



Modern Intrusion Practices

A vertical dotted line of grey dots on the left side of the slide, starting with four dots at the top and continuing down to the word "Introduction".

Introduction

A horizontal dotted line of red dots extending across the width of the slide, starting from the end of the vertical dotted line.

Introduction

Current pen-testing practices focus on hosts or networks as targets, and start with a noisy reconnaissance and information gathering phase regardless of the mission. We'll start reviewing this practices, and showing how some examples of targets not commonly used open new dimensions for planning attacks and creating new tools.

The main focus of this talk is to start walking the path to a new perspective for viewing cyberwarfare scenarios, by introducing different concepts and tools (a formal model) to evaluate the costs of an attack, to describe the theatre of operations, targets, missions, actions, plans and assets involved in cybernetic attacks. We'll talk about current and immediate uses of this tools for attack and defence, as well as some future-but-not-sci-fi applications of it.

Introduction

Why?

- Who are we?

Who?

- Who is this for?

What?

- Why have we done it?

When?

- What is it?

Where?

A decorative dotted line consisting of a horizontal row of four grey dots at the top left, followed by a vertical line of grey dots extending downwards, and a horizontal line of red dots extending to the right from the bottom of the vertical line.

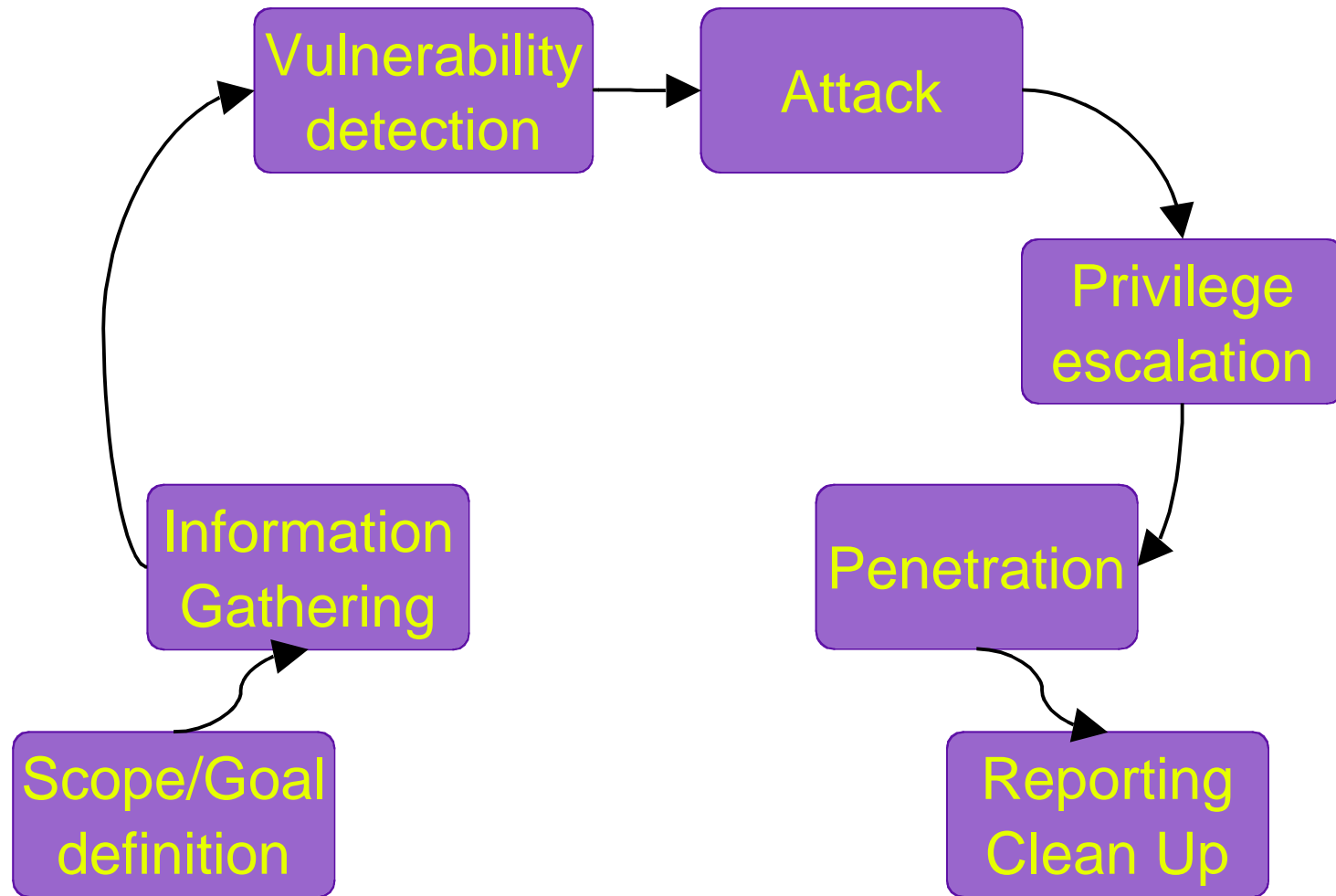
Initialization

•••• **Initialization – Current intrusion practices**

- What is your current pen-testing/hacking methodology?

