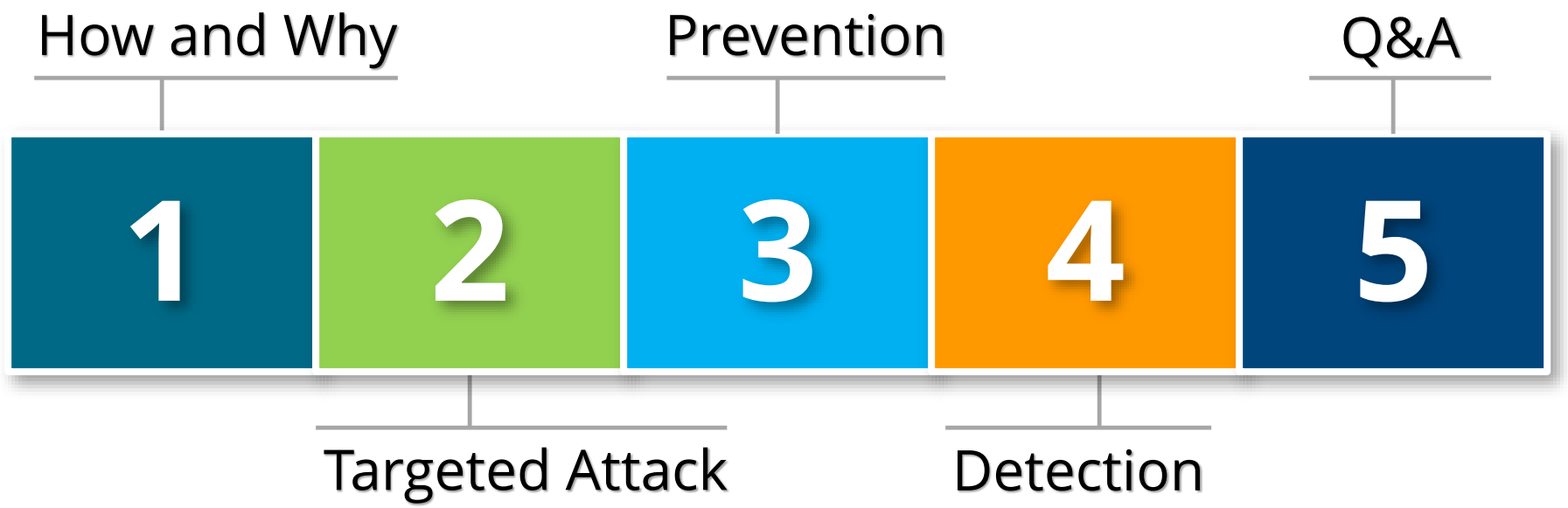
Detecting and Stopping Cyber Attacks against Oracle Databases

