Analysis Training Scenarios Documentation

Angela Horneman
Tim Shimeall
Timur Snoke

Contents

Rules of the Game 3

Introduction 3

About Me 3

- Who am I 3
- Knowledge in My Head 4
- What I do When I get to the Office 4

Company Info 4

- Executives 4
- SOC Team in the Org Char 4

IT Documentation 5

- Asset Info 5
- Service Information 5
- IT Contact Info 5
- Network Diagram 6

Rules of the Game

These scenarios have been created to illustrate various concepts covered in the "How to be an analyst" training. For all scenarios, you are an employee of the same company. You are described in "Who am I". The company is described in "Company Info". Please read these before beginning.

The goal of each scenario is to work through a cyber event and achieve a reasonable outcome. Throughout the scenario, there will be several tasks and decisions. To keep things simple and not require any special knowledge of tools, some tasks will be partially completed for you. Each task is assigned a theoretical "time spent" value. Not all tasks are necessarily required to achieve the desired outcome. Choosing which tasks to complete is part of the fun. If you do not initially complete a task, but later find out you need to do so (or redo a task) you can go back and do so. Each decision is assigned a "quality" value. Your objective is to maximize the quality score and hit a target time spent score. The target time spent score is based on completing only the tasks that contain the information or results required to maximize the quality score.

Please do not read through the whole scenario before executing tasks or making decisions! We were technologically and development time challenged so we could not implement something that would force you into working through the scenarios in order.

Additional information (hint, hint, environmental context) for the company is in the Documentation directory. Consulting these documents do not affect your time spent score, but they may improve your quality score.

Introduction

You've worked through your morning routine. After reading the morning reports, checking your email, and going over all your dash-boards, you have discovered three potential issues that you need to address. You have prioritized them as:

1. Major DNS usage increase
2. Phishing email you received
3. Well-known cyber group blabbing threats against the company

You can work through them by opening the relevant notebooks. Have a good day, or should I say happy saving the company!

About Me

Who am I

Name: Alex Smith
Role: SOC team lead, day-shift; tier-3 analyst

Team mates: Four tier-1 analysts, one tier-2 analyst, one threat intel analyst
Boss: Jody Jones, SOC manager
Favorite color: Yellow, on my toes
Coffee: Dark and black
Quirk: Color codes everything

Knowledge in My Head

Most useful threat intel sites: OnTopOCyber.org (great source of explanations); Industry-ISAC.com (great source of indicators)

Least useful threat intel sites: CyberSecTimes.com (only parrots least useful information of other sites); Round-about-security.net (round-about in a bad way)

What I do When I get to the Office

1. Read hand-off report from night-shift
2. Get coffee and talk with night-shift team lead and SOC manager
3. Check and categorize email
4. Look over event dash-boards
5. Check out server trends dash boards
6. Decide if anything beyond the normal needs handled
7. Meet with team

Company Info

Size: 500+ employees
Locations: Omaha, NE; Lexington, KY(Central Time)
Industry: Legal services
Culture: Laid-back, managers are approachable, expectation that employees take initiative and when they see things that need done they do them

Executives

CEO: Bob Acme
CIO: Sam Lee
CISO: Sam Lee
COO: A. J. Miller

SOC Team in the Org Char

```
CEO: Bob Acme
|
CISO: Sam Lee
|
Security Manager: Jesse Williams
|                    |
Day Team Lead:       Night Team Lead:
Alex Smith           Taylor Brown
```

IT Documentation

Asset Info

Desktops run Window's 10
HTTP/HTTPS internal server is RHEL.
HTTP/HTTPS public server is CDN hosted. Content mirrored from internal server.
SSH server is RHEL. Assessible to internal and remote employees only.
NTP is Debian. Syncs with the pool.ntp.org.
DNS internal server is RHEL.
DNS external server is CDN hosted.
Email servers are Microsoft Exchange.

Service Information

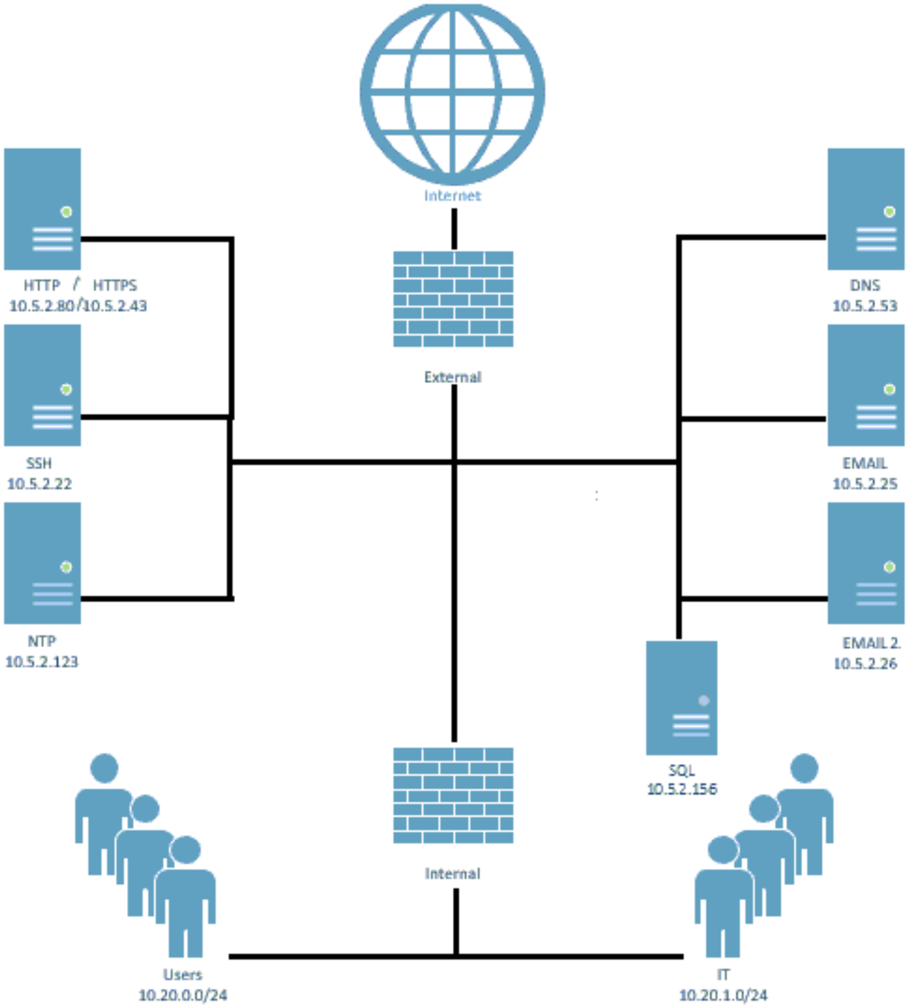
CDN provider is Smoke Screen Providers.
-Account number: 2793246345409
-Hosting contract expires: 08/09/2019
-Domain expires: 08/09/2021
-Contact info: 555-123-8765
-Contract summary:

Smoke Screen Providers (SSP) will maintain a 99.95% up-time for web and DNS services, less scheduled maintenance. To achieve this requirement, SSP will monitor the hosted website and DNS server for unauthorized access. SSP also provides DDoS protection guaranteed to be adequate up to 100Gbps.

IT Contact Info

Desktop Services: x7653
Shared Resource Services: x7624
Password Resets: x7611
Web Administration: x7680
Email Issues: x7625

Network Diagram



This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

DM18-1387