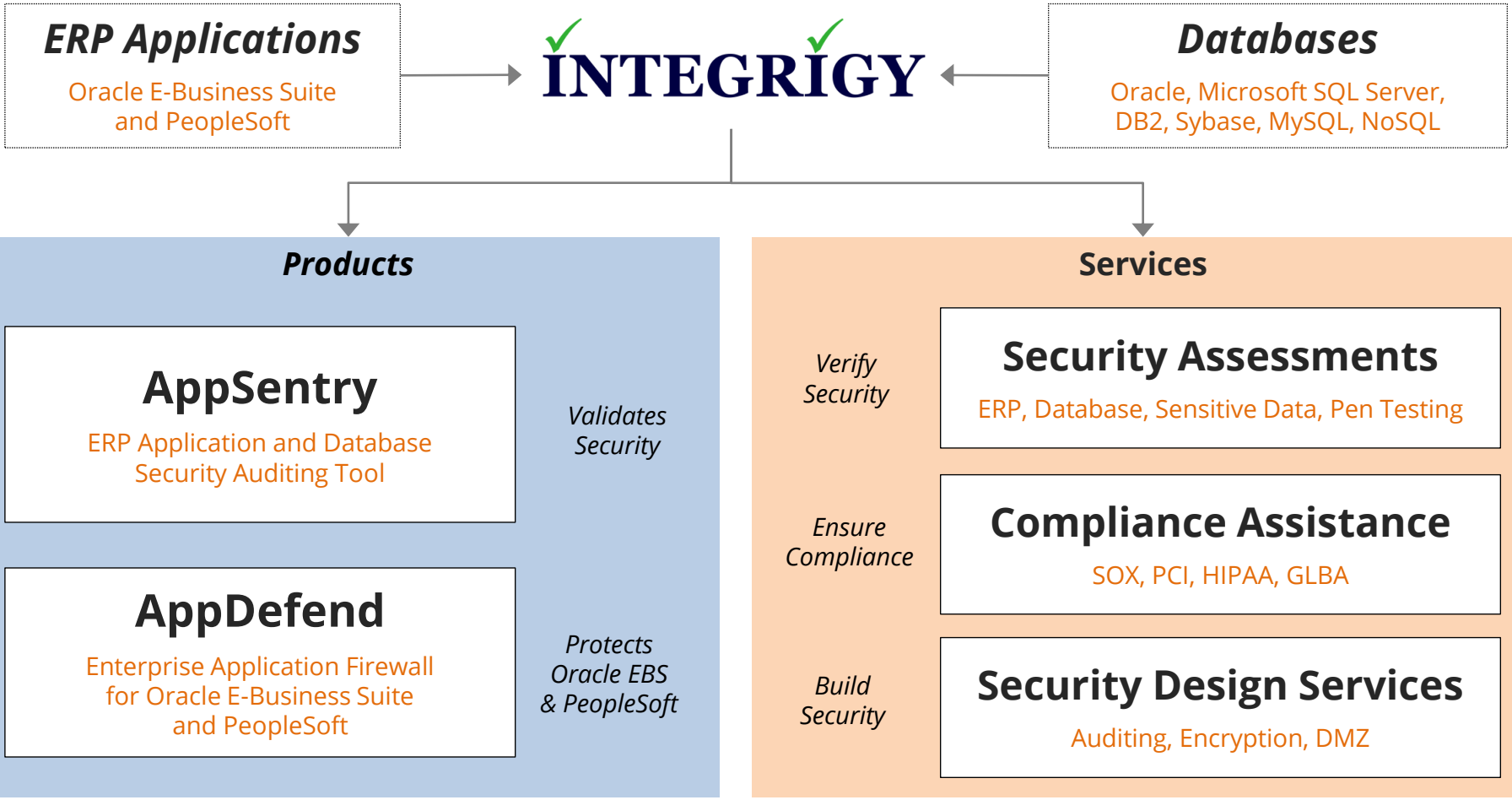
The Tools Hackers Are Using Against Your Oracle Database Webinar

May 6, 2020

Stephen Kost
Chief Technology Officer
Integrigy Corporation

Phil Reimann
Director of Business Development
Integrigy Corporation

About Integrigy



Integrigy Research Team

ERP Application and Database Security Research

ORACLE Gold Partner

Agenda

1. Background
2. Tools and the Attack
3. Prevention
4. Detection
5. Q & A

Agenda

1. Background
2. Tools and the Attack
3. Prevention
4. Detection
5. Q & A

Targeted Attack

Targeted Attack

Advanced Persistent Threat (APT)

State Sponsored

Anonymous, LulzSec, Legion of Doom, ...

