Security:
Threats, Risks and Attacks

Simon Balthazar, TZNIC

Presentation created by Merike Kaeo
merike@doubleshotsecurity.com

Securing The Network - Basic Terms

- **Threat**
  - An adversary that is motivated and capable of exploiting a vulnerability
- **Vulnerability**
  - A weakness in security procedures, network design, or implementation that can be exploited
- **Risk**
  - The possibility that a particular vulnerability will be exploited

What are you trying to protect?

Against whom?

What Are Security Goals?

- Controlling Data / Network Access
- Protecting Information in Transit
- Ensuring Network Availability
- Preventing Intrusions
- Responding To Incidences

Security Properties

- Confidentiality
  - Access to information is restricted to those who are privileged to see it
- Integrity
  - Having trust that information has not been altered during its transit from sender to intended recipient
- Accountability
  - Non-repudiation: property of a cryptographic system that prevents a sender from denying later that he or she sent a message or performed a certain action
- Availability
  - Information or resources are accessible when required

Security Services

- Authentication
  - Process of verifying the claimed identity of a device, user and/or application
- Authorization
  - Rights and permissions granted to a user, device or application that enables access to resources
- Access Control
  - Means by which authorized user has access to resources
- Encryption
  - Mechanism by which information is kept confidential
- Auditing
  - Process that keeps track of networked activity

Causes of Security Related Issues

- Protocol error
  - No one gets it right the first time
- Software bugs
  - Is it a bug or feature ?
- Active attack
  - Targeting specific devices
  - BotNets
  - DDoS [amplification attacks]
- Configuration mistakes
  - Very common form of problem

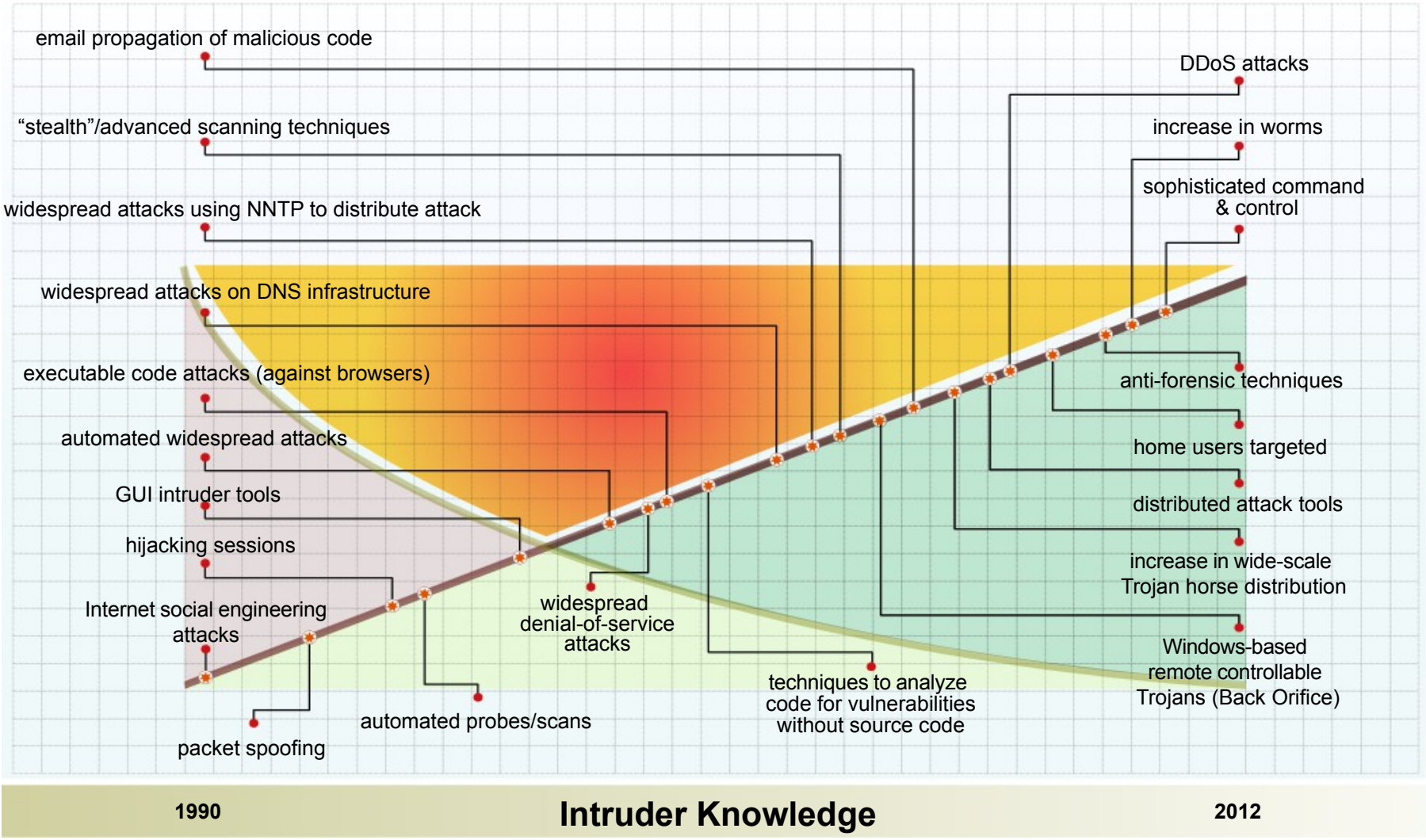
Passive vs Active Attacks

- Passive Attacks
  - Eavesdropping
  - Offline cryptographic attacks
- Active Attacks
  - Replay
  - Man-In-The-Middle
  - Message Insertion
  - Spoofing (device or user)
  - Denial of Service
  - Protocol specific attacks