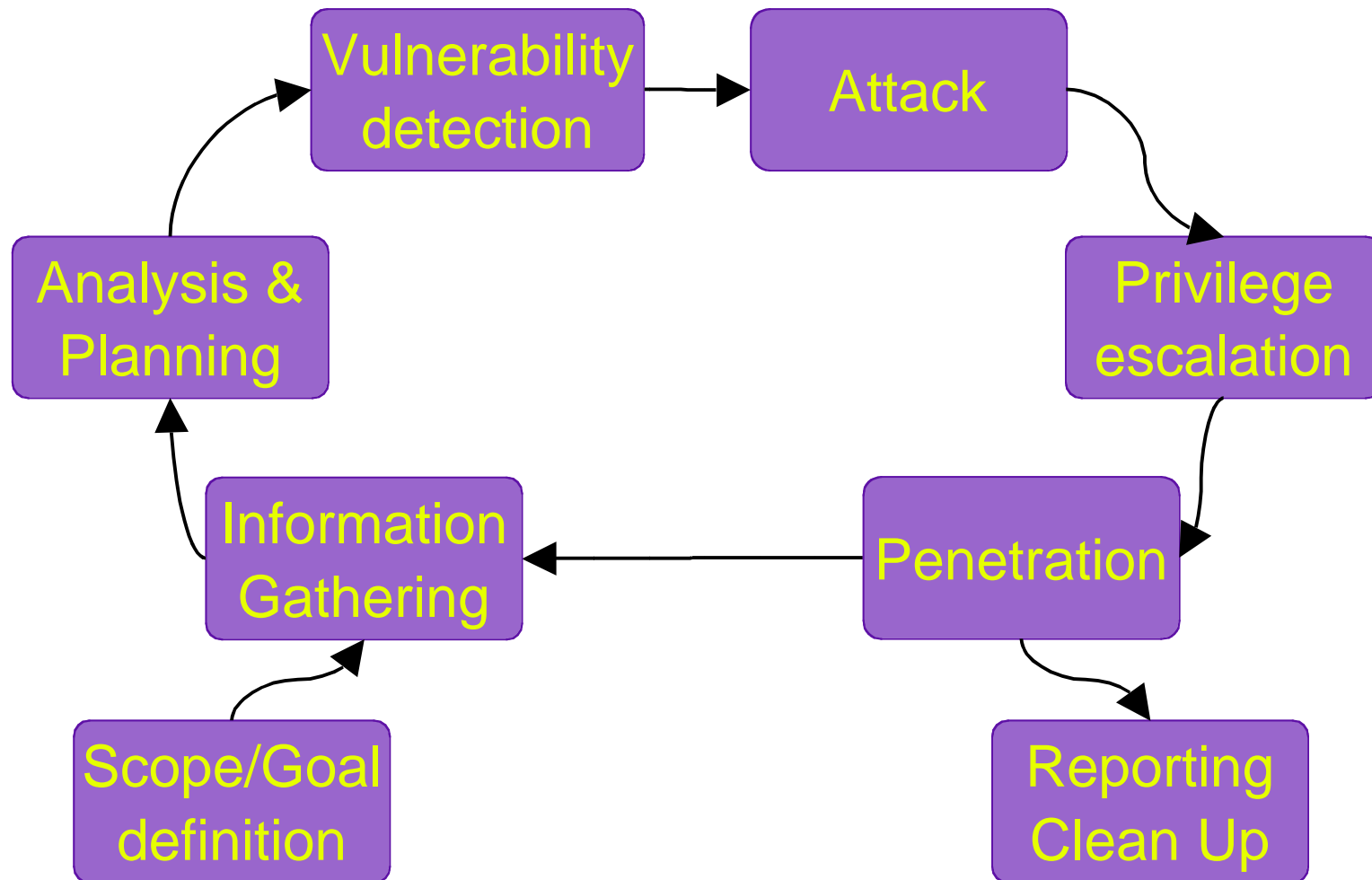
....

Initialization – Current intrusion practices



....

Initialization – Current intrusion practices



Outline

- Initialization
- More Targets
- Information Gathering Planning
- Boyd Cycle / OODA Loop
- A Model for Cyberwarfare Scenarios
- Using the Model

Questions!?

A vertical dotted line of grey dots on the left side of the slide, starting with four dots at the top and continuing down to the text.

More Targets

A horizontal dotted line of red dots extending across the width of the slide, starting from the left side of the text and ending on the right side.

More Targets

Introduced

- Hosts
- Networks
- Organizations
- Persons
- Anything else?

More Targets – Organization as target

quick notes

- Public information (whois/dns/www/etc)
- Commercial relationships
- Security beyond the perimeter
- The people is part of it
- Physical security
- Denial of service – Public image attacks

