**Red Team**

**Concept:** Exploitation of an enterprise-style network with approximate knowledge of design.

**Setting:** Immortals, Inc., is a mid-scale financial services company that provides business services to a number of high-profile enterprise clients. They maintain a large amount of sensitive customer data on internal company servers, which are routinely accessed by engineers as a port of normal job duties. The company also provides a number of services to their customers through a series of Web-facing servers located in a DMZ, including e-mail servers, DNS, and file storage. It is critical that these services remain up and accessible for the company’s clients, whose business continuity depends on these services being Web-accessible.

One of Immortals, Inc.’s most high-visibility clients is the Vanguard Technology Conglomerate, a mega-corporation whose rapid and ruthless acquisition of the technology and information industries has threatened to put hundreds of smaller corporations out of business. Known for buying out the competition then driving up prices, the Vanguard Technology Conglomerate will stop at nothing in its quest to steamroll all who stand in their way.

The very concept of small business, and even the free market as we know it, is at stake.

As members of the Netstalkers private security firm, you have been covertly hired by a group of small technology firms to stop the Vanguard menace. They have provided you with as much open-source information on Vanguard as they can, and will trust in your hacking skills to do the rest. Your goal is to penetrate the networks of Immortals, Inc in order to inflict as much damage on the Vanguard Conglomerate as possible. You know that they have a large amount of critical business files residing on Immortals, Inc’s network, rely on Immortals, Inc’s public-facing services for support, and frequently exchange e-mails with Immortals, Inc. employees for business support.

**Known Information:**

* General network diagram
* Known addressing for public-facing services
* Approximate addressing for user LAN
* Unknown addressing for internal servers and other LAN ranges
* When blue team arrives

**Goals:**

* Acquire and maintain access to network nodes inside of target space
* Establish persistence on accessed devices
* Pivot internally to neighbor devices and networks
* Corrupt, destroy, or otherwise render target data unusable
* Deface, degrade, and corrupt public-facing services supporting target
* Exfiltration sensitive target data
* Avoid detection by defensive personnel

**Blue Team:**

**Concept:** Incident response on a known network with a suspected intrusion of unknown extent.

**Setting:** Immortals, Inc. is a mid-scale financial services corporation that provides business services to a number of high-profile enterprise customers. They maintain a large amount of sensitive customer data on internal company servers, which are routinely accessed by engineers as a port of normal job duties. The company also provides a number of services to their customers through a series of Web-facing servers located in a DMZ, including e-mail servers, DNS, and file storage. It is critical that these services remain up and accessible for the company’s clients, whose business continuity depends on these services being Web-accessible.

Recently, the company’s IT department has been receiving a higher-than-normal amount of support requests related to Internet connectivity and slow workstation performance on the internal enterprise network. An IT admin sent to investigate discovered several unknown files present on multiple users’ desktops, all of whom admitted to opening an attachment from e-mails that were sent from an outside address. While all of the company’s external-facing services remain accessible, some of them have also been displaying irregular behavior.

Immortals, Inc. has requested outside support from Avengers, LLC, to assist with investigation and response into the possible intrusion. Your job, as incident response technicians, is to investigate the scope of the breach, contain it, and secure Immortals, Inc’s networks against future compromise.

**Known Information:**

* Fairly accurate network diagram of company IT environment
* Accurate addressing of user, admin, and DMZ LANs
* Inaccurate addressing of internal servers with inaccurate accounting of services
* Standard profile of user activity and connections
* PCAP from known-good network traffic
* PCAPs on a 20-minute interval following team’s arrival

**Goals:**

* Determine the scope and scale of the compromise
* Determine which, if any, sensitive files have been accessed and/or exfiltrated
* Contain spread of actor’s access to the network
* Eradicate actor presence on enterprise network
* Secure and harden company’s networks and devices against future compromise
* Maintain and/or restore public-facing services
* Maintain Internet connectivity for network
* Determine adversary’s intent, if possible