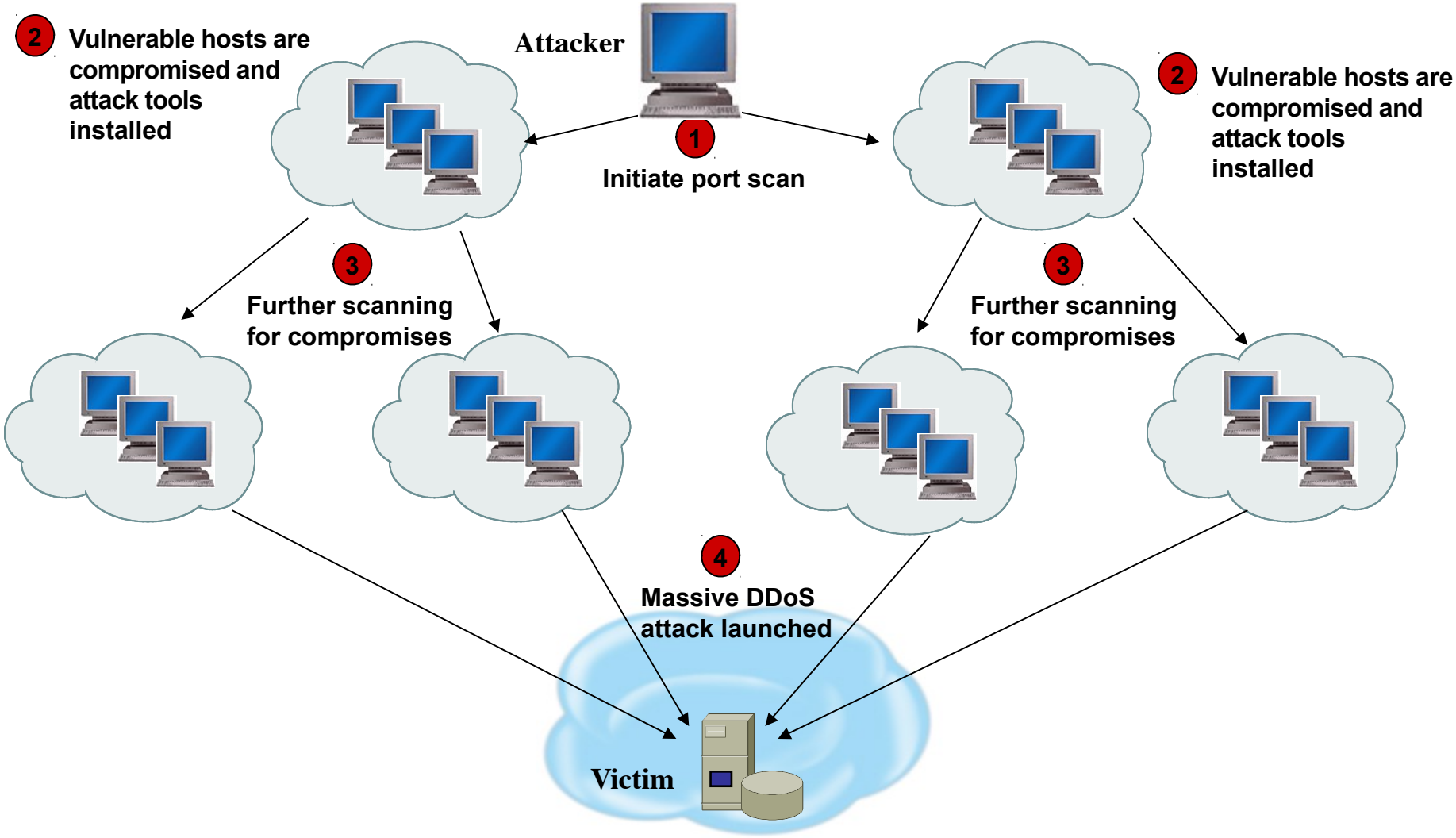
What Can Attackers Do?

- Eavesdrop for reconnaissance
- Send arbitrary messages (spoof IP headers and options)
- Replay recorded messages
- Modify messages in transit
- Write malicious code and trick people into running it
- Exploit bugs in software to ‘take over’ machines and use them as a base for future attacks

Evolution of Attack Landscape



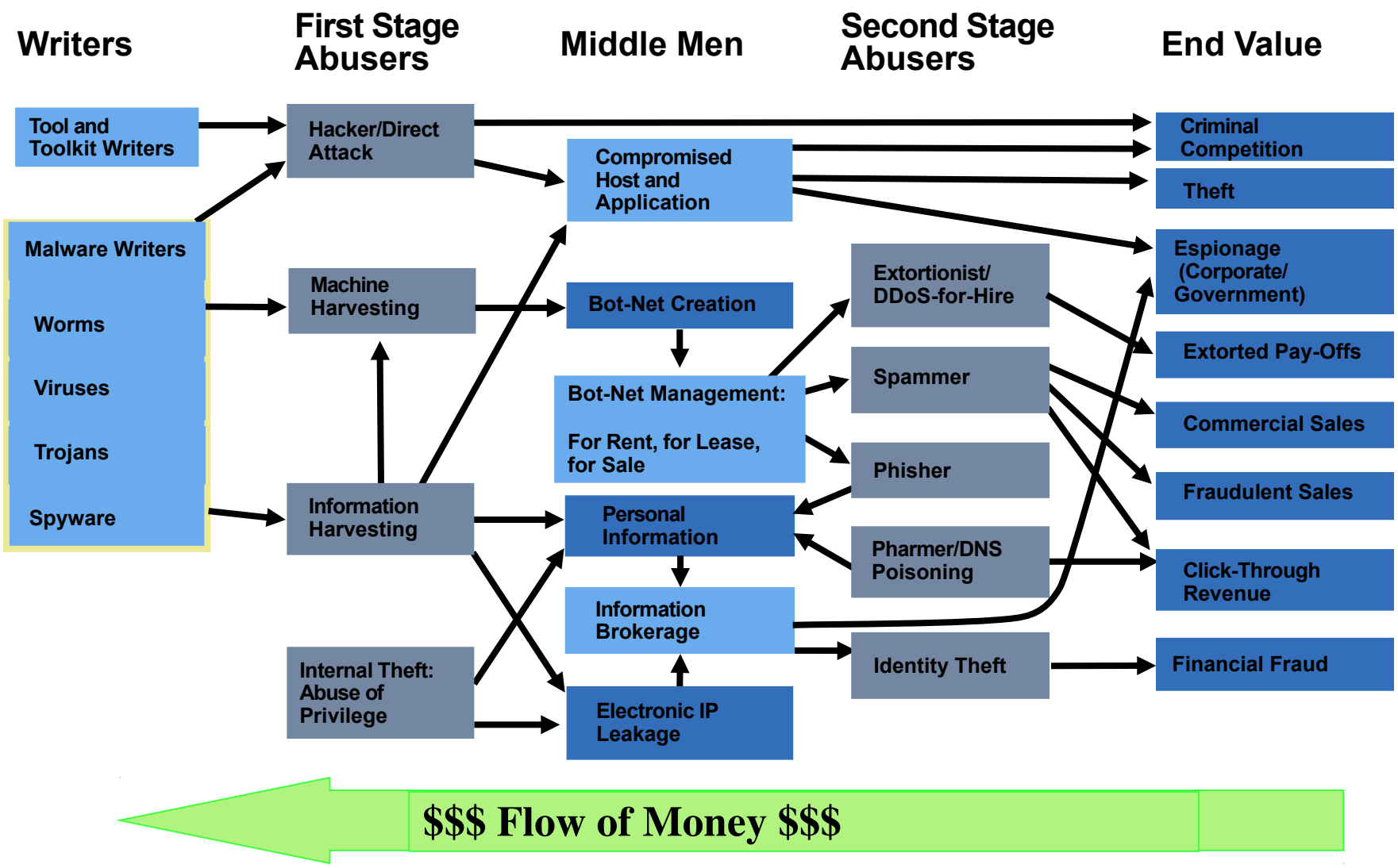
Automated DDoS Attack



Attack Motivation

- Criminal
  - Criminal who use critical infrastructure as a tools to commit crime
  - Their motivation is money
- War Fighting/Espionage/Terrorist
  - What most people think of when talking about threats to critical infrastructure
- Patriotic/Principle
  - Larges group of people motivated by cause be it national pride or a passion aka Anonmous