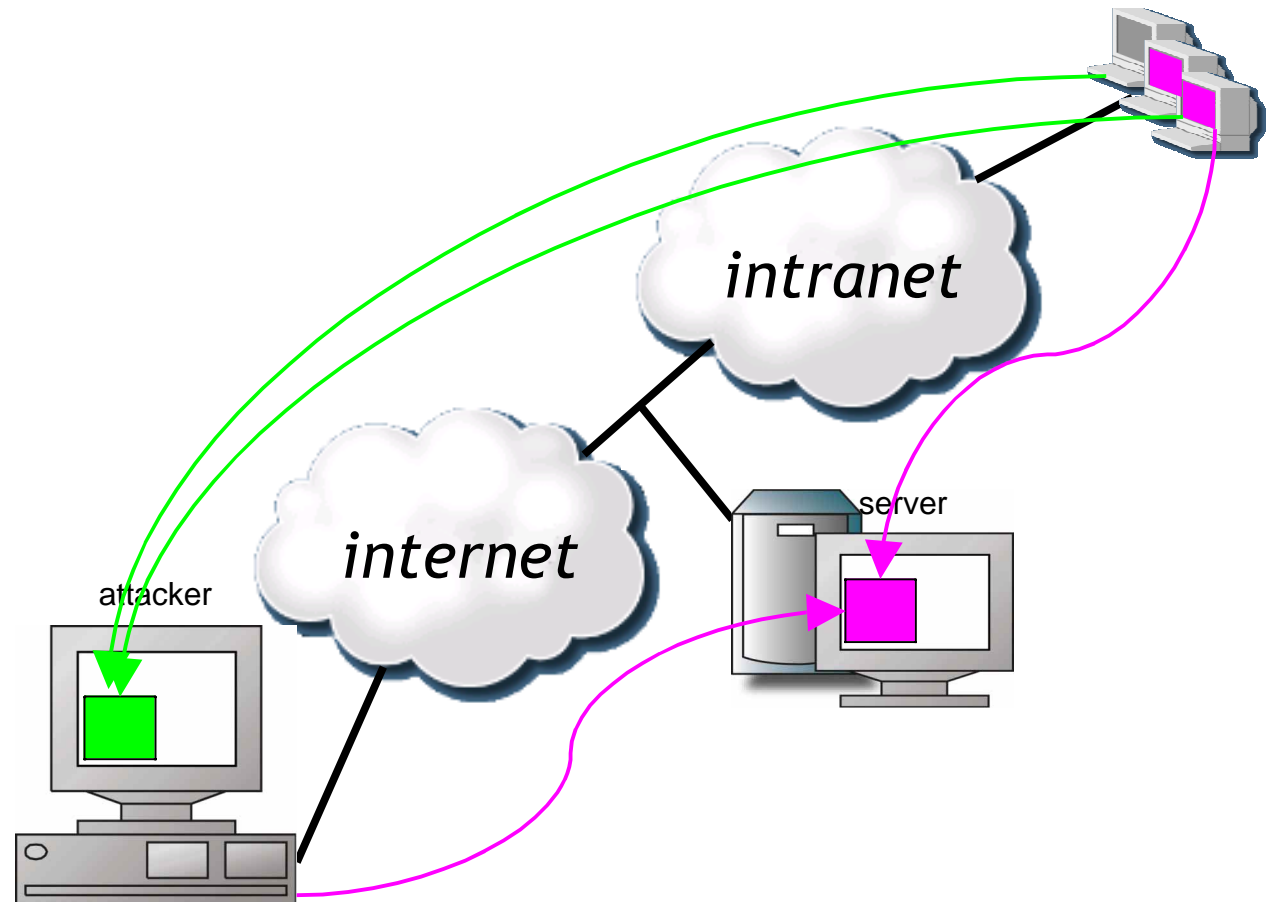
More Targets – Person as target

quick notes

- Some examples
- Representations of a Person
- Impersonation attacks
- Use the front door (not the backdoor)
- Person vs. Workstation vs. Client side
- Internal honeypots / IDS

More Targets – Person as target

architecture



More Targets – Person as target

pros

- Lighter maintenance
- Less skilled enemy
- More software (and lots of bugs)
- More targets
- Right to the inside
- Diversity is better

••••

More Targets – Person as target

cons

- Tougher tuning
- It may be more noisy
- Asynchronous nature
- Communication channel
- Uptime

More Targets – Person as target

••••

reconnaissance

- Network mapping using email headers
- Person discovery tools
- Craft profiles / trust relationships graphs
- OS and Application Detection
- Reverse traceroute

Questions!?

A vertical dotted line of grey dots on the left side of the slide, starting from the top and ending at the level of the section header.

Information Gathering Planning

A horizontal dotted line of red dots extending across the width of the slide, positioned below the section header.

... Information Gathering – Current practices

**starting the
attack**

- Establish candidate target hosts
- Determine host liveness
- Network mapping
- OS Detection
- Identification of target services