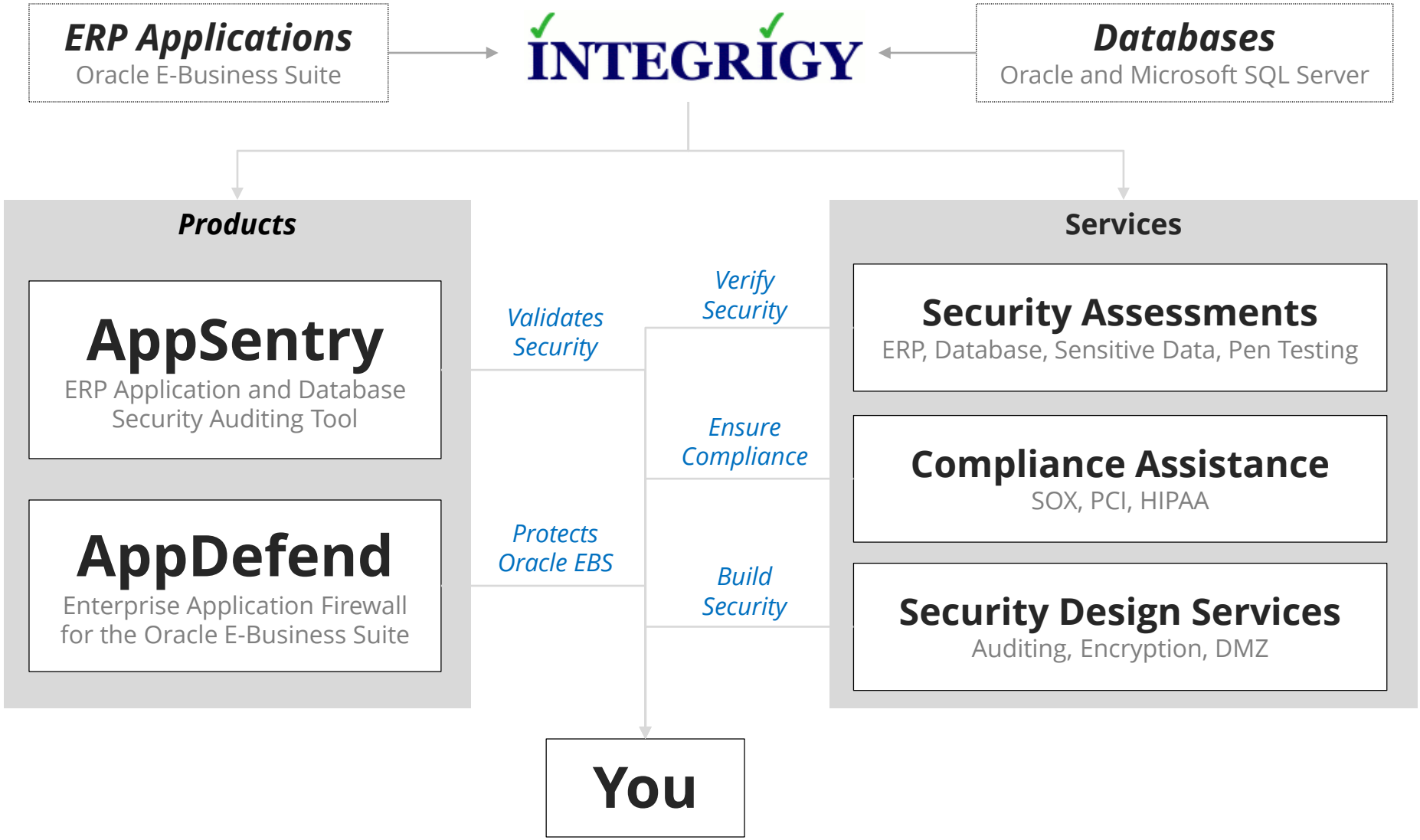
Oracle OpenWorld 2015

Stephen Kost
Chief Technology Officer
Integrigy Corporation

Agenda



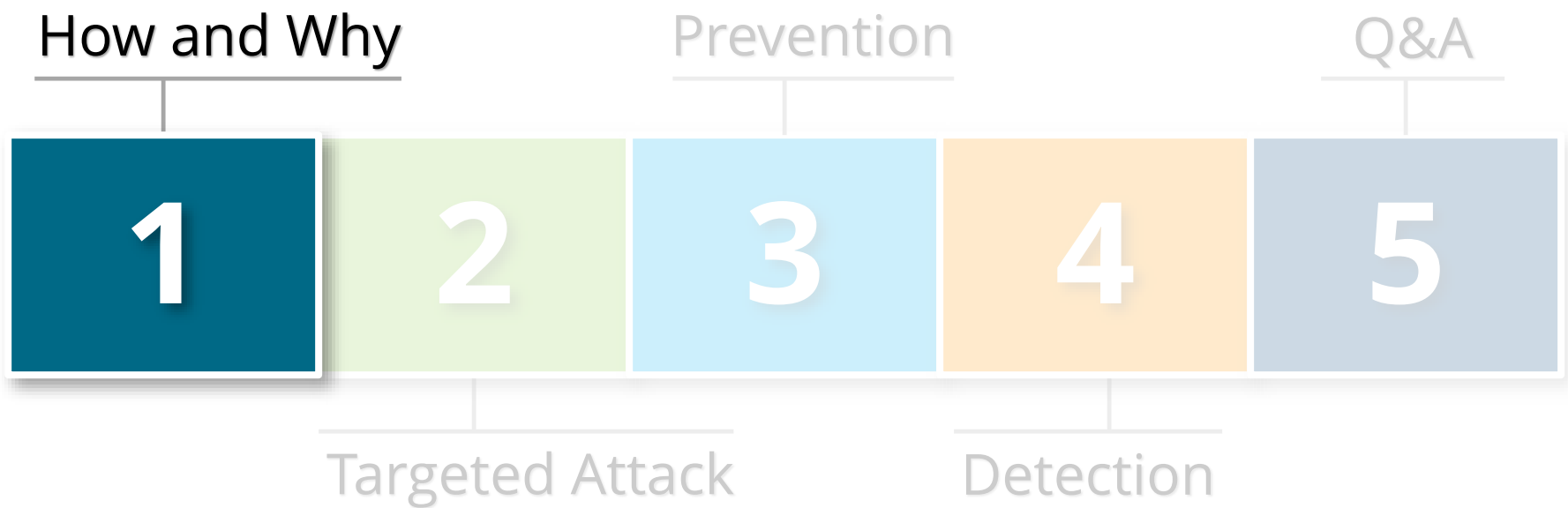
About Integrigy



Integrigy Published Security Alerts

Security Alert	Versions	Security Vulnerabilities
Critical Patch Update April 2012	11.5.10 – 12.1.x	▪ Oracle E-Business Suite security architecture issue
Critical Patch Update July 2011	11.5.10 – 12.1.x	▪ Oracle E-Business Suite security configuration issue
Critical Patch Update October 2010	11.5.10 – 12.1.x	▪ 2 Oracle E-Business Suite security weaknesses
Critical Patch Update July 2008	Oracle 11g 11.5.8 – 12.0.x	▪ 2 Issues in Oracle RDBMS Authentication ▪ 2 Oracle E-Business Suite vulnerabilities
Critical Patch Update April 2008	12.0.x 11.5.7 – 11.5.10	▪ 8 vulnerabilities, SQL injection, XSS, information disclosure, etc.
Critical Patch Update July 2007	12.0.x 11.5.1 – 11.5.10	▪ 11 vulnerabilities, SQL injection, XSS, information disclosure, etc.
Critical Patch Update October 2005	11.0.x, 11.5.1 – 11.5.10	▪ Default configuration issues
Critical Patch Update July 2005	11.0.x, 11.5.1 – 11.5.10	▪ SQL injection vulnerabilities and Information disclosure
Critical Patch Update April 2005	11.0.x, 11.5.1 – 11.5.10	▪ SQL injection vulnerabilities and Information disclosure
Critical Patch Update Jan 2005	11.0.x, 11.5.1 – 11.5.10	▪ SQL injection vulnerabilities
Oracle Security Alert #68	Oracle 8i, 9i, 10g	▪ Buffer overflows ▪ Listener information leakage
Oracle Security Alert #67	11.0.x, 11.5.1 – 11.5.8	▪ 10 SQL injection vulnerabilities
Oracle Security Alert #56	11.0.x, 11.5.1 – 11.5.8	▪ Buffer overflow in FNDWRR.exe
Oracle Security Alert #55	11.5.1 – 11.5.8	▪ Multiple vulnerabilities in AOL/J Setup Test ▪ Obtain sensitive information (valid session)
Oracle Security Alert #53	10.7, 11.0.x 11.5.1 – 11.5.8	▪ No authentication in FNDFS program ▪ Retrieve any file from O/S

Agenda



Targeted Attack

Targeted Attack

Advanced Persistent Threat (APT)

Organized Crime

State Sponsored

Anonymous, LulzSec, Legion of Doom, ...

What are they after?

Credit Card Fraud
 	
Credit Card Data
	▪ Credit Card Number
	  ▪ *Primary Account Number (PAN)*
	▪ CVV/CV2/CID
	  ▪ *3 digits on the back for Visa/MC*
	  ▪ *4 digits on the front for AMEX*
	▪ Magnetic Stripe Data

Identify Theft/Tax Fraud
 	
Personally Identifiable Information (PII)
	▪ First and last name
	▪ Date of Birth
	▪ Plus one of the following:
	  ▪ **Social security number**
	  ▪ Bank account number
	  ▪ Financial account number
	  ▪ Driver license or state ID number

Health Insurance Fraud
 	
Health Information
	▪ First and last name
	▪ Plus one of the following (Protected Health Information)
	  ▪ "the past, present, or future physical or mental health, or condition of an individual"
	  ▪ "provision of health care to an individual"
	  ▪ "payment for the provision of health care to an individual"

In 2013, the health care industry accounted for 44% of all breaches

- Identity Theft Resource Center

What is your data worth? Credit Cards

Credit Card Price	*Black Market Classification*
$20 – $45	**Freshly acquired**
$10 – $12	**Flooded**
$2 – $7	**Clearance (“stale” data)**

Source: Krebs on Security

What is your data worth? Identify Theft

$1 – $5	▪ First and last name ▪ Social Security number	**Tax information (e.g., 1099)**
$20 – $40	▪ First and last name ▪ Social Security number ▪ Current address ▪ Date of birth	**Human Resources** **Health care**
$30 – $100	▪ First and last name ▪ Social Security number ▪ Current address ▪ Date of birth ▪ Bank account number or credit card number ▪ Salary	**Payroll**

- **FY 2013 – 1 million fraudulent tax returns**
- **FY 2013 – $5.8 billion in fraudulent tax refunds**
- **Identity Protection PIN not available until Tax Year 2017**

- General Accounting Office (GAO) Report

Identity Protection PIN – If you live in DC, Florida, or Georgia – GET ONE NOW!

Database Valuation

Calculate the black market value of the data contained in your database to help evaluate risk.

Data Type	*Formula*
Credit Cards	**(number of unique, unexpired cards) * $10**
Social Security Numbers	**(number of unique SSN + Name + DoB) * $20** **or (number of unique SSN + Bank) * $50**

Agenda

Methods of Database Compromise

Direct	▪ Direct compromise of the database through direct database access ▪ Obtain credentials to the database and escalate privileges
Indirect	▪ Compromise is through an application, ancillary system, or operating system ▪ Application and ancillary system compromise most often will be SQL injection ▪ Operating system typically is theft of database files

Anatomy of the Targeted Attack

1 **Point of Entry**	Breach the perimeter network through a network compromise, phishing attack, or social engineering.
2 **Persistence**	Once inside, establish a “beach-head” and maintain the compromise over time (days, months, years).
3 **Lateral Movement**	Expand the compromise to more devices and systems.
4 **Asset and Data Discovery**	The **Targeted Attack** has already identified “data of interest” and will being searching for it. *How to do this without detection?*
5 **Data Exfiltration**	Once the “data of interest” has been gathered, it must be **transferred externally** without being detected. *How do you quietly steal gigabytes or terabytes of data?*

Asset (Database) Discovery Techniques

Passive	▪ Search internal knowledge repositories for architecture diagrams, design documents, code repositories, etc. ▪ Find TNSNAMES.ORA files
Active	▪ Compromise DBA credentials through phishing or social engineering attacks ▪ Install malware on DBA machines and steal credentials, such as saved in SQL Developer ▪ Use Nmap to scan internal network for Oracle Databases on default port 1521 – very noisy