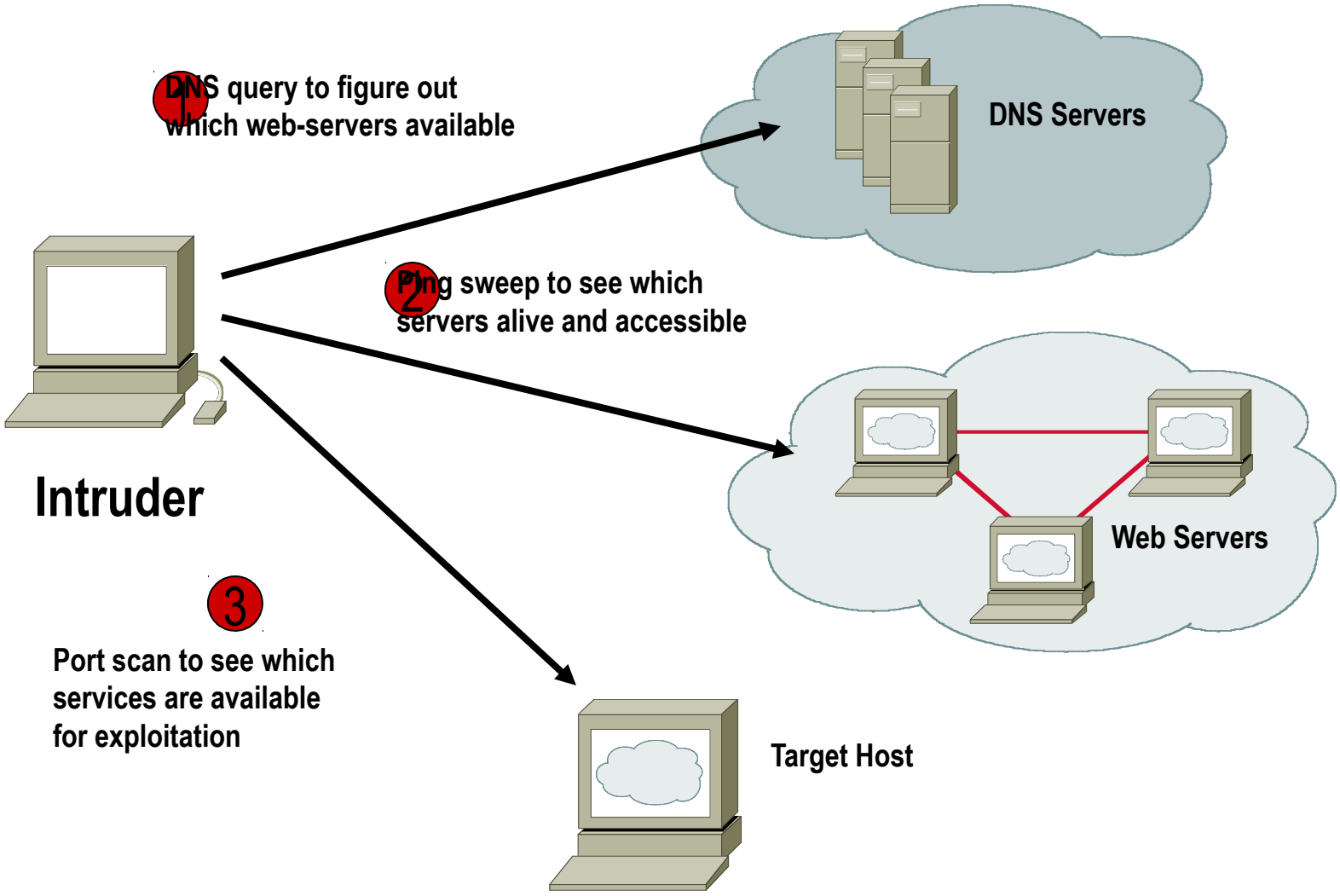
Threat Economy: Today



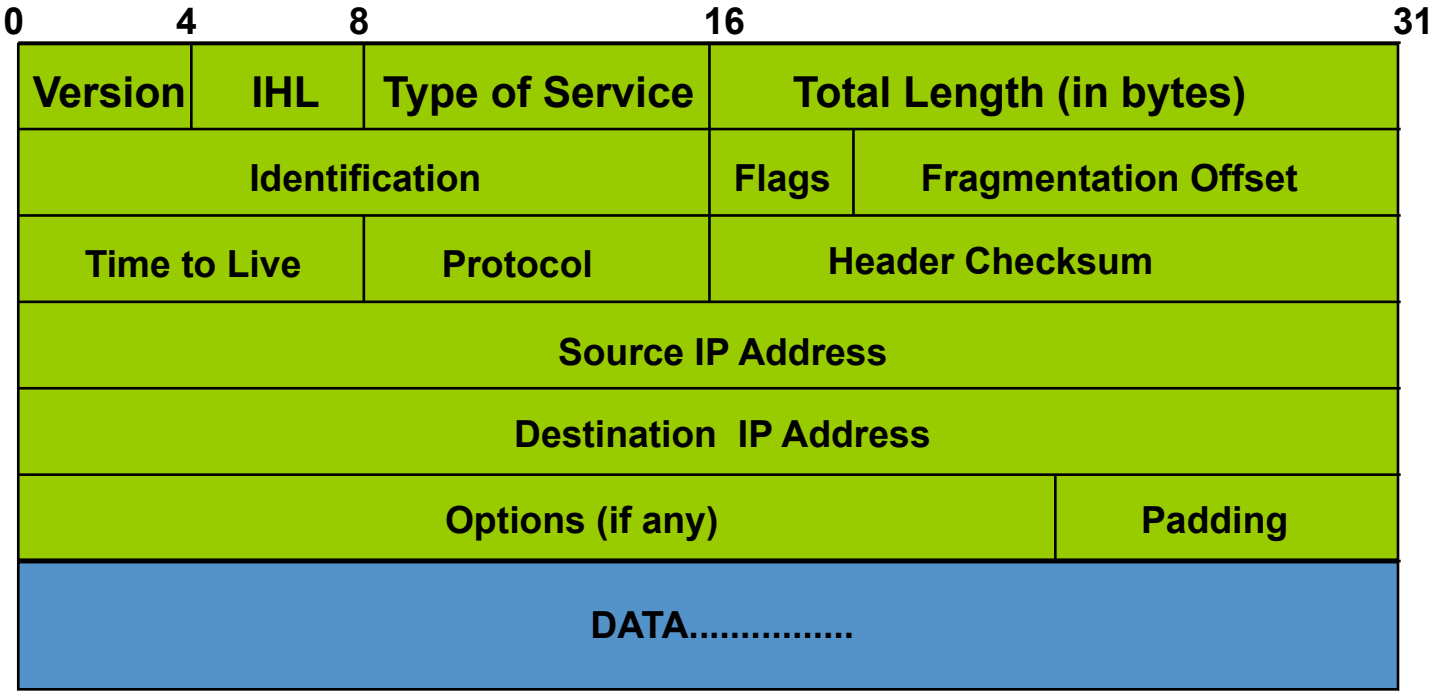
Most Common Threats and Attacks

- Opportunistic
  - Port scanning to exploit known vulnerabilities
  - Password cracking
  - Phishing attacks
- Targeted Attacks
  - You have something they want
  - Amplification attacks, spear-phishing
- Advance Persistent Threat (APT)
  - Very skilled attackers aiming at specific targets
  - Will target CPU, memory, bandwidth
  - Creative BotNets

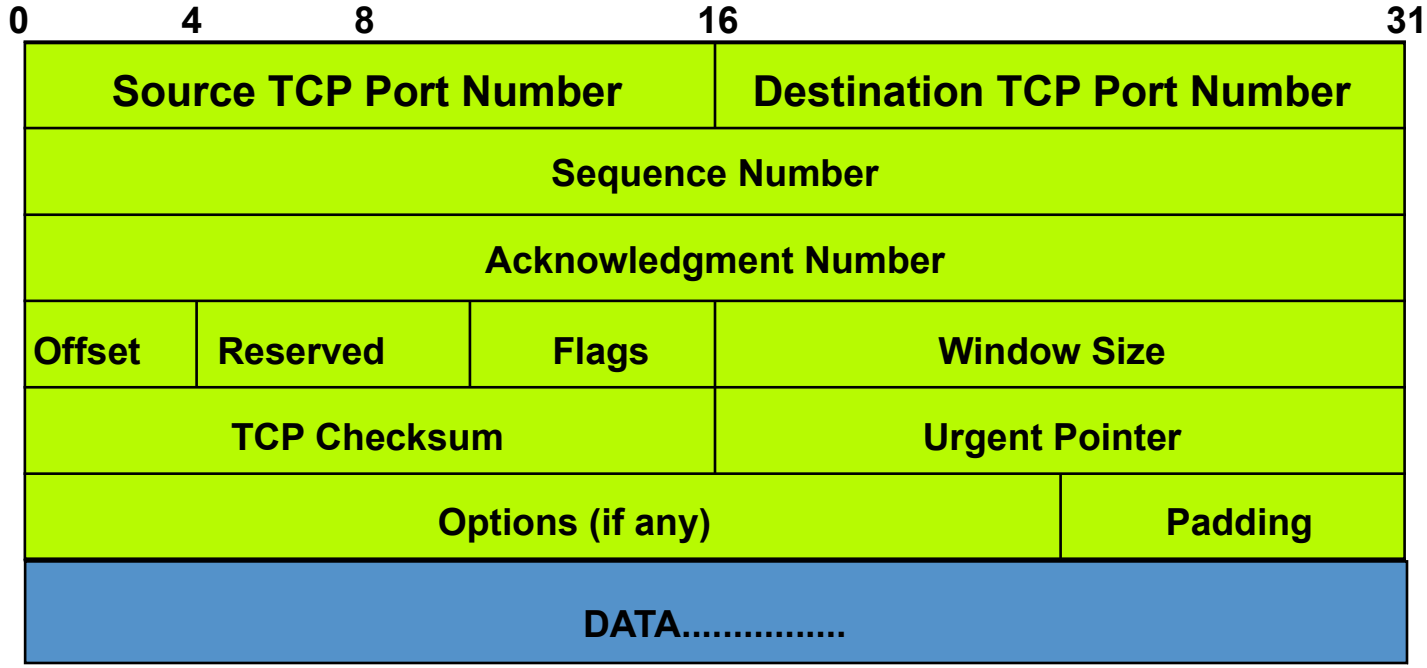
Example Reconnaissance Attempt



IPv4 Protocol Header



TCP Header



FLAGS:

- URG: indicates urgent data in data stream
- ACK: acknowledgement of earlier packet
- PSH: flush packet and not queue for later delivery
- RST: reset connection due to error or other interruption
- SYN: used during session establishment to synchronize sequence numbers
- FIN: used to tear down a session

DoS and DDoS Attacks

- TCP SYN
- TCP ACK
- UDP, ICMP, TCP floods
- Fragmented Packets
- IGMP flood
- Spoofed and un-spoofed

Mistakes IT People Make

- Connecting systems to the Internet before hardening them.
- Connecting test systems to the Internet with default accounts/passwords
- Failing to update systems when security holes are found
- Using telnet and other unencrypted protocols for managing systems, routers, firewalls, and PKI.
- Giving users passwords over the phone or changing user passwords in response to telephone or personal requests when the requester is not authenticated.
- Failing to maintain and test backups.
- Running unnecessary services : ftpd, telnetd, finger, rpc, mail, rservices
- Implementing firewalls with rules that don't stop malicious or dangerous traffic - incoming and outgoing.
- Failing to implement or update virus detection software
- Failing to educate users on what to look for and what to do when they see a potential security problem.

Security Policy / Incident Handling

- How much you worry depends on risk assessment analysis
  - ***Risk analysis***: the process of identifying security risks, determining their impact, and identifying areas requiring protection
- Must compare need to protect asset with implementation costs
- Define an effective security policy with incident handling procedures

First Step…..Security Policy

- What are you trying to protect?
  - What data is confidential?
  - What resources are precious?
- What are you trying to protect against?
  - Unauthorized access to confidential data?
  - Malicious attacks on network resources?
- How can you protect your site?

Creating A Security Policy

- Start With Something Basic
  - Acceptable Use Policy
  - Authentication Policy
  - Network Access Policy
  - Email Policy
  - Mobile Device Policy
- What Regulatory Compliance Do You Have To Follow?