Information Gathering – Current practices

quick questions

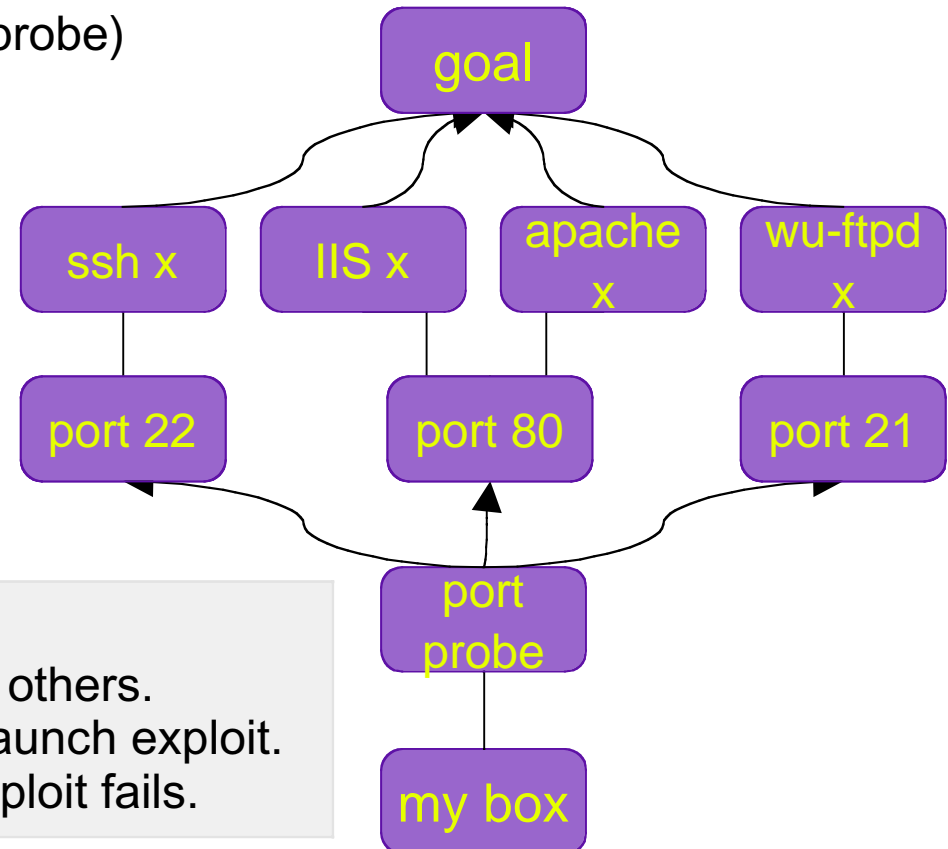
- **How do we use the outcome of IG?**
- Do we use all the information we gather?
- Does it really matter if port 9 is open?
- Does help to know the OS of every host?
- Is it really worth using a Vuln. Scanner?

Information Gathering Planning – Example 1

Goal: To gain control of a given host

I have: Target's IP address
Control of my box

I can: test if a given port is open (port probe)
exploit ssh (on an OpenBSD)
exploit wu-ftp (on a Linux)
exploit IIS (on a Windows)
exploit apache (on a Linux)



Plan: Probe only ports 22, 80 and 21.
Furthermore, probe port 80 before others.
As soon as a port is found open, launch exploit.
Keep probing other ports only if exploit fails.

... Information Gathering Planning – Example 1

quick notes

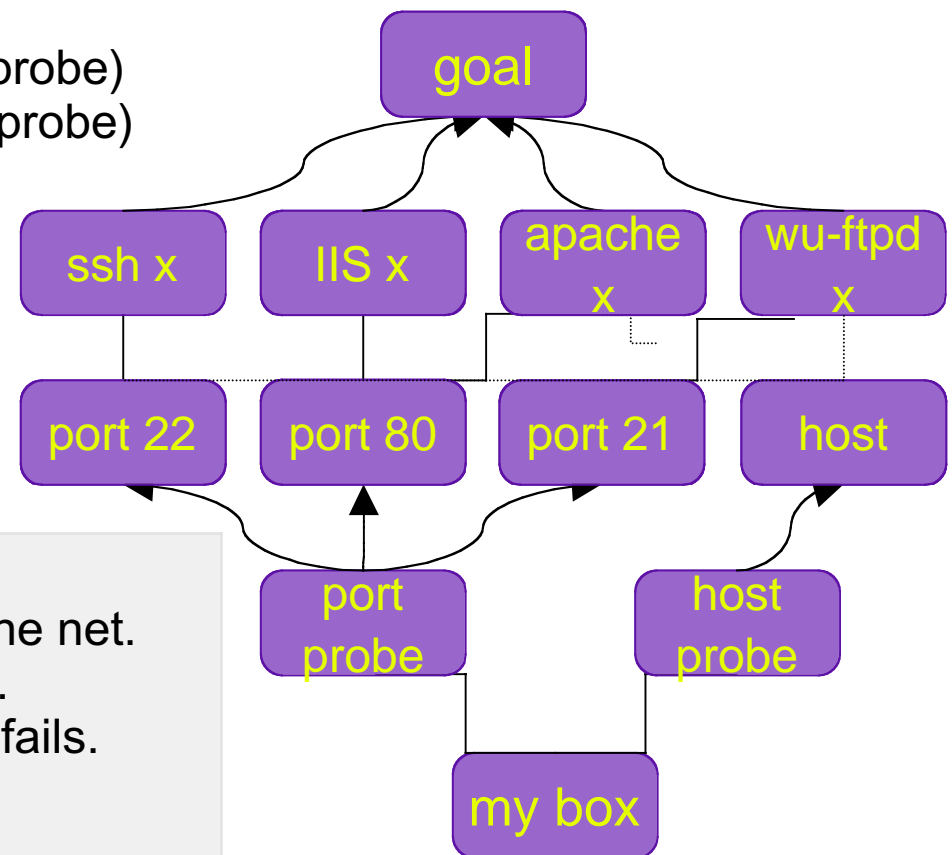
- Planning for exploits we already have
- Planning for services on standard ports
- Simple goal
- Different priorities would influence the plan
- Do we really need to port probe?
- How could we use an OS detector?