Demo – Search for TNSNAMES.ORA Files

Findings tnsnames.ora files using **internal** search engines or wiki's

www.google.com

```
search: tnsnames filetype:ora site:.edu
```

Demo – Search Source Code

Obtaining passwords from
internal source code repositories

www.github.com

`search: “alter user” “identified by”`

Demo – Decrypt SQL Developer Passwords

Decrypt SQL Developer passwords

`https://github.com/tomecode/show-me-password-sqldev-jdev`

Use extension in SQL Developer

Demo – Scan for Databases on Port 1521

Using Nmap to find Oracle databases

www.nmap.com

```
nmap -sT -sV -p 1521-1529 -T4 -v -n -Pn -open 192.168.2.11-50
```

Demo – Brute Force SID

Using Nmap to brute force SID

www.nmap.com

```
nmap -p 1521 -v --script oracle-sid-brute 192.168.56.10
```

Detect Brute Force SID – listener.log

```
<msg time='2015-04-13T10:28:44.192-04:00' org_id='oracle' comp_id='tnslsnr'
 type='UNKNOWN' level='16' host_id='testdb'
 host_addr='127.0.0.1'>
 <txt>13-APR-2015 10:28:44 *
(CONNECT_DATA=(SID=ORCL1)(CID=(PROGRAM=)(HOST=__jdbc__)(USER=))) *
(ADDRESS=(PROTOCOL=tcp)(HOST=192.168.56.1)(PORT=17927)) * establish * ORCL1 *
12505
 </txt>
</msg>
<msg time='2015-04-13T10:28:44.192-04:00' org_id='oracle' comp_id='tnslsnr'
 type='UNKNOWN' level='16' host_id='testdb'
 host_addr='127.0.0.1'>
 <txt>TNS-12505: TNS:listener does not currently know of SID given in connect
descriptor
 </txt>
</msg>
```

Default Oracle Password Statistics

Database Account	Default Password	Exists in Database %	Default Password %
SYS	CHANGE_ON_INSTALL	100%	3%
SYSTEM	MANAGER	100%	4%
DBSNMP	**DBSNMP**	**99%**	**52%**
OUTLN	**OUTLN**	**98%**	**43%**
MDSYS	MDSYS	77%	18%
ORDPLUGINS	ORDPLUGINS	77%	16%
ORDSYS	ORDSYS	77%	16%
XDB	CHANGE_ON_INSTALL	75%	15%
DIP	DIP	63%	19%
WMSYS	WMSYS	63%	12%
CTXSYS	**CTXSYS**	**54%**	**32%**

* Sample of 120 production databases

Demo

Brute forcing Oracle Database Passwords

Integrigy internal tool

google: `oracle password cracker`

`free tools: woraauthbf, orabf`

Demo

Using Nmap for Database Password Guessing

www.nmap.com

```
nmap -p 1521 -v --script oracle-brute
--script-args oracle-brute.sid=ORCL 192.168.56.10
```

Detect Password Brute Force – Database Audit Trail

OS_USERNAME	USERNAME	USERHOST	TIMESTAMP	ACTION	ACTION_NAME	RETURNCODE
nmap_22032	ZX	nmap_target	25-OCT-15	100	LOGON	1017
nmap_18405	ZSA	nmap_target	25-OCT-15	100	LOGON	1017
nmap_20933	ZPB	nmap_target	25-OCT-15	100	LOGON	1017
nmap_16072	ZFA	nmap_target	25-OCT-15	100	LOGON	1017
nmap_3103	XTR	nmap_target	25-OCT-15	100	LOGON	1017
nmap_8908	YCAMPOS	nmap_target	25-OCT-15	100	LOGON	1017
nmap_26995	XNS	nmap_target	25-OCT-15	100	LOGON	1017
nmap_17004	YSANCHEZ	nmap_target	25-OCT-15	100	LOGON	28000
nmap_16306	XNM	nmap_target	25-OCT-15	100	LOGON	1017
nmap_24233	XNP	nmap_target	25-OCT-15	100	LOGON	1017
nmap_11503	SYSMAN	nmap_target	25-OCT-15	100	LOGON	1017
nmap_8458	XNI	nmap_target	25-OCT-15	100	LOGON	1017
nmap_11510	XNB	nmap_target	25-OCT-15	100	LOGON	1017
nmap_23924	XNC	nmap_target	25-OCT-15	100	LOGON	1017
nmap_10518	XLE	nmap_target	25-OCT-15	100	LOGON	1017
nmap_23234	XDO	nmap_target	25-OCT-15	100	LOGON	1017
nmap_23125	XLA	nmap_target	25-OCT-15	100	LOGON	28000

What Do I Need and How Did I Get It?

IP Address	1. Scanning – Nmap 2. TNSNAMES.ORA 3. Internal resources
Port	1. Default port 1521 – Nmap 2. TNSNAMES.ORA 3. Internal resources
SID/Service Name	1. TNSNAMES.ORA 2. Internal resources 3. SID brute force
User Name	1. Default user names (1,000+) 2. Inside the database (all_users) 3. Internal resources
Password	1. Default passwords 2. Password guessing 3. Source code
Privileges	1. Get lucky with an account 2. Missing security patches 3. Application vulnerabilities

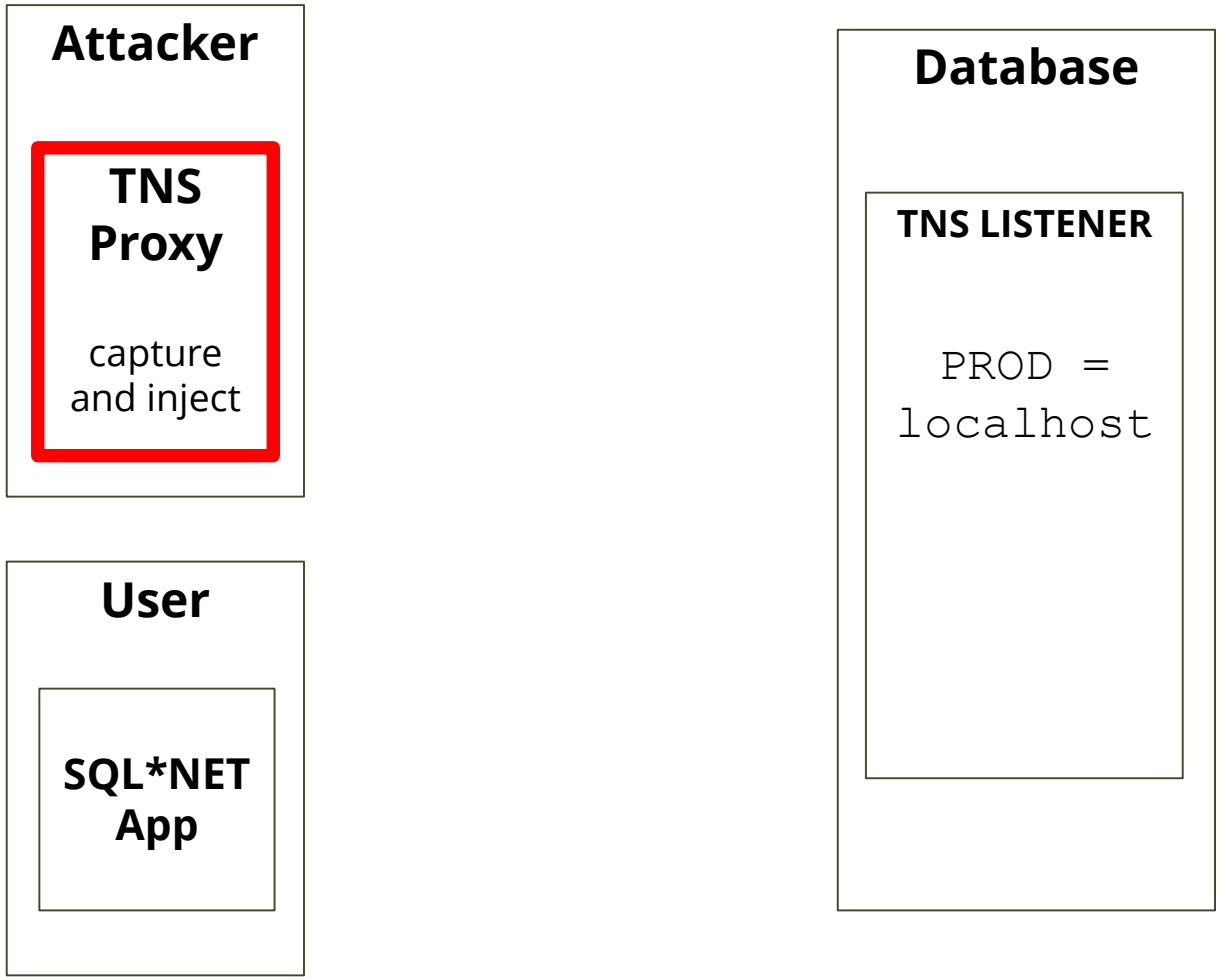
TNS Poisoning Attack – One-off – April 30, 2012

