Cyber Attack Scenario Overview

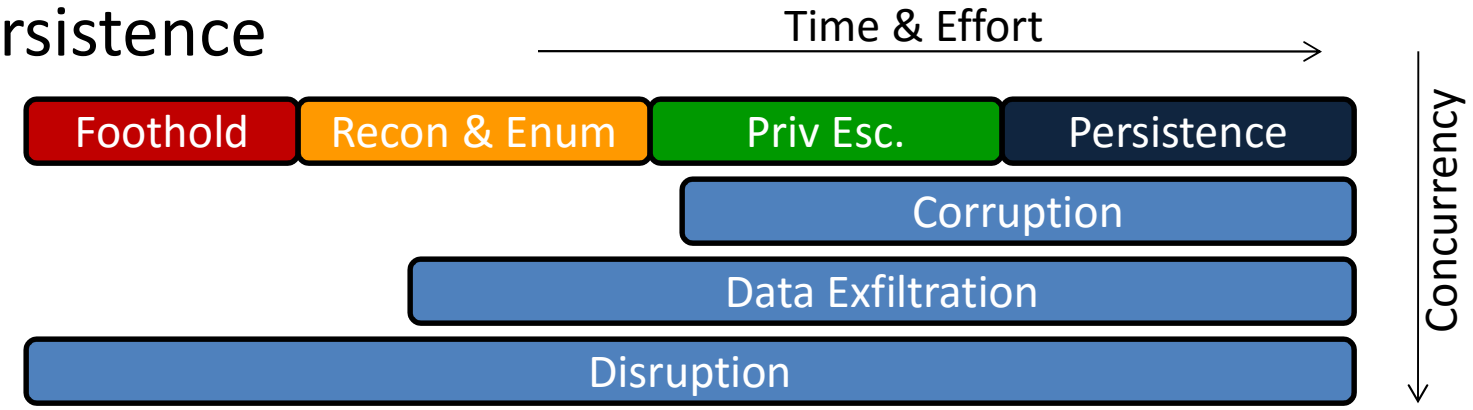
Based on SROC class given by Hervey Allen, Chris Evans, and Phil Regnauld 2009 Santiago, Chile

Overview

- Cyber Attack Categorizations
- Cyber Attack Demonstration Structure

Cyber Attack Categorization

- Foothold
- Reconnaissance & Enumeration
- Privilege Escalation
- Corruption
- Disruption
- Data Exfiltration
- Persistence



Cyber Attack Categorization

- Foothold
  - Initial attempts to access and establish a remote connection into the network
  - Phishing Email with Malware Attachments
  - Website Hosted Malware Installations

From: "networksolutions.com Tech Support" <customerservice@networksolutions.com>

Date: October 29, 2008 1:48:14 PM PDT

To: [redacted]

Subject: Attention: domain will be expired soon.

Dear Network Solutions Customer,

This is a fraudulent email

We recently notified you that the registration period for your Network Solutions domain name had expired. As a benefit of having previously registered a domain name(s) with Network Solutions, you are eligible to receive a percentage of the net proceeds that were generated from the renewal and transfer of the domain name you chose not to renew. Since you have chosen not to renew the domain name listed below during the applicable grace period, we were successful in securing a backorder for this domain name on your behalf and it has been transferred to another party in accordance with the Service Agreement.

Renew your domain now - http://www.networksolutions.com <http://www.networksolutions.com.com42.asia>

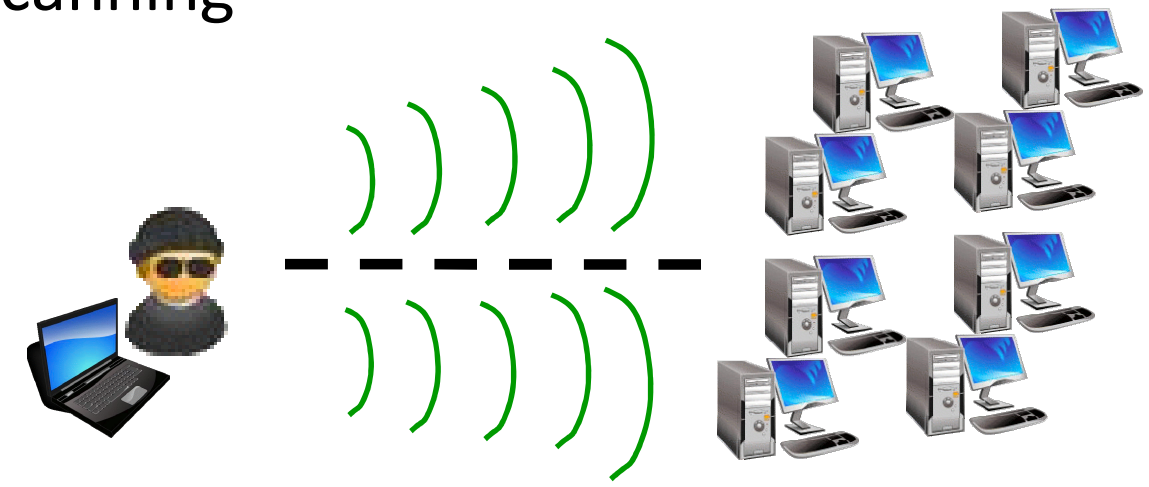
You must click on the following link, enter your domain name, and confirm your contact information in order to claim these funds. If your contact information is not correct, you must enter Account Manager and make the appropriate changes prior to clicking "submit" from the confirmation screen. If you do not do this, you will be confirming inaccurate information and will not receive any payment. Checks will only be made payable and mailed to the Account Holder of record.