Information Gathering Planning – Example 2

Goal: To gain control of all possible hosts on a given network

I have: Target netblock
Control of my box

I can: test if a given port is open (port probe)
test if a given host is alive (host probe)
exploit ssh (on an OpenBSD)
exploit wu-ftpd (on a Linux)
exploit IIS (on a Windows)
exploit apache (on a Linux)



Plan: We won't use the host probe first.
Again, first probe port 80, across the net.
Launch exploit for every open port.
Keep probing other ports if exploit fails.
[Host probe remaining hosts]
[Probe nonstandard ports]



observations

Boyd cycle / OODA loop

- Observe, Orient, Decide, Act
- Maneuver vs. Attrition warfare
- Attacker vs. Attacker
- Attacker vs. Defender
- OODA Loop vs. Technology race

... **Boyd cycle / OODA loop / Technology Race**

defensive

- Bug -> Patch -> Patched system
- IDS/Logs/Alerts -> Reaction
- Vulnerability Scan -> Fix
- Pen-test/Audit -> Fix

offensive

- IG -> Analysis -> Planning -> Attack
- Find service -> Find bug -> code x -> attack
- Publish advisory vs. Save bug for future

Questions!?

A decorative dotted line that starts with four grey dots in a horizontal row, then continues as a vertical line of grey dots, and finally as a horizontal line of red dots.

The Model

The Model – Introduction

components

- Actions Things you can do
- Assets Things you can have or know
- Agents The actors, who can do Actions
- Goals Mission or single Action Goal
- Costs The cost of a given Action
- Plan Actions needed to fulfil a Goal
- Attack Graph Union of all possible plans

... The Model – Assets, Goals and the Environment

Asset

Any information or resource the attacker may need in the course of an attack, either as intermediate result or to complete the mission.

- host 192.168.1.1
- TCPConnectivity to port 80 of host 192.168.1.1
- OS of host 10.1.1.2
- Banner for port 21 of host 10.1.1.2
- Agent installed on host 192.0.34.166

Goal

Goals are expressed as questions or requests whose answers are **Assets**. To fulfil a given **Goal** some **Action** will be executed.

- I want an Agent installed on host 192.0.34.166
- What is the OS of host 10.1.1.2?

Environment

The **Environment** is the current knowledge about the world, and it's expressed as a collection of **Assets**.

... The Model – Actions, Plan and Attack Graph

Actions

Anything an **Agent** can do is represented as an **Action**. Each **Action** will have a **cost** some **results** and **requirements** (expressed as **Assets**).

- Apache chunked encoding Exploit
- Banner grabber
- TCP/UDP/ARP/ICMP/DNS host probe
- Connect/SYNRST/FIN TCP port probe
- Password sniffer

Plan

Chain of actions needed to fulfil a **Goal**. A **Plan** is a path from a given initial **Environment** to the desired **Goal**.

Attack Graph

Union of all possible **Plans**, and description of how all **Actions** are related to each other. It's a directed graph, starting in the initial **Environment** and ending in the final **Goal**.

The Model – Agents

Agent

One who acts for, or in the place of, another.

Human Agent

The attacker is the **Agent** who will start an attack by formulating the mission **Goal**. Also, some **Actions** may require human intervention (actions for social engineering or perception management, usually when the target is a Person who has to be fooled).

Software Agent

There are two types of **Software Agents**, those which given a **Goal** can create a **Plan** to fulfil it, and probably require or install new **Agents** in the process, to whom it assigns **Goals**, **Plans** or **Actions** to execute. And those who offer a certain set of capabilities, like accessing the file system of a host, or establishing TCP connections. The capabilities of each agent determine which **Actions** that **Agent** will be able to execute.