Vuln #	Component	Protocol	Package and/or Privilege Required	Remote Exploit without Auth.?
CVE-2012-1675	**Listener**	**Oracle Net**	**None**	**Yes**

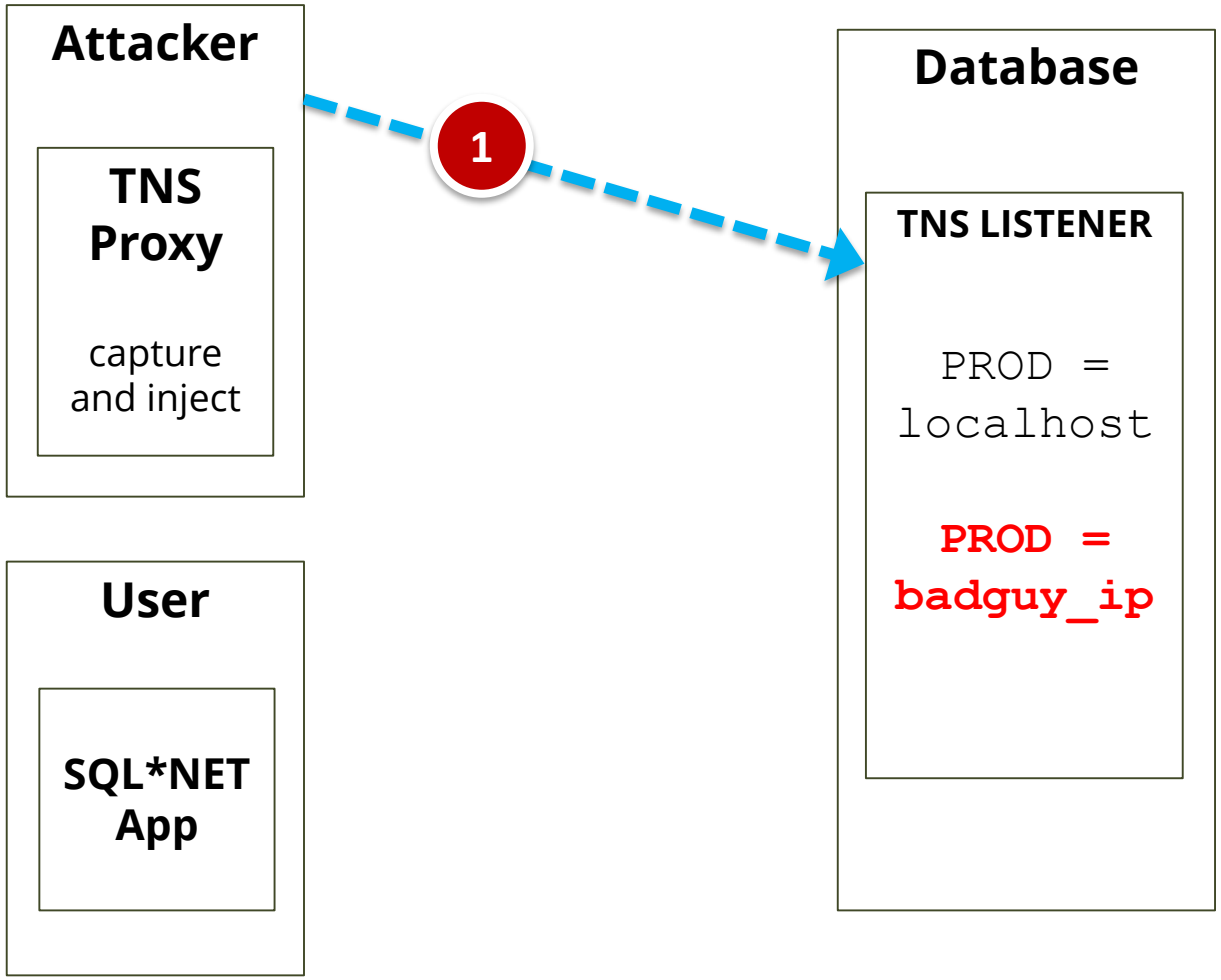
CVSS VERSION 2.0 RISK							Last Affected Patch set (per Supported Release)
Base Score	Access Vector	Access Complexity	Authentication	Confidentiality	Integrity	Availability	
7.5	**Network**	**Low**	**None**	**Partial+**	**Partial+**	**Partial**	**ALL VERSIONS**

- **This vulnerability is not patched by a SPU or PSU.** The TNS Listener configuration must be secured.
- **ALL VERSIONS** of the Oracle Database are affected.
- 12c and 11.2.0.4 protected by default, but vulnerable when Valid Node Checking Registration (VNCR) is disabled.