Know What You Are Protecting

- Identify Critical Assets
  - Hardware, software, data, people, documentation
- Place a Value on the Asset
  - Intangible asset – importance or criticality
  - Tangible asset – replacement value and/or training costs
- Determine Likelihood of Security Breaches
  - What are threats and vulnerabilities ?

Varying Degrees of Robustness for Security Elements

Will I Go Bankrupt ?

- Spend More Money
- Spend More Time

Is It An Embarrassment ?

NEED TO DO A RISK ANALYSIS !

Risk Mitigation vs Cost of Security

Risk mitigation: the process of selecting appropriate controls to reduce risk to an acceptable level.

The ***level of acceptable risk*** is determined by comparing the risk of security hole exposure to the cost of implementing and enforcing the security policy.

Assess the cost of certain losses and do not spend more to protect something than it is actually worth.

Characteristics of a Good Policy

- Can it be implemented technically?
- Are you able to implement it organizationally?
- Can you enforce it with security tools and/or sanctions?
- Does it clearly define areas of responsibility for the users, administrators, and management?
- Is it flexible and adaptable to changing environments?

Creating a Security Policy

- Security Policy Templates:
  - http://www.sans.org/security-resources/policies/
    - Computer Security Policy
    - Desktop Security Policy
    - Email Security Policy
    - Internet Security Policy
    - Mobile Security Policy
    - Network Security Policy
    - Physical Security Policy
    - Server Security Policy
    - Wireless Security Policy

Incident Response

- It is always best to have a plan in place before something bad happens
- DO NOT PANIC!
- If you set appropriate guidelines now, it will make things a lot easier when a security incident happens

Create a checklist that can be followed when a significant security incident does occur!!

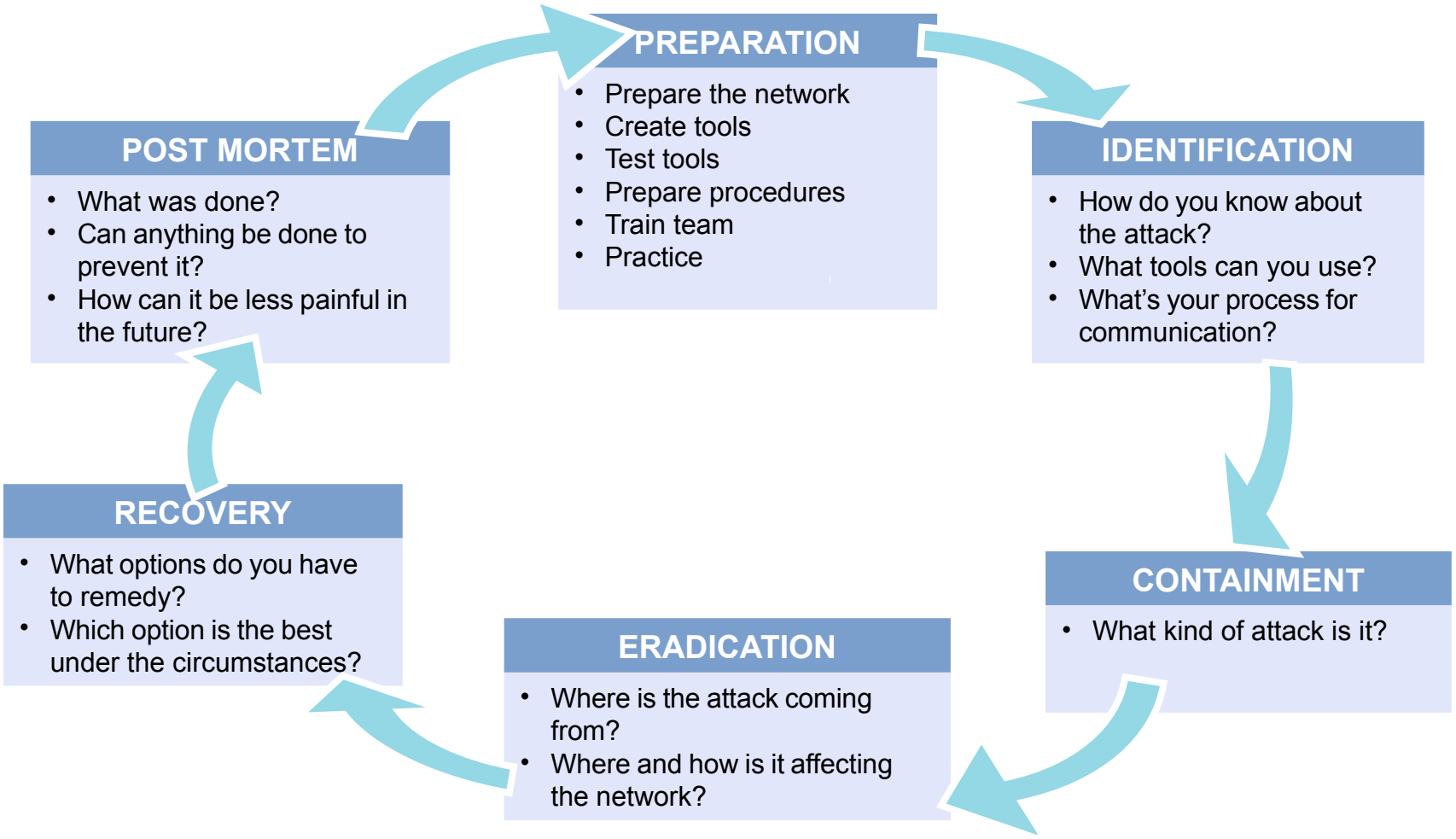
What Incidents Should Be Reported?

- Any suspicious activity should be reported
  - This includes suspicious user account behavior, computer system failures or misbehavior, accidental publication of internal email, loss of equipment / account information, etc.
- Reporting methods
  - Internal
    - Online support ticketing system
    - Technical support email
  - External
    - Abuse / incident email contact
    - Public web-based contact form
    - Telephone number specifically for reporting abuse

Information for Reporting An Incident

- Date and time of the event
- Description of the event
- Assets that are affected or at risk as a result of the event
- Whether the event is in progress or has concluded
- Actions taken by the party reporting the event
- Informal assessment of the harm or impact to the asset
- Informal assessment of collaterally affected assets
- Data (logs, files, reports) that may assist the CIRT in analyzing the event

Six Phases of Incident Response



Preparation

- Includes technical and non-technical elements
- Know the enemy
  - Understand what drives the attacker
  - Understand their techniques
- Create the security team and plan
  - Who handles security during an event? Is it the security folks? The networking folks? The lawyers?
- Harden the devices
- Prepare the tools needed for forensics

Identification

- Goal is to gather events, analyze them and determine whether you have an incident
- Assign Incident Handlers
  - Select a person to handle identification and assessment
  - Empower them to escalate if needed
- Control the Flow of Information
  - Enforce “need to know” policy
  - Tell details to minimum number of people possible
- Create Trusted Communication Channels

Identification

How Do You Know You Are Under Attack?