Sincerely,

Network SolutionsŽ Customer Support

Cyber Attack Categorization

- Reconnaissance & Enumeration
  - The act of scanning a network to determine its layout, hosts, services, users, and other information which may be useful in a cyber attack
  - Network Mapping
  - Port Scanning



Cyber Attack Categorization

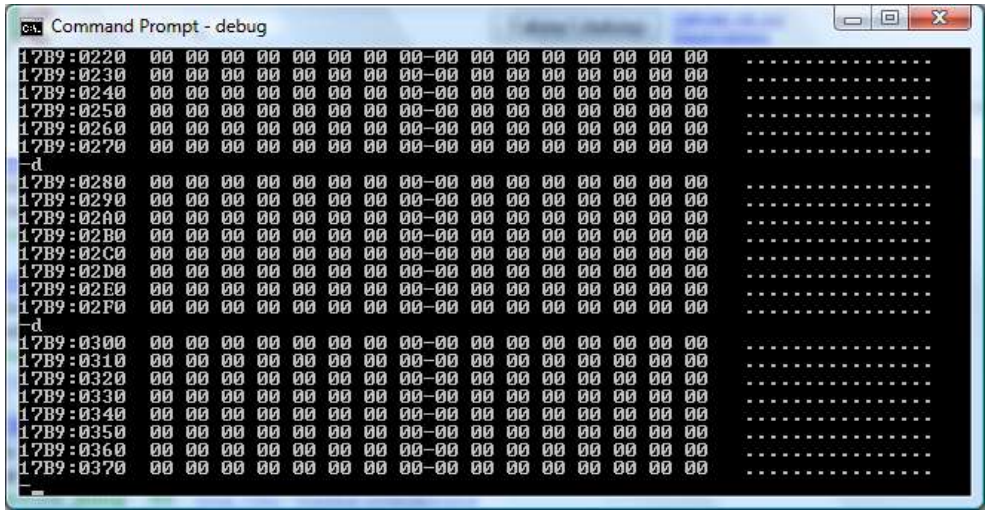
- Privilege Escalation
  - Obtaining credentials, beyond what is normally available, for the purpose of accessing systems or information
  - Username / Password Cracking
  - Social Engineering

MetaSploit

Cyber Attack Categorization

- Corruption
  - Modifying information or content on a system or application
  - Website Defacement
  - Cache Poisoning

01110100101

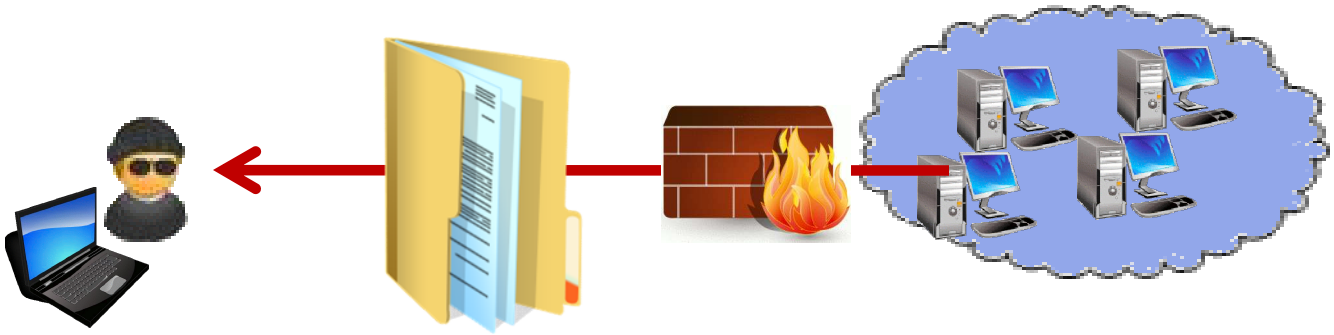


Cyber Attack Categorization

- Disruption
  - Denying, degrading, or otherwise limiting the availability of services provided by a system or application
  - Packet Floods
  - Deleting Operating System Files

