

# ANITIAN



## Red Team Testing

# Outline

1. Penetration Test vs. Red Team
2. External Enumeration
3. Social Engineering
4. Remote Access
5. Live Demo
  1. Local Privilege Escalation
  2. Domain Privilege Escalation
6. How to Defend Against These Attacks

# Penetration Test vs. Red Team

## Penetration Testing

- Scope defined and provided by client
- Remote access is provided for internal testing
- Employees are typically aware of the test
- Rules are well defined
- Systems are tested independently

## Red Team

- Red team identifies potential scope
- External / Internal / Web applications / Social Engineering
- Limited number of employees are aware
- Almost anything goes
- Systems are tested simultaneously

# External Techniques

# External Enumeration - Passive

## Passive Intelligence Gathering - What

- Brands
- Domain names
- Hostnames
- IP addresses
- Employee names and contact information
- Technical information
- Website browsing
  
- What is your footprint?

# External Enumeration - Passive

## Passive Intelligence Gathering - How

- Whois/DNS
- Domainbigdata.com
- Google searching/dorking (passive)
- Shodan/Maltego
- Social media/Pastebin/Github
- Haveibeenpwned.com
- Sales tools
- Website browsing
- OSINT tools (theHarvester, Spiderfoot, etc...)

# External Enumeration - Active

## **Active Intelligence Gathering - What**

- Running services and version information
- Web applications
- Hidden pages or applications
- Missing patches
- Phone and PBX information
- Google Dorking (active)

# External Enumeration - Active

## Active Intelligence Gathering - How

- nmap
- netcat
- Burpsuite
- Nikto
- Vulnerability Scanning platforms (Nessus, Nexpose, Qualys)
- Phone calls



# Social Engineering

- “Social engineering is using deception, manipulation and influence to convince a human who has access to a computer system to do something, like click on an attachment in an e-mail”  
–Kevin Mitnick
- Humans just want to help
- Exploit kindness, annoyance, fear
- Testing policies and procedures rather than systems or software
- Almost always a weak link

# Social Engineering

## Email

- Ask for passwords
- Send malicious links
- Malicious attachments (back door)

## Phone

- Ask for passwords
- Convince victim to perform actions

## In Person

- Access to terminals, documents, trash
- Plant rogue devices
- Take photos

# Breaking In

# Information Gathering – Employee Data

The screenshot shows the LinkedIn search interface with the query 'company: google'. The results are filtered to show people. The top navigation bar includes links for Home, My Network, Jobs, Messaging, Notifications, Me, and Work. The search bar is at the top left, and the search button is at the top right. The results are displayed in a list format, showing profiles of Jonathan Rosenberg, Noam Bardin, John Maeda, and Avinash Kaushik. Each profile includes a profile picture, name, current position, and a 'Send InMail' button. A sidebar on the right provides filters for connections, keywords, locations, and current companies.

Showing 72,191 results.

**Jonathan Rosenberg** • 3rd  
High Tech Product Management Executive: Google, Excite@Home, Apple, Dialog. A...  
United States  
Current: Senior Vice President, Products at Google  
[Send InMail](#)

**Noam Bardin** • 3rd  
Chief Wazer at Google  
San Francisco Bay Area  
[InMail](#)

**John Maeda** • 3rd  
Global Head, Computational Design and Inclusion at Automattic  
San Francisco Bay Area  
Current: Technical Advisory Board Member at Google  
[InMail](#)

**Avinash Kaushik** • 3rd  
Author, Blogger, Digital Marketing Evangelist  
San Francisco Bay Area  
Current: Digital Marketing Evangelist at Google  
[InMail](#)

**Filter People by** [Clear all \(2\)](#)

**Connections** [^](#)

☐ 1st ☐ 2nd ☒ 3rd+

**Keywords** [v](#)

**Locations** [v](#)

**Current companies** [^](#)

☒ Google  
☐ 5392727  
☐ Google, Social Marketing Tools  
☐ YouTube  
☐ Google AdWords Certified  
[+ Add](#)

# Social Engineering - Email




Tue 11/8/2016 12:47 PM

Progress <progresssoftware@businessmaking.progress.net>

Webinar | Hybrid Data Pipeline is the Future of Data Connectivity

To Rick Osgood

 If there are problems with how this message is displayed, click here to view it in a web browser.

[Bing Maps](#)

Changing the way cloud apps access external data

## New Product Announcement: Hybrid Data Pipeline

Meet Progress® DataDirect® Hybrid Data Pipeline™, the industry's first vendor-agnostic hybrid connectivity service that can run independently with any single or multi-vendor technology stack open standards for SQL and REST. [Explore how our service revolutionizes](#)

# Social Engineering - Email

COMPOSE

Inbox (81)

Starred

Sent Mail

Drafts

More ▾

P

Progress ▾

Q

□

☆

W

Inbox

Automatic reply: Webinar | Hybrid Data Pipeline is the Future of Data Connectivity -

□

☆

M

Inbox

Automatic reply: Webinar | Hybrid Data Pipeline is the Future of Data Connectivity -

□

☆

F

Inbox

Automatic reply: Webinar | Hybrid Data Pipeline is the Future of Data Connectivity -

□

☆

B

Inbox

Automatic reply: Webinar | Hybrid Data Pipeline is the Future of Data Connectivity -

□

☆

G

Inbox

Automatic reply: Webinar | Hybrid Data Pipeline is the Future of Data Connectivity -

□

☆

C

Inbox

Automatic reply: Webinar | Hybrid Data Pipeline is the Future of Data Connectivity -