Bitcoin/Monero Mining

Sensitive Data in Databases

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 (very rare)

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"

Last three years, the health care industry accounted for 42.5% of all breaches

- Identity Theft Resource Center

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	**Health care** **Human Resources**
$30 – $100	▪ First and last name ▪ Social Security number ▪ Current address ▪ Date of birth ▪ Bank account number or credit card number ▪ Salary	**Payroll**

- **2017 – 1.1 million potentially fraudulent tax returns**
- **2017 – IRS paid $4.4 billion in fraudulent tax refunds**
- **3,000 IRS employees dedicated to tax Fraud**

- General Accounting Office (GAO) Report

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

1. Background
2. Tools and the Attack
3. Prevention
4. Detection
5. Q & A

Oracle Database Attack Tools

Nmap	**nmap.org** ▪ Database discovery, version, SID enumeration/brute force, password guessing, limited exploits
ODAT	**github.com/quentinhardy/odat** ▪ SID enumeration/brute force, password guessing, common exploits, Oracle OS attacks
Metasploit	**www.metasploit.com** ▪ SID enumeration/brute force, password guessing, limited exploits
Hydra	**github.com/vanhauser-thc/thc-hydra** ▪ SID enumeration/brute force, password guessing
Oscanner	**gitlab.com/kalilinux/packages/oscanner (7 years old)** ▪ SID enumeration/brute force, password guessing

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 Discovery**	The **Targeted Attack** has already identified “data of interest” and will being searching for it. *How to discover assets this without detection?*
5 **Asset Compromise**	The database is attacked in order to gain unauthorized access to “data of interest”. *How to compromise asset this without detection?*
6 **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?*

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 Engine (Internal)

- Findings tnsnames.ora files using internal search engines

- www.google.com
- search: `tnsnames filetype:ora`

Demo – Source Code Repositories

Obtaining passwords from internal source code repositories

www.github.com

search: `"alter user" "identified by"`

http://www.github.com

Note: To search all code repositories must be signed into Github with an account (including free accounts).

Demo – Developer Tools – Compromised Desktop

Decrypt SQL Developer passwords

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

Use extension in SQL Developer

Demo – Network Scanning – Find Databases

If the attacker can't find databases through other means, then the old-fashioned way by scanning the network.

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 – Determine the SID if Unknown

To connect to a database need IP address/hostname, TNS port number, and SID/Service Name.

Using Nmap to brute force SID

www.nmap.com

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

Database Compromise – Login into Database

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 – mostly production ERP databases such as SAP, Oracle EBS, and PeopleSoft