The Model – Cost

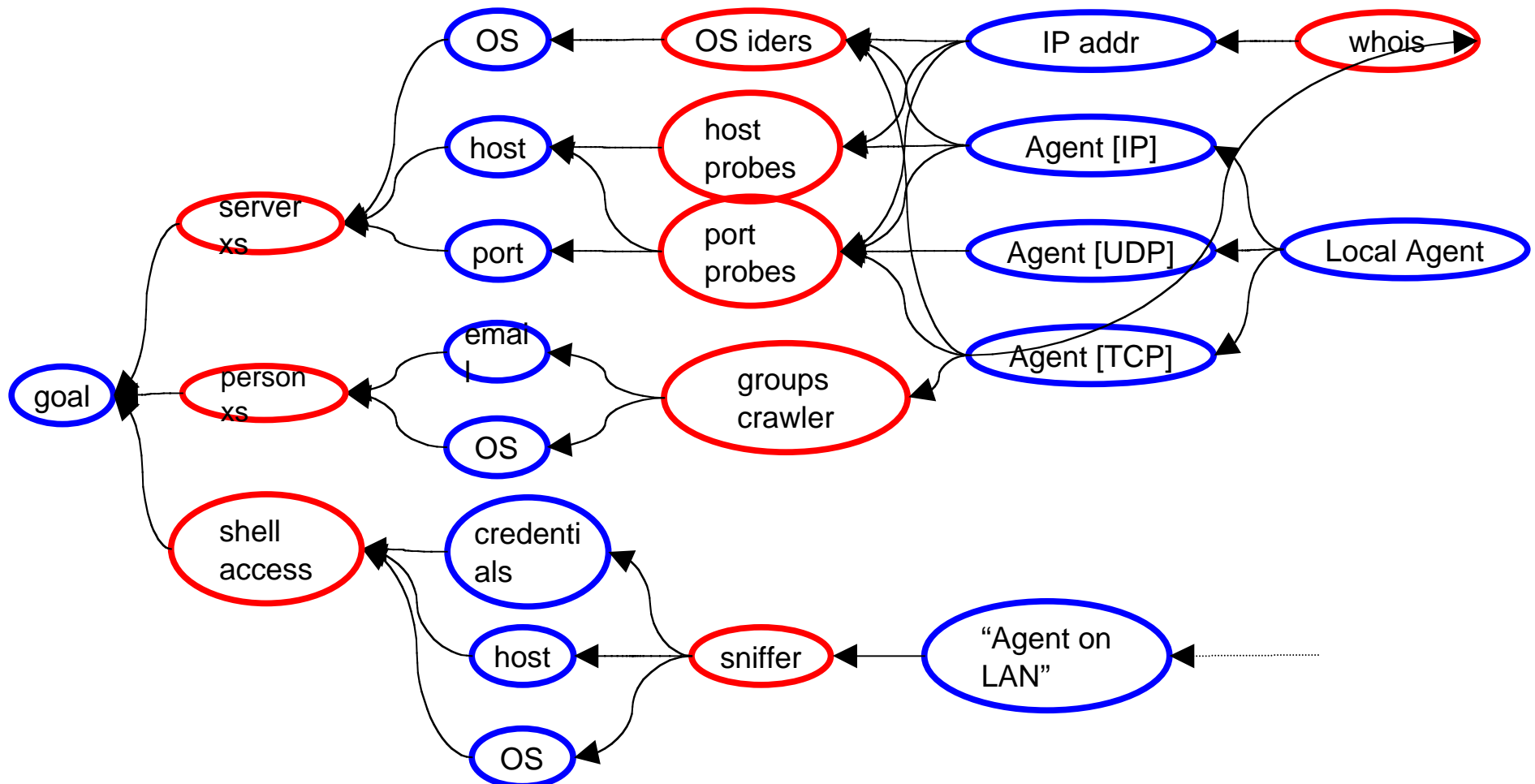
• • • •

dimensions

- Produced noise / Stealthiness
- Running time
- Probability of success
- Trust
- Traceability
- 0day-ness