TNS Poisoning Attack Illustrated

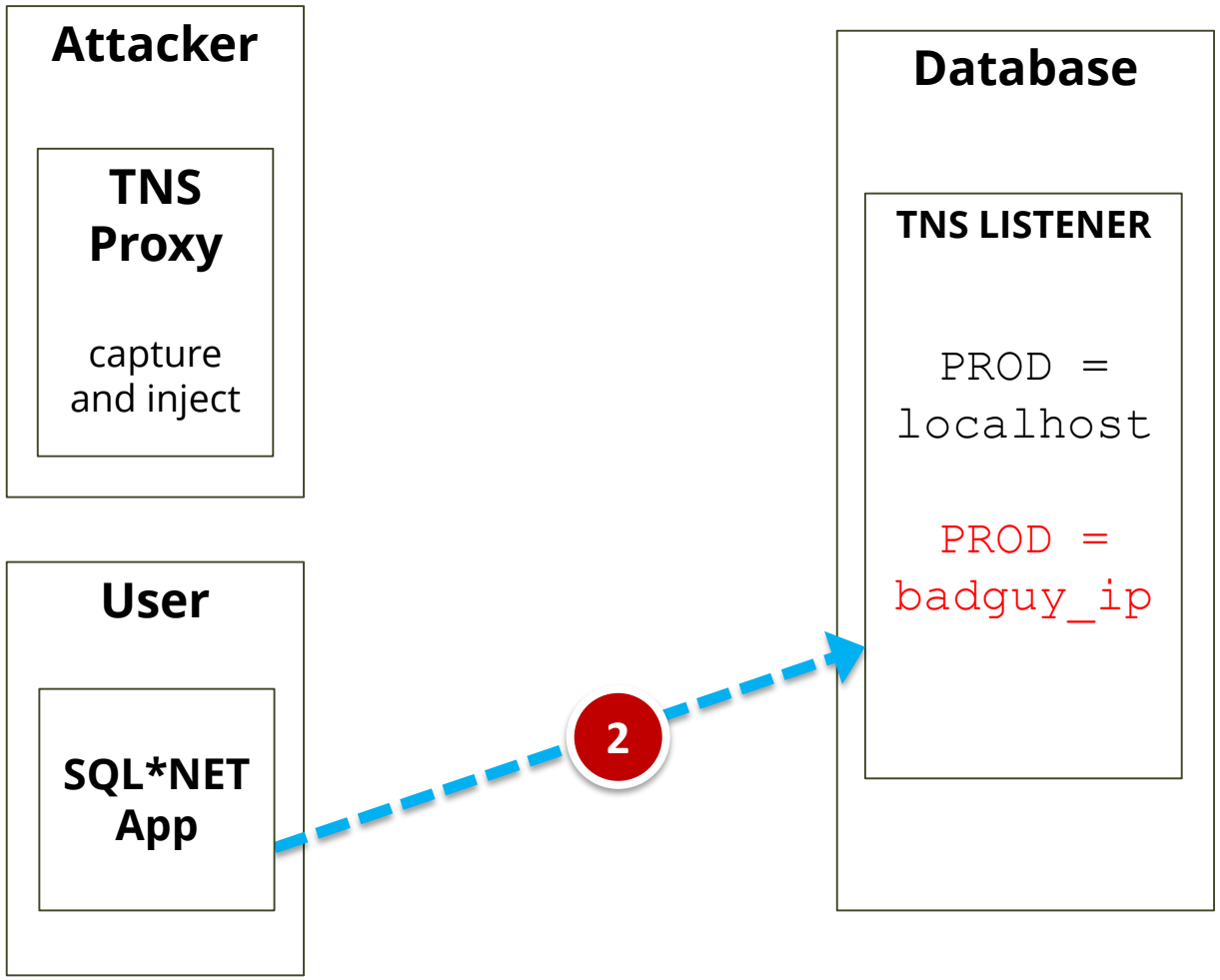


TNS Poisoning Attack Illustrated



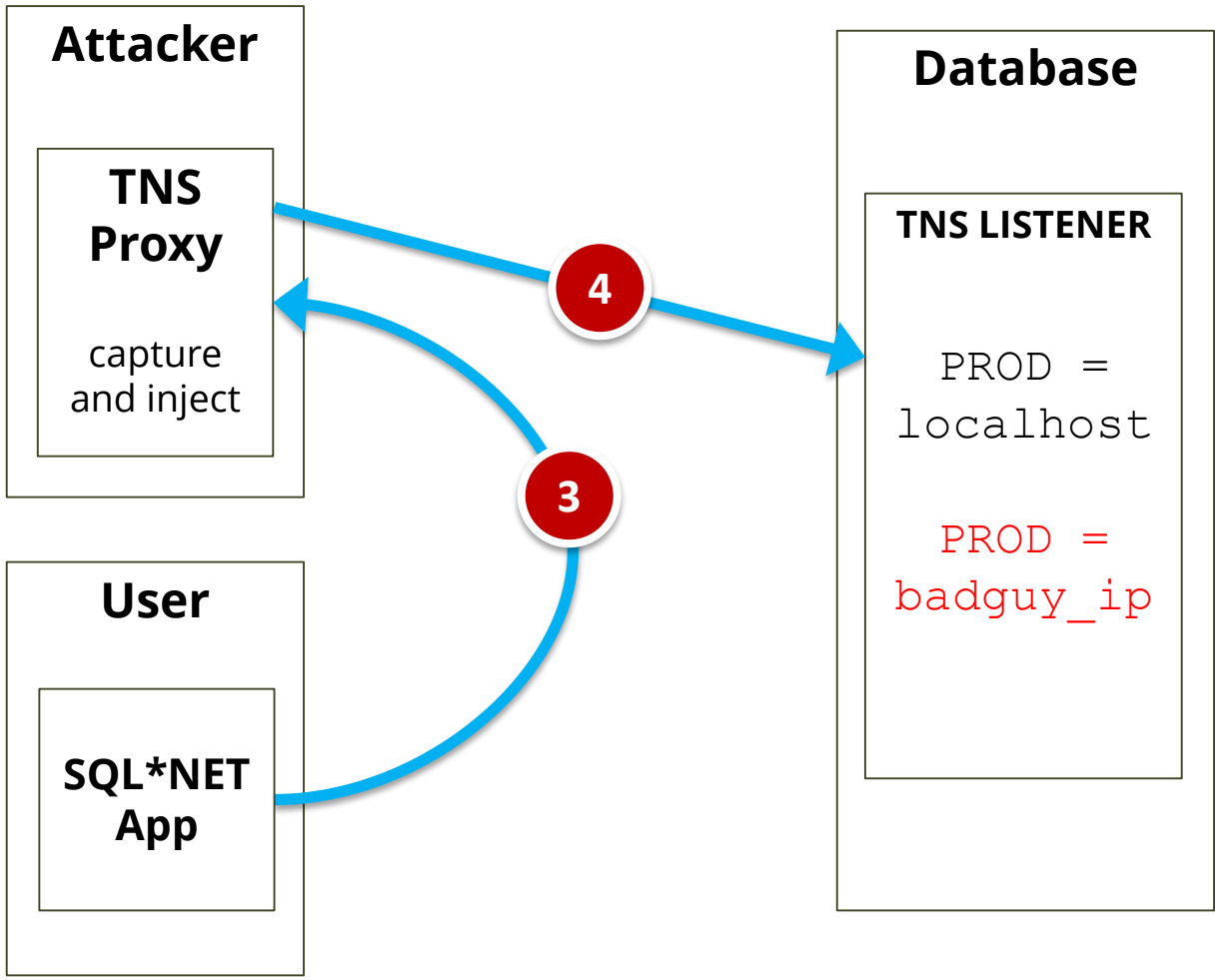
1 Attacker dynamically registers Service with database.