- Understand the details and scope of the attack
  - Identification is not sufficient; once an attack is identified, details matter
  - Guides subsequent actions
- Qualify and quantify the attack without jeopardizing services availability (e.g., crashing a router):
  - What type of attack has been identified?
  - What's the effect of the attack on the victim(s)?
  - What next steps are required (if any)?
- At the very least:
  - Source and destination address
  - Protocol information
  - Port information

Containment

- Stopping the Damage
  - Prevent attacker from getting any deeper into the impacted systems, or spreading to other systems
- Inform Management
- Notify your local or organizational incident handling team
- Additional 3 phases
  - Short term containment
  - Gathering evidence / backup
  - Long term containment

Short Term Containment

- Try to prevent attacker from causing more damage
- Want untainted evidence
- Some possible actions:
  - Disconnect network cable
  - Pull the power cable (loses volatile memory and may damage drive)
  - Isolate switch port so that system can no longer send/receive data
  - Apply filters to routers and/or firewalls
  - Change a target's name in DNS to point to a different IP address

Image Creation

- This is never easy under pressure
- Hint: Play with these tools and make sure you know how to use them before an incident happens
  - dd for Unix/Linux and Windows
  - Ghost (the latest versions – default is not bit-by-bit so know how to configure)
  - Drive duplicator hardware and write blockers

Long Term Containment

- Once back-up created for forensics analysis the changes for long term containment can begin
- Apply temporary solution(s) to stay in production while building a clean system
  - Patch system
  - Change passwords
  - Remove accounts used by hacker
  - Change file permissions
  - Shutdown backdoor processes used by attacker

Eradication

- Goal is to get rid of any traces on network device(s) that an attack occurred
- Determine how the attack was executed from the gathered evidence
- Restore operating systems and configurations from clean backups
- May require starting from completely wiped systems
- Improve defenses

Recovery

- Goal is to get impacted systems back into production in a safe manner
- Perform system validations
  - Run vulnerability scanners
  - Carefully check application and device logs
- Use network and host-based intrusion detection systems to monitor reoccurrence of attack
- Apply any newly identified mitigation techniques

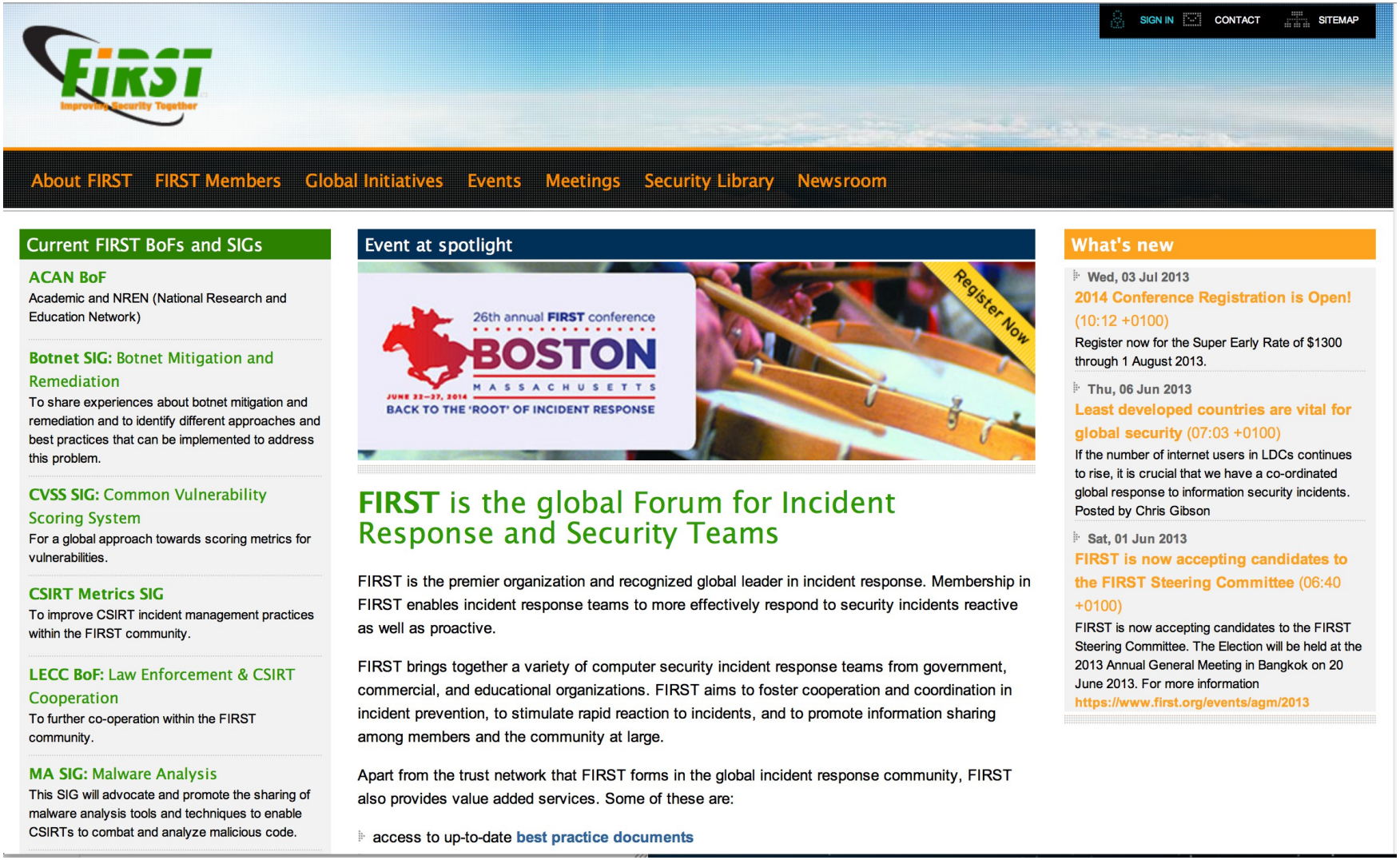
Post Mortem

- A post mortem will help analyze the event after normal operations has resumed (and people have caught up on sleep)
- Have the meeting soon after the incident passed so everyone has details fresh in their minds
- Do NOT blame anyone for doing something incorrectly
- The primary goal is to address lessons learned and not make the same mistakes next time
- What can you do to make recovery faster, easier, less painful in the future?

Do You Have A CIRT?