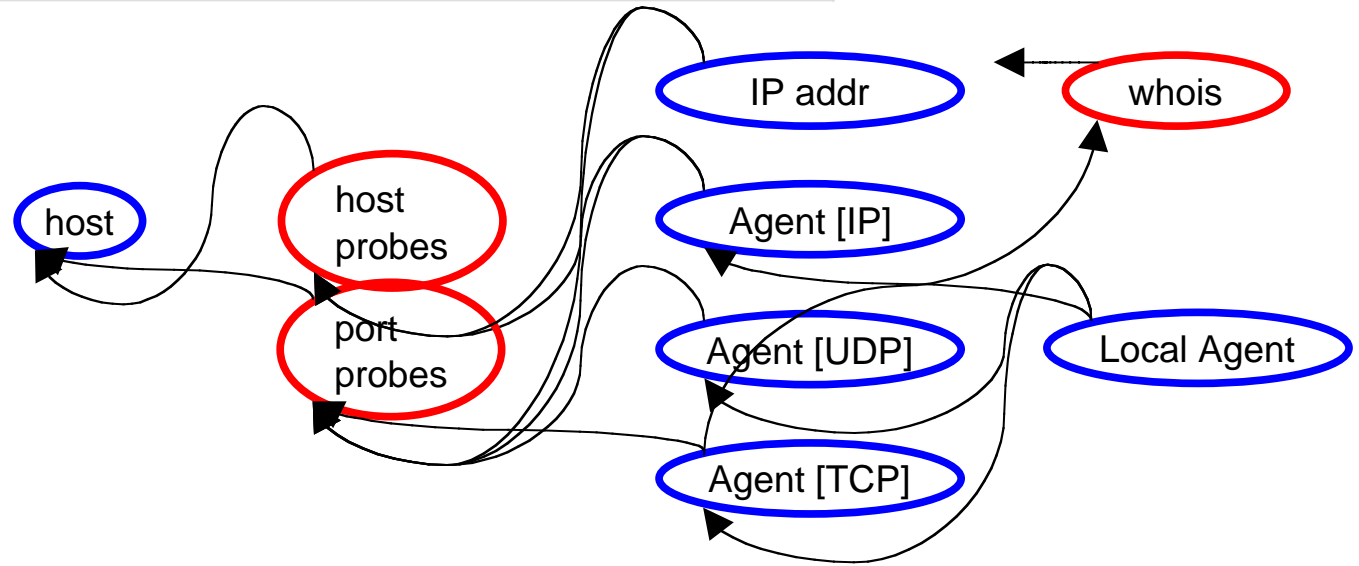
The Model – Building an attack graph

Goal: To gain control of all possible hosts on a given domain



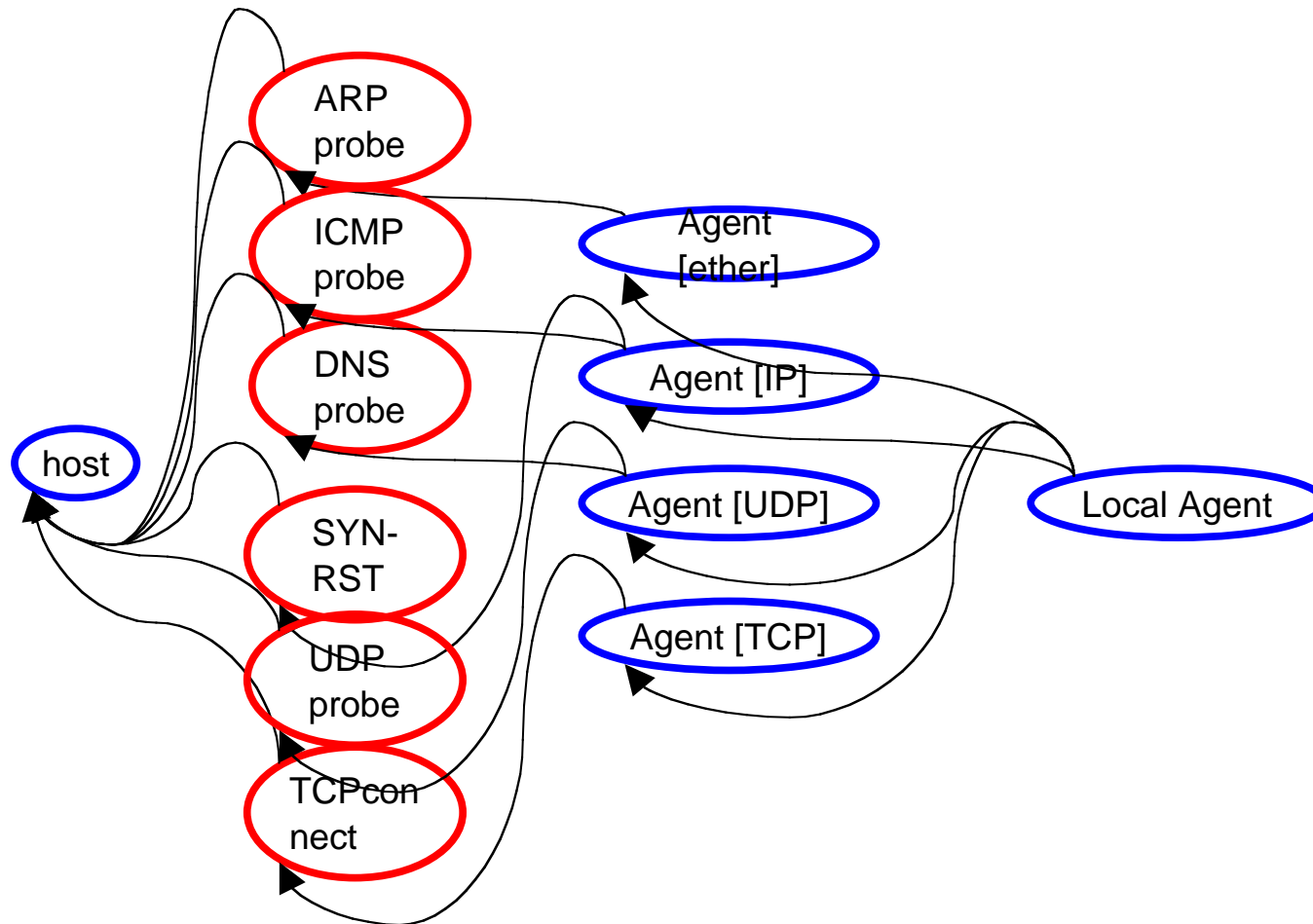
The Model – Building an attack graph

subgoal: To obtain possible target hosts for a given domain



The Model – Building an attack graph

subgoal: To obtain possible target hosts for a given netblock



The Model

Some Uses

- Attack planning
- Risk assessment
- Attacker profiling
- Higher level IDS
- Assisted intrussion
- Automated intrussion
- Action developement prioritizing

Outline

- Current practices
- More Targets
- Information Gathering Planning
- Boyd Cycle / OODA Loop
- A Model for Cyberwarfare Scenarios
- Using the Model

.....Outline

Questions!?

The Model

Breaking into computer networks from the internet.