TNS Poisoning Attack Illustrated



2 User connects and is “Load Balanced” to attacker.

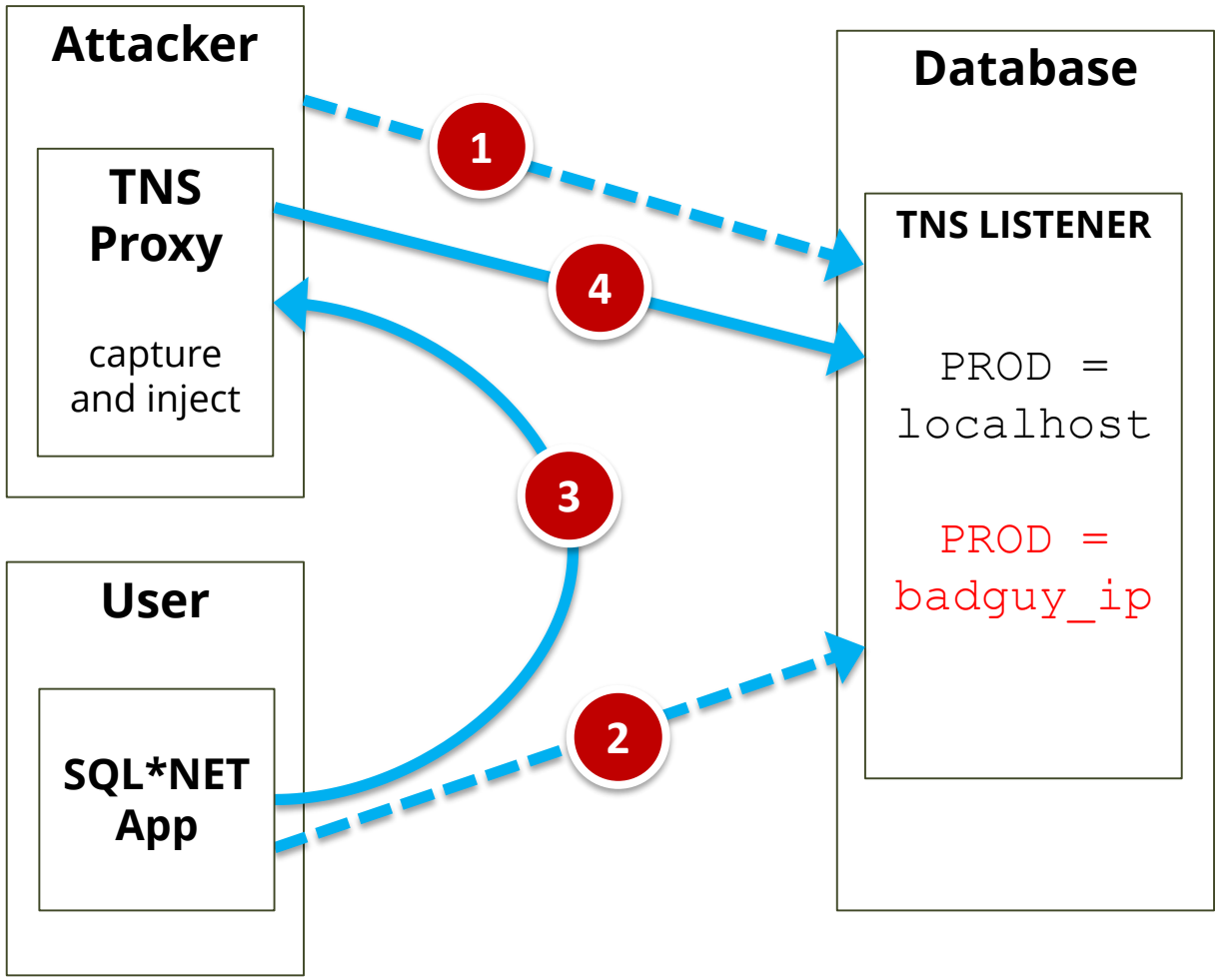
TNS Poisoning Attack Illustrated



3 User connect to attacker rather than database.

4 Attacker forwards to database.

TNS Poisoning Attack Illustrated



1. Attacker dynamically registers Service with database.
2. User connects and is “Load Balanced” to attacker.
3. User connect to attacker rather than database.
4. Attacker forwards to database.

TNS Poisoning Mitigation

Database Version	***SSL Encrypt with Cert***	***COST*** *class of secure transport*	***VNCR*** *Valid node checking registration*
References	See ASO	1453883.1 1340831.1 (RAC)	1600630.1
8.1.7.x – 10.2.0.3	✓		
10.2.0.3 – 10.2.0.5	✓	✓	
11.1.0.x	✓	✓	
11.2.0.1 – 11.2.0.3	✓	✓	
11.2.0.4*	✓	✓	✓ (Enabled by default)
12.1.0.x*	✓	✓	✓ (Enabled by default)

* 11.2.0.4 and 12c does not allow remote registration by default.

Demo

TNS Poisoning Attack

http://joxeankoret.com/research.html

Exploit Information

- **Joxean Koret**
  - http://joxeankoret.com/research.html
  - Oracle TNS Poison un-auth proof on concept (Oracle 9i, 10g and 11g)
- **tnspoisonv1.py**
  - Used to poison the remote database listener
- **proxy.py**
  - Proxy on attacker machine to accept client connections and forward to database server

Stealth Password Cracking Bug – October 2012

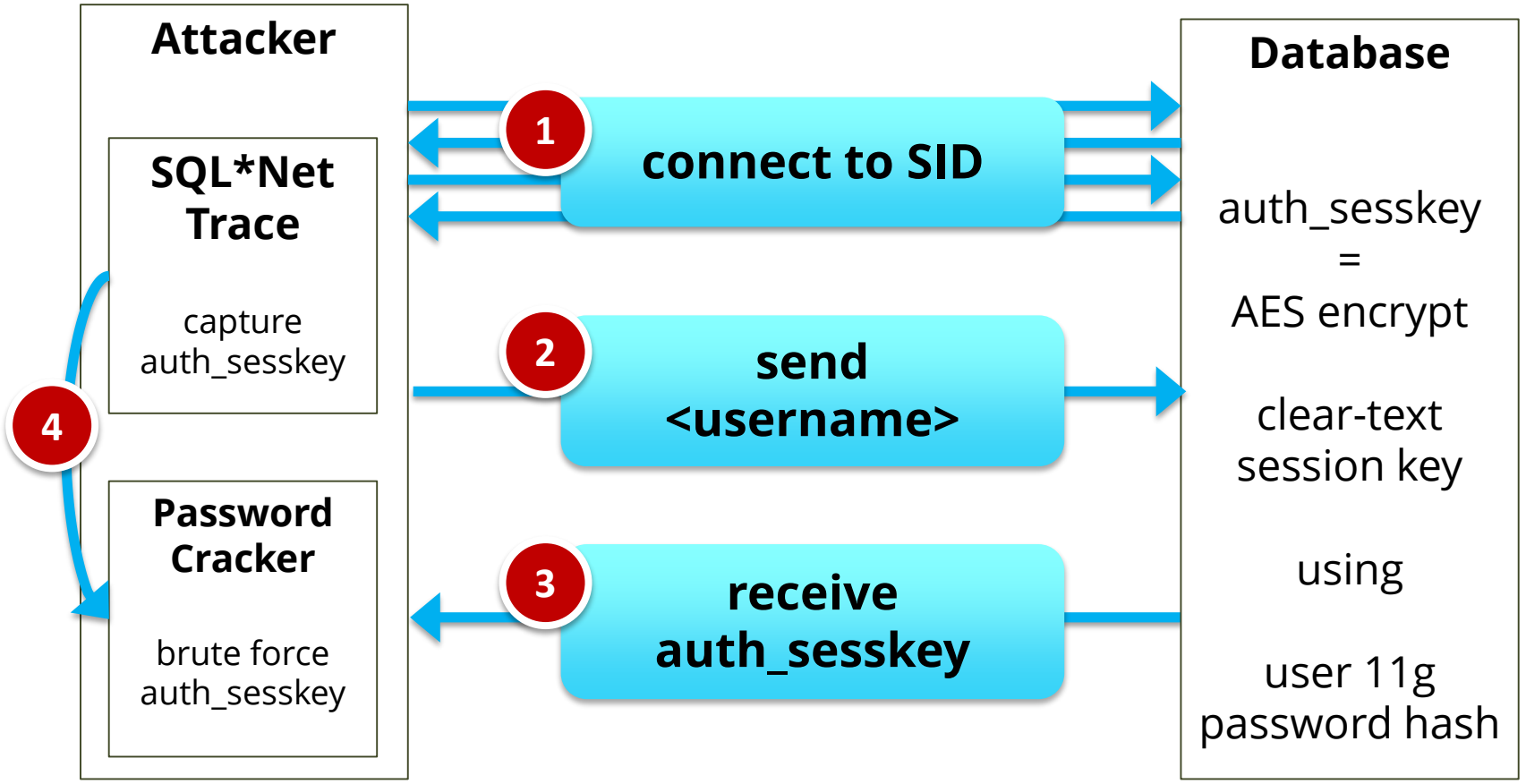
Vuln #	Component	Protocol	Package and/or Privilege Required	Remote Exploit without Auth.?
CVE-2012-3137	**Oracle RDBMS**	**Oracle Net**	**None**	**Yes**

CVSS VERSION 2.0 RISK							Last Affected Patch set (per Supported Release)
Base Score	Access Vector	Access Complexity	Authentication	Confidentiality	Integrity	Availability	
10.0	**Network**	**Low**	**None**	**Complete**	**Complete**	**Complete**	**11.1.0.x 11.2.0.1 11.2.0.2 11.2.0.3**

Vulnerable if using "11G" passwords (see USER$). 10.2.0.x is also vulnerable if using Enterprise User Security (EUS) with an SHA-1 password verifier.

