develop, maintain, improve, and sustain its enterprise risk management and compliance frameworks.

The proposed risk management framework identifies 3 levels for bridging the gaps in industry frameworks of prudent risk management and information assurance.

Context-sensitive adaptation can be enabled by integration across vulnerability analysis and penetration testing embedded within overall systems and networks controls framework and risk management frameworks.

Keywords: *Cyber Risk Management, Cybersecurity and Penetration Testing, Computer Science Curricula, Professional Standards of Practice, Networks Protocols and Network Analysis, Systems and Networks Infrastructure, Risk Management & Controls Policy, Access to Technologies and Innovations, Innovative design and development Practices, Technology Innovations Impacting Engineering and Engineering Technology Education, STEM Education Developments.*



TOWARD INTEGRATED ENTERPRISE RISK MANAGEMENT, MODEL RISK MANAGEMENT, & CYBER-FINANCE RISK MANAGEMENT:

BRIDGING NETWORKS, SYSTEMS, AND, CONTROLS FRAMEWORKS FOR CYBERSECURITY CURRICULA & STANDARDS DEVELOPMENT

Yogi

Dr. Yogesh Malhotra

PhD, MSQF, MSCS, MSNCS, MSAcc, MBAEco, BE,
C.Eng., CCP/CDP, CISSP, CISA, CEH
Who's Who in America®, Who's Who in the World®,
Who's Who in Finance & Industry®,Who's Who in Science & Engineering®
Founder & Chief Research Scientist,
Global Risk Management Network, LLC

www.yogeshmalhotra.com dr.yogesh.malhotra@gmail.com

2015 NY Cyber Security & Engineering Technology Association Conference, Oct. 22, 2015
Rochester Institute of Technology, Rosica Hall, NTID, Rochester, New York