Roelof Temmingh & SensePost

<http://www.sensepost.com>

Security - Hacking Methodology

Ryan Net Works, LLC

<http://www.cybertrace.com/papers/hack101.html>

Attack Methodology

hack-gear

<http://web.archive.org/web/20020610051120/http://www.hack-gear.com/methods.html>

Training "Hacking Inside-Out"

Aszure nv/sa

<http://www.aszure.com/education/Sheet%20Training%20HackingInsideOut%20v4.pdf>

ISS's from Ethical Hacking course (public material only)

http://www.iss.net/education/pacasia/course_descriptions/vendor_neutral_courses/ethical_hacking.php

http://www.iss.net/education/course_descriptions/security_courses/ethicalhacking.php

Ethical Hacking course material:

Reto Baumann / SANS

http://www.giac.org/practical/GSEC/Reto_Baumann_GSEC.pdf

Ultimate Hacking course (public material only)

Foundstone

http://www.foundstone.com/services/ultimate_hacking-outline.html

Hacking: An analysis of Current Methodology

John Tobler and Kevin O'Connor

http://www.cs.wisc.edu/~tobler/_private/Hacking.pdf

The Model



Automated Penetration Testing: *A new challenge for the IS industry?*

Ivan Arce and Maximiliano Caceres – Core Security Technologies – BlackHat Briefings 2001

<http://www1.corest.com/common/showdoc.php?idxseccion=13&idx=136>

Security Consulting Services

Core Security Technologies

<http://www1.corest.com/services/consulting/index.php>

Attack Trends - The Weakest Link Revisited

Elias Levy – Ivan Arce

IEEE Computer Society - Security & Privacy Magazine, Vol. 1, No. 2.

<http://www1.corest.com/common/showdoc.php?idx=320&idxseccion=51&idxmenu=32>

Widows of Vulnerability: A Case Study Analysis

William A. Arbaugh – William L. Fithen – John McHugh

IEEE – COMPUTER

<http://csdl.computer.org/comp/mags/co/2000/12/rz052abs.htm>

Timing the Application of Security Patches for Optimal Uptime

Steve Beattie, Seth Arnold, Crispin Cowan, Perry Wagle and Chris Wright

WireX Communications, Inc.

<http://wirex.com/%7Ecrispin/time-to-patch-usenix-lisa02.ps.gz>

Offensive Fundamentals I

United States Marines Corps – Basic Officer Course

<http://www.leatherneck.marines.usna.edu/images/Pubs/b0354.pdf>

Historical Applications Of Maneuver Warfare In The 20th Century

Major Peter E. Higgins, USMC

<http://www.globalsecurity.org/military/library/report/1990/HPE.htm>

The Model



Introduction to Asymmetric Warfare (AW), 4th Generation Warfare (4GW) and Maneuver Warfare (MW)

GySgt Bob Howard, USMC

http://www.d-n-i.net/fcs/ppt/howard_intro_to_4GW.ppt

Building Computer Networks Attacks

Ariel Futoransky, Luciano Notarfrancesco, Gerardo Richarte, Carlos Sarraute

Soon to be published

Lessons Learned Writing Exploits I

Ivan Arce, Gerardo Richarte

CanSecWest 2002

<http://www1.corest.com/common/showdoc.php?idx=226&idxseccion=13&idxmenu=35>

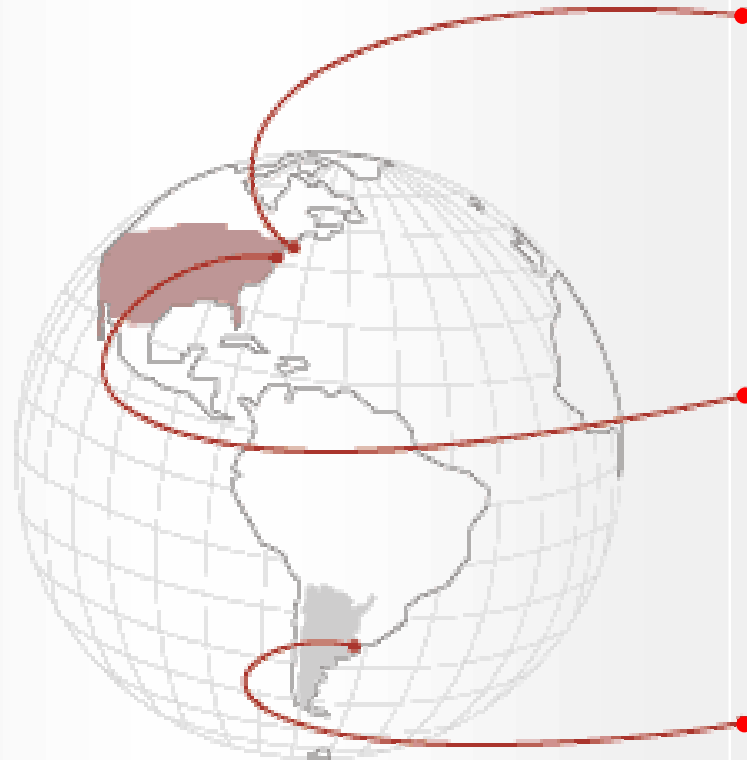
Lessons Learned Writing Exploits II

Gerardo Richarte

G-Con 1

http://www.g-con.org/speakers/Automated_Pen_Testing

CORE SECURITY TECHNOLOGIES · Contact Information



Headquarters · Boston, MA

46 Farnsworth St
Boston, MA 02210-1211 | USA
Ph: (617) 399-6980
info.usa@coresecurity.com

Sales Office · New York, NY

44 Wall Street | 12th Floor
New York, NY 10005 | USA
Ph: (212) 461-2345 | Fax: (212) 461-2346
info.usa@coresecurity.com



Research and Development Center

Florida 141 | 2º cuerpo | 7º piso
(C1005AAC) Buenos Aires | Argentina
Tel/Fax: (54 11) 5032-CORE (2673)
info.argentina@coresecurity.com

www.coresecurity.com