Stealth Password Attack Illustrated

Flaw in the 11g O5Logon protocol allows for brute forcing of the password using the authsess_key.



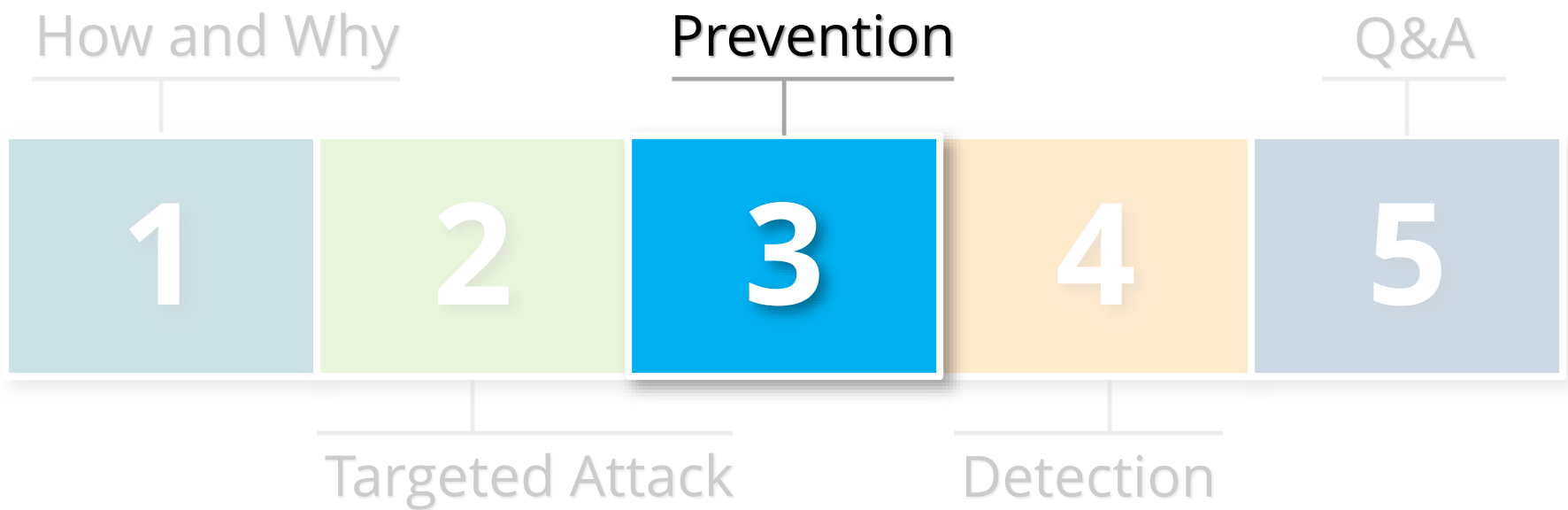
Exploit Information

- **SQL*Net Trace on client**
  - Capture SQL*Net connection and auth_sesskey
  - TRACE_LEVEL_CLIENT = SUPPORT
- **nmap**
  - Legendary network scanning tool
  - oracle-brute-stealth script
  - Retrieves auth_sesskey for selected users
- **John the Ripper**
  - Legendary password cracking tool
  - Use o5logon

Commonly Used Oracle Attack Tools

- **Metasploit – Oracle Modules**
  - SID brute force, password guessing, privilege escalation modules
- **Nmap**
  - network scanning, SID brute force, password guessing modules
- **ODAT (Oracle Database Attack Tool)**
  - SID brute force, password guessing, privilege escalation features

Agenda



Integrigy's #1 Security Recommendation

- **Limit direct database access whenever possible**
  - Much harder to hack database if an attacker can not connect to it – **can't connect, can't hack it**
  - Would have to use another avenue such as a web application or reporting tool (e.g., OBIEE)

- **Use firewalls in front of data center, network ACLs, TNS invited nodes, Oracle Connection Manager, Oracle Database Firewall, etc.**
  - DBAs should use bastion hosts to manage databases

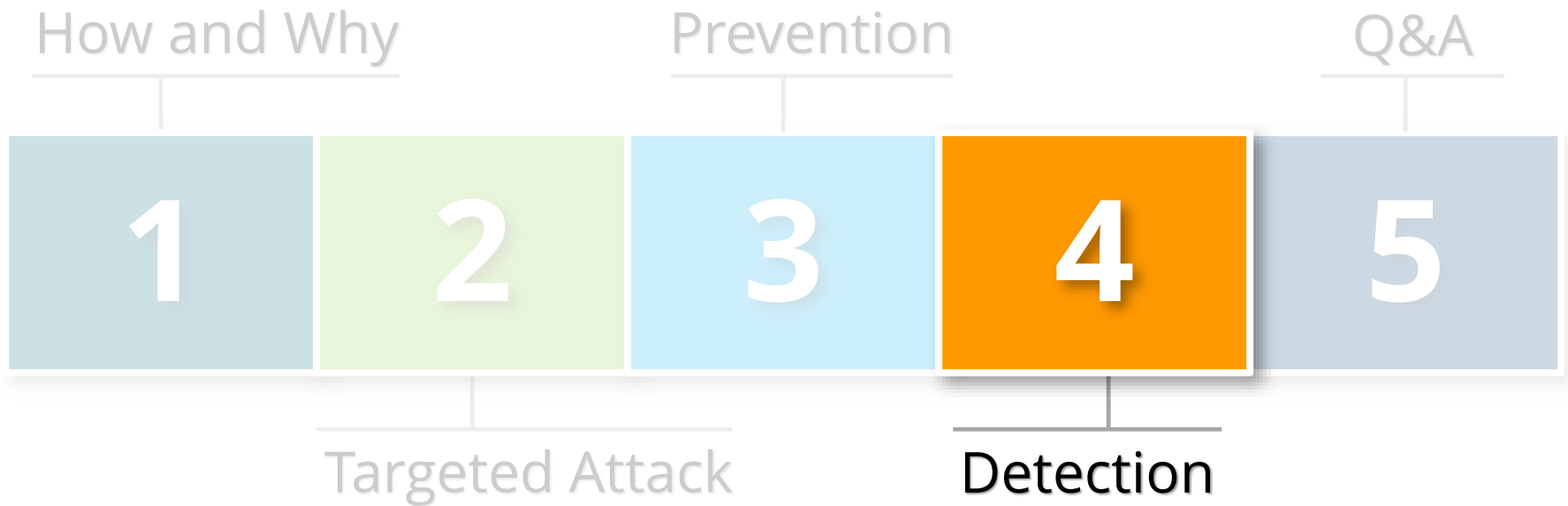
Database Security Preventative Controls

- **Check for default and weak passwords constantly**
  - Use multiple tools to check passwords
  - Install database profiles to enforce strong passwords
- **Harden database configurations**
  - Develop comprehensive database security standard
  - Validate configurations on regular basis
- **Apply Oracle Critical Patch Updates on a regular basis on all databases**
  - Reduce risk of compromise and escalation of privileges