- You should have a Computer Incident Response Team established
- Who is part of this?
- What are their responsibilities?
- Important – define a single individual to be in charge of final decisions (also have a backup for this individual)
- Know who you need to contact
  - Legal / regulatory responsibility
  - Upstream ISPs who may help filter on DDoS attacks
  - Impacted individuals

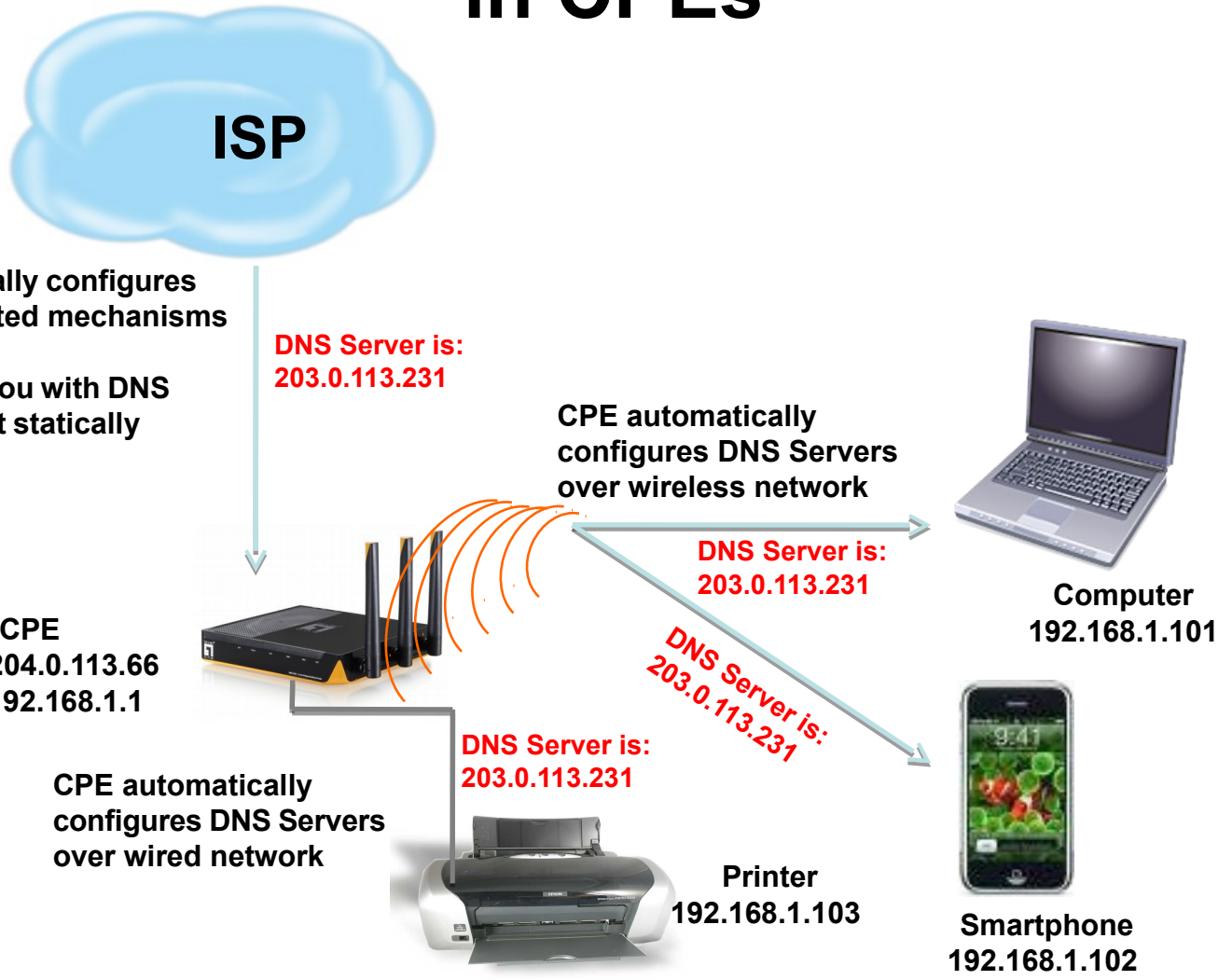
If you have a CIRT Team…..



Examples of Sophisticated Attacks

- DNS Changer
  - Install malware on PCs and MACs, changes the DNS, and tries to reconfigure the home gateway's DNS.
  - Point the DNS configurations to DNS resolvers in specific address blocks and use it for their criminal enterprise.
- BroBot DDoS
  - Computers linked to high-bandwidth websites and web-hosting data centers compromised mostly thru outdated versions of Joomla, WordPress and cPanel applications.
  - Then near-invisible code is embedded onto these hosts into the extensions' HTML
- DNS Amplification DDoS
  - Utilize forged (spoofed) traffic and unmanaged open recursive resolvers to launch large bandwidth attacks