Cyber Attack Categorization

- Data Exfiltration
  - Copying data, that is not publicly accessible, from a network for malicious purposes
  - "Smash & Grab"
  - Corporate Espionage



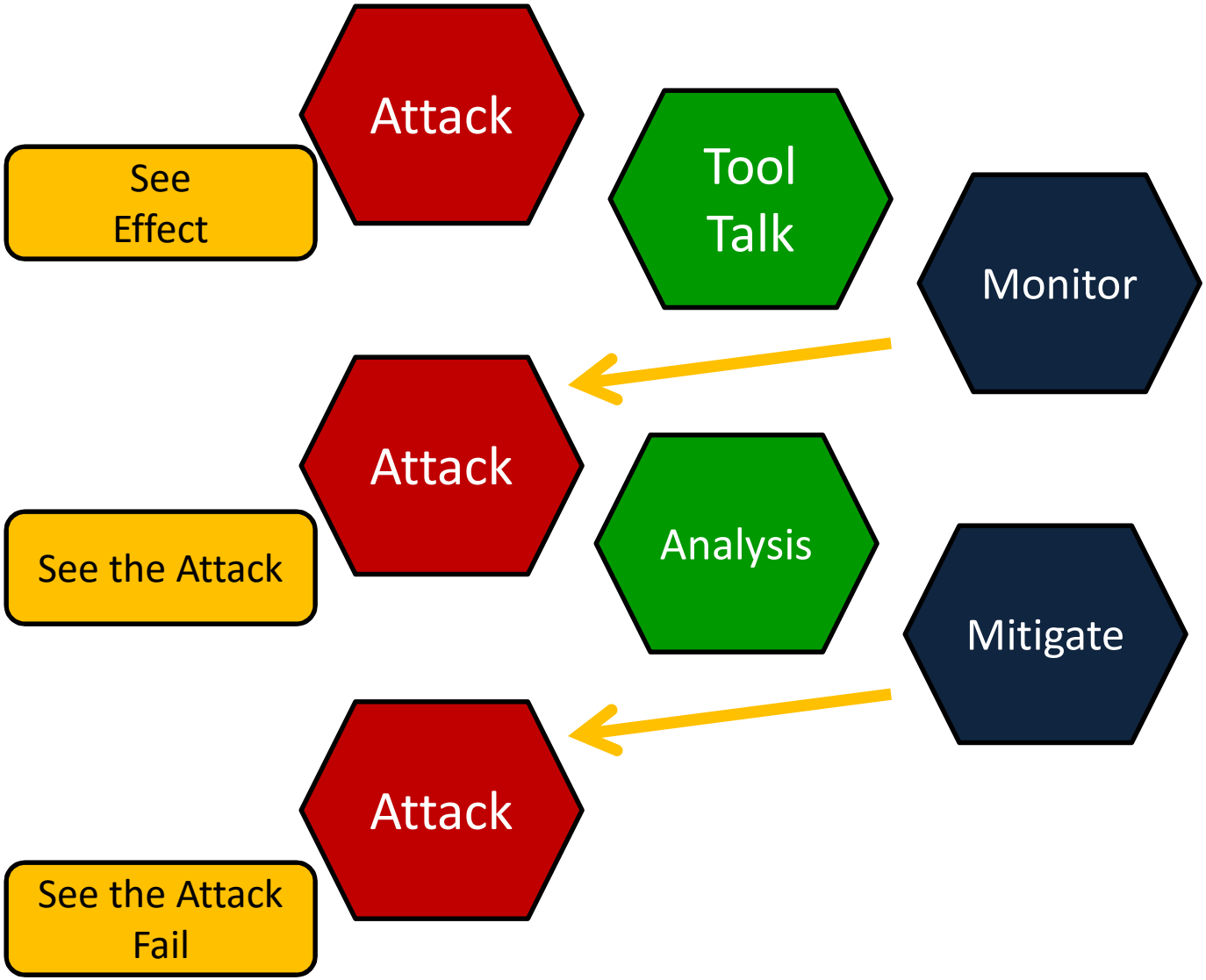
Cyber Attack Categorization

- Persistence
  - Establishing an unauthorized, constant, presence on the network and thwarting administrator removal attempts
  - Root Kits
  - Monitoring Administrator Actions

Cyber Attack Demonstration Structure

- How the cyber attacks will be demonstrated:
  - Attack Demonstration (Round 1)
  - Discussion of Monitoring Tools
  - Installation, Configuration, Operation of Tools
  - Establishing a Baseline
  - Attack Demonstration (Round 2)
  - Analysis of Results
  - Discussion of Response & Recovery Actions
  - Enact Response / Recovery Actions
  - Attack Demonstration (Round 3)

Cyber Attack Demonstration Structure



QUESTIONS?

- Do you have any questions about …
  - Cyber Attack Categorizations
  - How the Cyber Attacks Will Be Demonstrated to You?