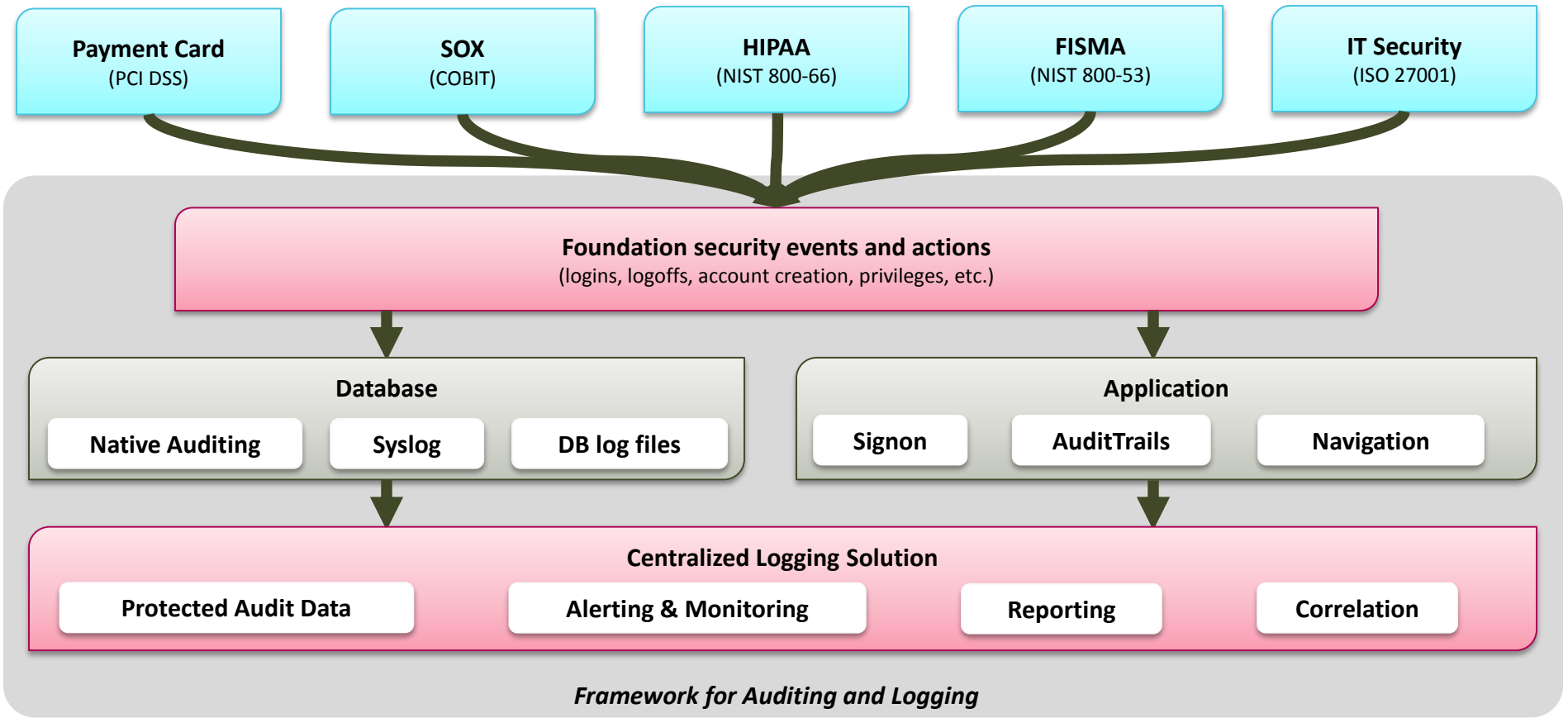
How to Check Database Passwords

- **Use Oracle's DBA_USERS_WITH_DEFPWD**
  - **Limited set of accounts**
  - **Single password** for each account
- **Command line tools (orabf, etc.)**
  - Command line only – not easy to use
- **Integrigy AppSentry**
  1. Checks all database accounts
  2. Uses passwords lists - > 1 million passwords
  3. Allows custom passwords

Agenda



Framework for Auditing and Logging



Framework for Auditing and Logging

Foundation Security Events and Actions

The foundation of the framework is a set of key security events and actions derived from and mapped to compliance and security requirements that are critical for all organizations.

E1 - **Login**	*E8* - **Modify role**
E2 - **Logoff**	*E9* - **Grant/revoke user privileges**
E3 - **Unsuccessful login**	*E10* - **Grant/revoke role privileges**
E4 - **Modify auth mechanisms**	*E11* - **Privileged commands**
E5 - **Create user account**	*E12* - **Modify audit and logging**
E6 - **Modify user account**	*E13* - **Create, Modify or Delete object**
E7 - **Create role**	*E14* - **Modify configuration settings**

Foundation Security Events Mapping

Security Events and Actions	PCI DSS 10.2	SOX (COBIT)	HIPAA (NIST 800-66)	IT Security (ISO 27001)	FISMA (NIST 800-53)
E1 - Login	10.2.5	A12.3	164.312(c)(2)	A 10.10.1	AU-2
E2 - Logoff	10.2.5	DS5.5	164.312(c)(2)	A 10.10.1	AU-2
E3 - Unsuccessful login	10.2.4	DS5.5	164.312(c)(2)	A 10.10.1 A.11.5.1	AC-7
E4 - Modify authentication mechanisms	10.2.5	DS5.5	164.312(c)(2)	A 10.10.1	AU-2
E5 – Create user account	10.2.5	DS5.5	164.312(c)(2)	A 10.10.1	AU-2
E6 - Modify user account	10.2.5	DS5.5	164.312(c)(2)	A 10.10.1	AU-2
E7 - Create role	10.2.5	DS5.5	164.312(c)(2)	A 10.10.1	AU-2
E8 - Modify role	10.2.5	DS5.5	164.312(c)(2)	A 10.10.1	AU-2
E9 - Grant/revoke user privileges	10.2.5	DS5.5	164.312(c)(2)	A 10.10.1	AU-2
E10 - Grant/revoke role privileges	10.2.5	DS5.5	164.312(c)(2)	A 10.10.1	AU-2
E11 - Privileged commands	10.2.2	DS5.5	164.312(c)(2)	A 10.10.1	AU-2
E12 - Modify audit and logging	10.2.6	DS5.5	164.312(c)(2)	A 10.10.1	AU-2 AU-9
E13 - Objects Create/Modify/Delete	10.2.7	DS5.5	164.312(c)(2)	A 10.10.1	AU-2 AU-14
E14 - Modify configuration settings	10.2.2	DS5.5	164.312(c)(2)	A 10.10.1	AU-2

Foundation Database Logging

Object	Oracle Audit Statement	Resulting Audited SQL Statements
Session	session	Database logons and failed logons
Users	user	create user alter user drop user
Roles	role	create role alter role drop role
Database Links **Public Database Links**	database link public database link	create database link drop database link create public database link drop public database link
System	alter system	alter system
Database	alter database	alter database
Grants **(system privileges and roles)**	system grant	grant revoke
Profiles	profile	create profile alter profile drop profile
SYSDBA and SYSOPER	sysdba sysoper	All SQL executed with sysdba and sysoper privileges

Detecting Attacks

IP Address	1. Scanning – Nmap 2. TNSNAMES.ORA 3. Internal resources	▪ Network intrusion detection (IDS)
Port	1. Default port 1521 – Nmap 2. TNSNAMES.ORA 3. Internal resources	▪ Network intrusion detection (IDS)
SID	1. TNSNAMES.ORA 2. Internal resources 3. SID brute force	▪ Monitor listener logs for SID and service name errors
User Name	1. Default user names (1,000+) 2. Inside the database (all_users) 3. Internal resources	▪ Alert on any use of standard accounts like CTXSYS ▪ Monitor for logins to locked accounts
Password	1. Default passwords 2. Password guessing 3. Source code	▪ Watch for horizontal and vertical failed password attempts
Privileges	1. Get lucky with an account 2. Missing security patches 3. Application vulnerabilities	▪ Monitor for common security errors ▪ Monitor for security vulnerability exploits

Agenda

Contact Information

Stephen Kost

Chief Technology Officer

Integrigy Corporation

web: **www.integrigy.com**

e-mail: **info@integrigy.com**

blog: **integrigy.com/oracle-security-blog**

youtube: **youtube.com/integrigy**