How DNS Servers Are Assigned in CPEs

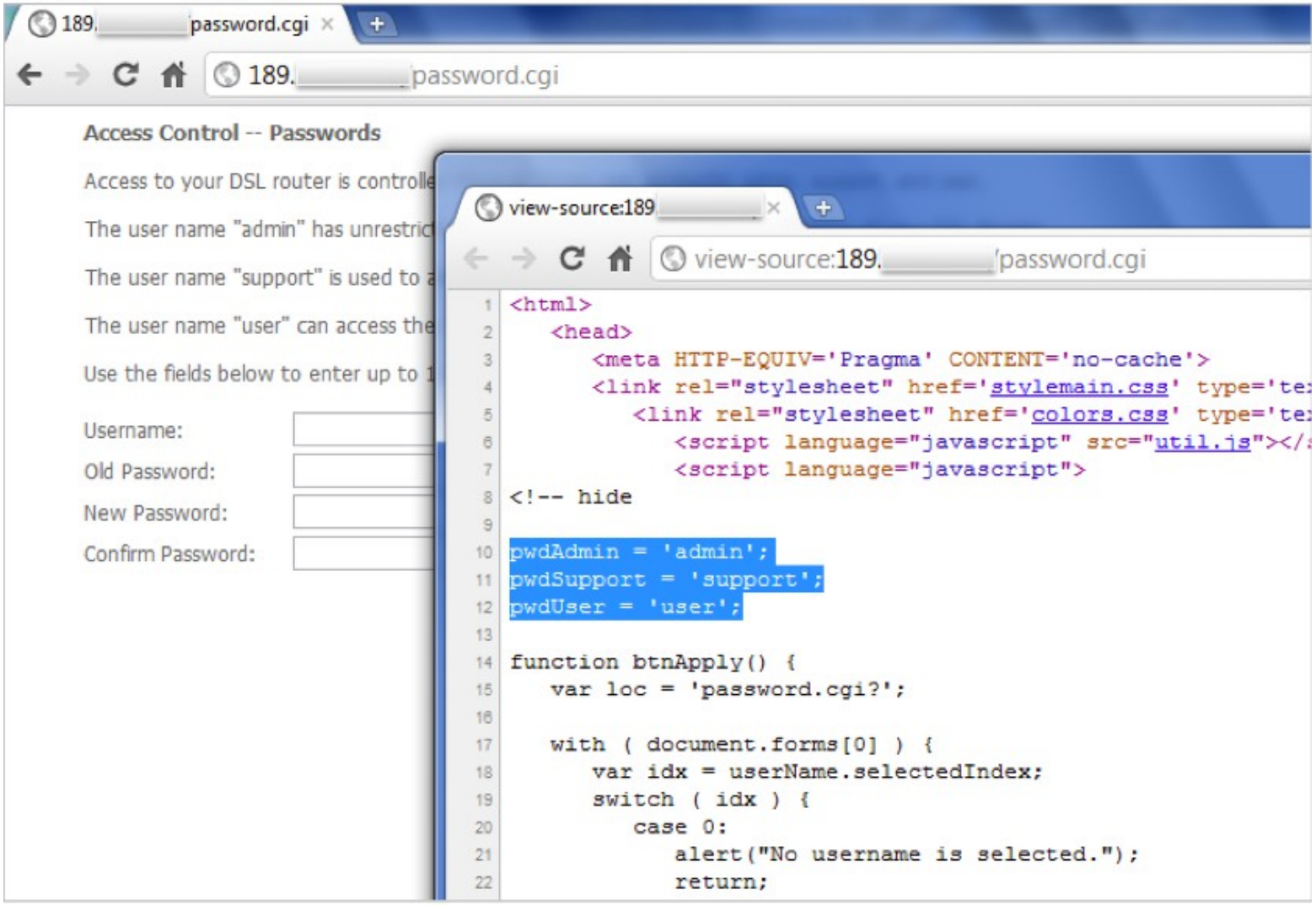


How easily can CPE DNS Server be compromised?

Think of ALL Devices

- The following problem was reported last year and affects low-end CPEs (ADSL connections only)
  - Admin password exposed via web interface
  - Allow WAN management (this means anyone on Internet)
  - Bug fixed and reintroduced depending on the firmware version
- The bug is quite a number of years old

Password Visible via Web Interface



How CPEs Exploited

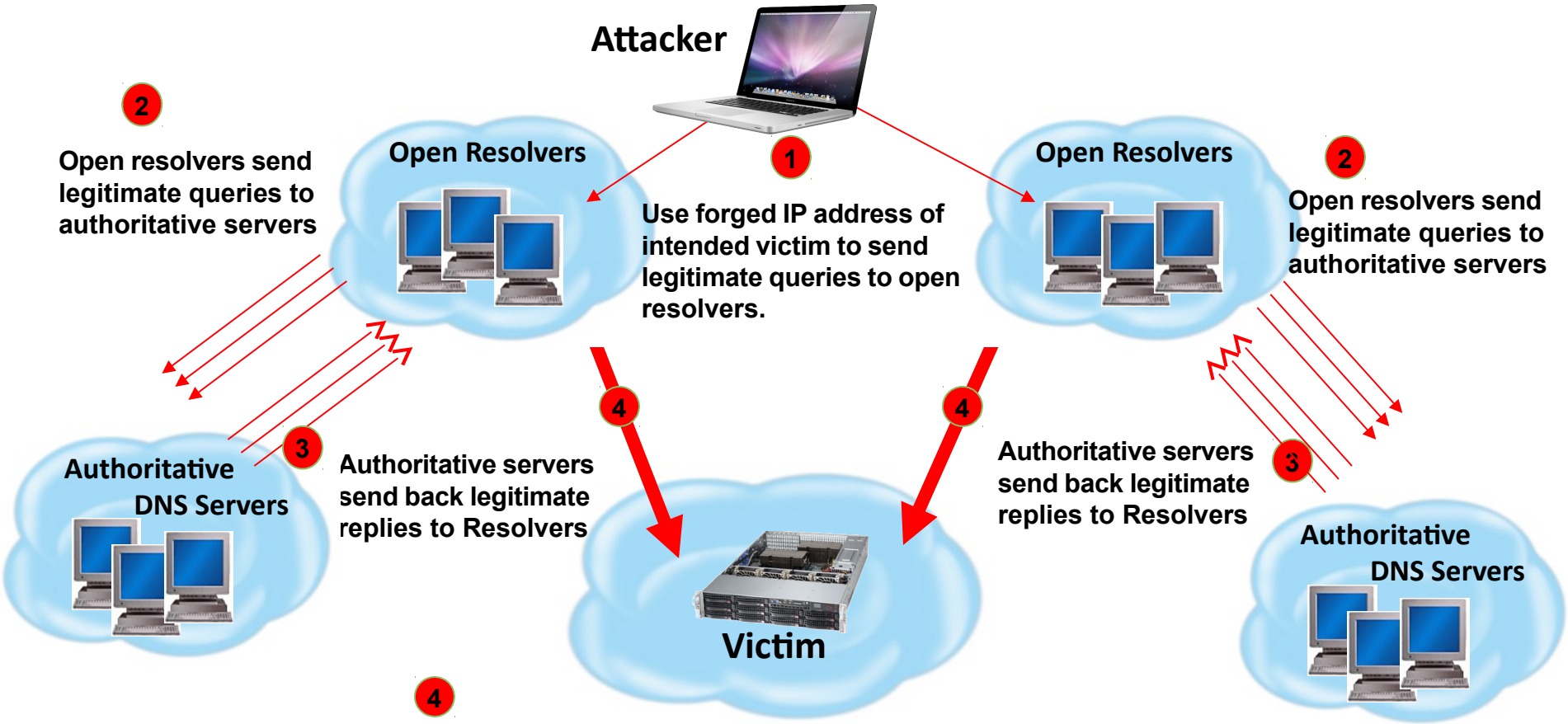
scan → Find vulnerable CPE → Change password (PW=0Wn3D) → Change CPE DNS Servers (DNS=bad server) → DNS incorrectly resolves names for high profile sites → redirected to a page with links to a malware that disables banking protections → Once the protection is disabled, DNS incorrectly resolves names for several banks (for short periods of time)

Magnitude of Problem

- 4.5 Million CPEs (ADSL Modems) using a unique malicious DNS
- In early 2012 more than 300,000 CPEs still infected
- 40 malicious DNS servers found

Could device hardening have made a difference?
(We will discuss this in another module)

Open Resolver Amplification Attack Utilizing Forged (Spoofed) IP Addresses



4 Open resolver legitimate responses create massive DDoS attack to victim's IP address.

What Is Your Next Move?

Thank You!