Demo – Brute Force Database Accounts

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
```

Demo – Able to Connect and Access USER$

Brute forcing Oracle Database Passwords

Integrigy internal tool

google: `oracle password cracker`

free tools: woraauthbf, orabf

Final Step – Privilege Escalation

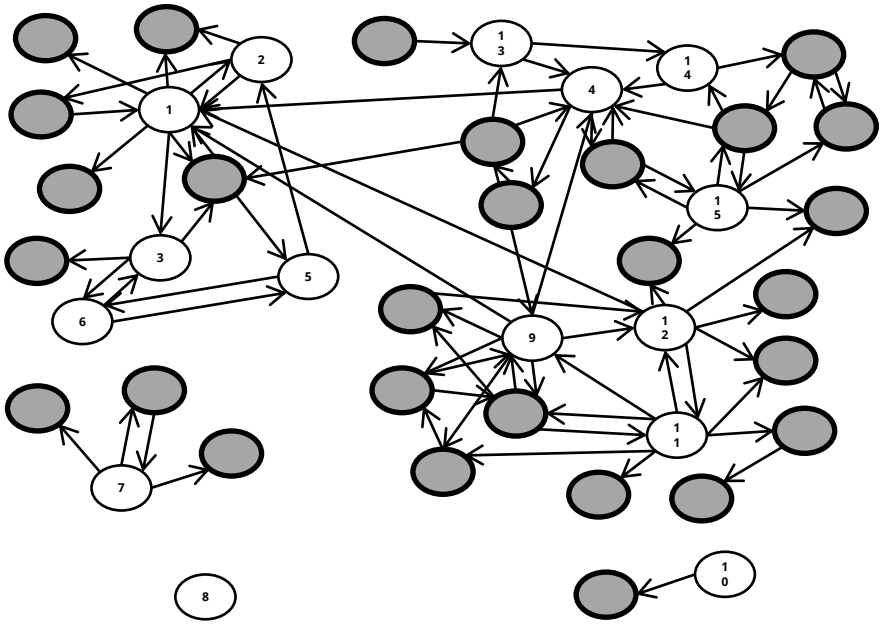
Last step is to escalate privileges by exploiting an unpatched vulnerability.

- Applying Critical Patch Updates (CPU) provided little protection until this point. CPU security patches matter at this point.
- Database hardening and configuration are as important.

The compromised database account privileges and the skill and creativity of the attacker matter most for this last step.

google: `oracle database privilege escalation`

Lateral Movement After Database Compromise



Overview

- Organization with about 150 production Oracle Databases
- Assessed15 key SOX and PCI compliance Oracle databases
- Reviewed database links for connectivity and appropriateness

Conclusion

- Compromised 28 other databases just through database links.

Agenda

1. Background
2. Tools and the Attack
3. Prevention
4. Detection
5. Q & A

Integrigy #1 Security Recommendation

- **Limit direct database access whenever possible**
  - Much harder to hack database if an attacker can not connect to 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

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

Routinely Check for Default Passwords

- **Use Oracle's DBA_USERS_WITH_DEFPWD**
  - Limited set of accounts
  - Single password for each account

- **Command line tools (orabf, etc.)**
  - Difficult to run – command line only

- **AppSentry**
  - Checks all database accounts
  - Uses passwords lists - > 1 million passwords
  - Allows custom passwords

Agenda

1. Background
2. Tools and the Attack
3. Prevention
4. Detection
5. Q & A

Auditing Design

Use Integrigy Database Auditing and Logging Framework as starting point!

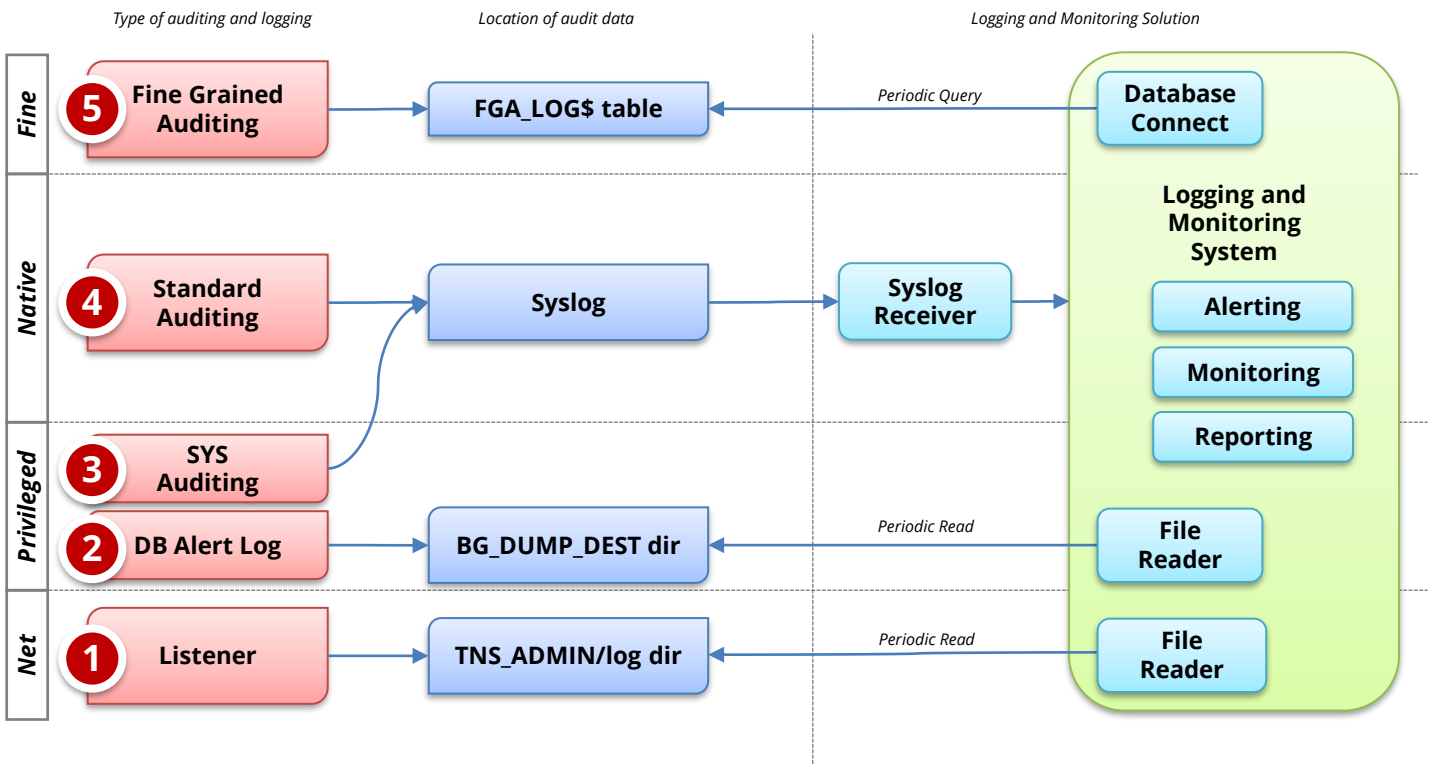
E1 - **Login**	*E8* - **Modify role**
E2 - **Logoff**	*E9* - **Grant/revoke user privileges**
E3 - **Unsuccessful login**	*E10* - **Grant/revoke role privileges**
E4 - **Modify auth mechanisms**	*E11* - **Privileged commands**
E5 - **Create user account**	*E12* - **Modify audit and logging**
E6 - **Modify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

https://www.integrigy.com/security-resources/integrigy-guide-database-auditing-and-logging

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

Traditional Database Auditing (pre 12c, 12c Mixed Mode)



Agenda

1. Background
2. Tools and the Attack
3. Prevention
4. Detection
5. Q & A

Integrigy 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**