□

☆

K

Inbox

Automatic reply: Webinar | Hybrid Data Pipeline is the Future of Data Connectivity -

□

☆

S

Inbox

Automatic reply: Webinar | Hybrid Data Pipeline is the Future of Data Connectivity -

□

☆

D

Inbox

Automatic reply: Webinar | Hybrid Data Pipeline is the Future of Data Connectivity -

□

☆

B

Inbox

Automatic reply: Webinar | Hybrid Data Pipeline is the Future of Data Connectivity -

□

☆

L

Inbox

Automatic reply: Webinar | Hybrid Data Pipeline is the Future of Data Connectivity -

□

☆

C

Inbox

Automatic reply: Webinar | Hybrid Data Pipeline is the Future of Data Connectivity -

□

☆

Ir

Inbox

Automatic reply: Webinar | Hybrid Data Pipeline is the Future of Data Connectivity -

□

☆

C

Inbox

Automatic reply: Webinar | Hybrid Data Pipeline is the Future of Data Connectivity -

“”

No recent chats

[Start a new one](#)

# Active Testing – Lockouts and Remote Access

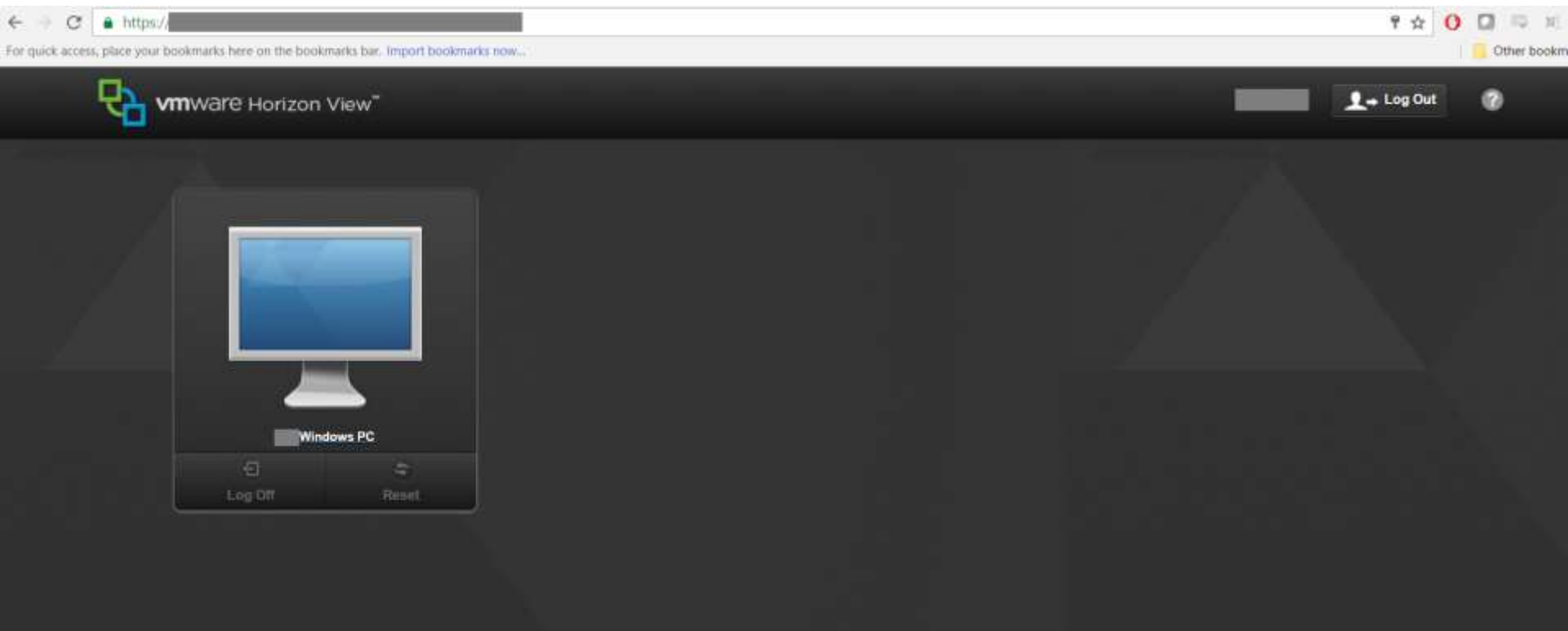


# Social Engineering - Phone





# Remote Access



# Prevention

## **Policies and Procedures**

- Verify employee identification for password resets
  - Secret questions
  - Call-back
- Discourage use of auto responders

## **Technical controls**

- MFA for remote access
- Tarpitting: prevent username enumeration techniques
- Disable external access to helpdesk, or require stronger verification procedures

# Privilege Escalation – Demonstration



# Prevention

## **Policies and Procedures**

- Discourage storing passwords in plaintext
- Educate employees to choose strong passwords

## **Technical controls**

- Provide a secure password storage solution
- Do not use group policy preferences for passwords
  - Microsoft LAPS
- Use unique passwords between accounts and systems
- Configure least privilege access
- Configure SIEM logging and alerts

# Red Teaming

## Why?

- Test your entire security program
- Discover the weak links
- Simulate a real-world motivated attacker (no constraints)

## Who?

- You feel your security is strong and you want to test it
- You need ammunition for management buy-in

# Thank you! Questions?

Use the chat feature to ask your questions

Rick Osgood – [rick.osgood@anitian.com](mailto:rick.osgood@anitian.com)

Robert Cooper – [robert.cooper@anitian.com](mailto:robert.cooper@anitian.com)