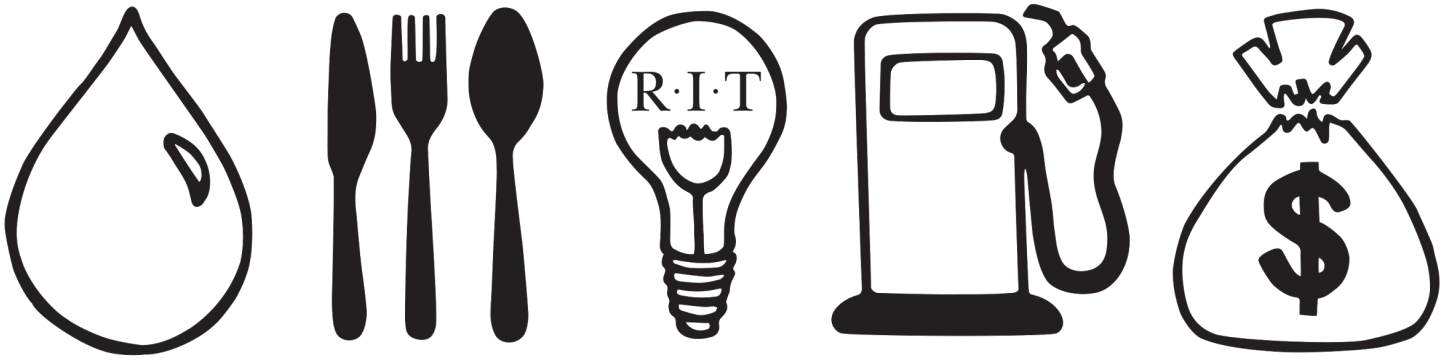


ISTS XV SPARSA

SPARSA's Information Security Talent Search 15

Blue Team Packet

3 March 2017 - 5 March 2017

Silver Sponsers

MITRE

COBALT STRIKE
ADVANCED THREAT TACTICS FOR PENETRATION TESTERS

CS
CARVE SYSTEMS, LLC

CRYPSIS™
RESPOND • PREVENT

amazon

Bronze Sponsers

SMP

indeed®
How the world works.™

SIG®
SUSQUEHANNA

box

FACTSET

R·I·T

Networking, Security, and Systems Administration
NSSA

GCCIS

COMPUTING
SECURITY

Agenda 4
Scoring Breakdown 5
Topology Information 6
Corporate Network 7
Production Network 7
Theme Explanation 8
Important Topology Information 10
Virtual Machine Credentials 11
Bank Account Information 11
Alarm System Information 11
Important Addresses 12
Functional Services 12
Scored Services 12

Agenda

Friday (GCCIS Auditorium, 70-1400):

- Opening remarks 6 - 8pm
  - White team remarks 6:30 - 7pm
  - Keynote 7 - 8pm

Saturday:

- Breakfast 8 am
- Competition start 9 am
  - Lunch 12 pm
  - *Competition breaks for lunch*
- Competition end 6 pm
- Mixer, Salsarita's 7pm -10pm
  - (Global Village Plaza, Building 400. *Right outside of Innovation center*)

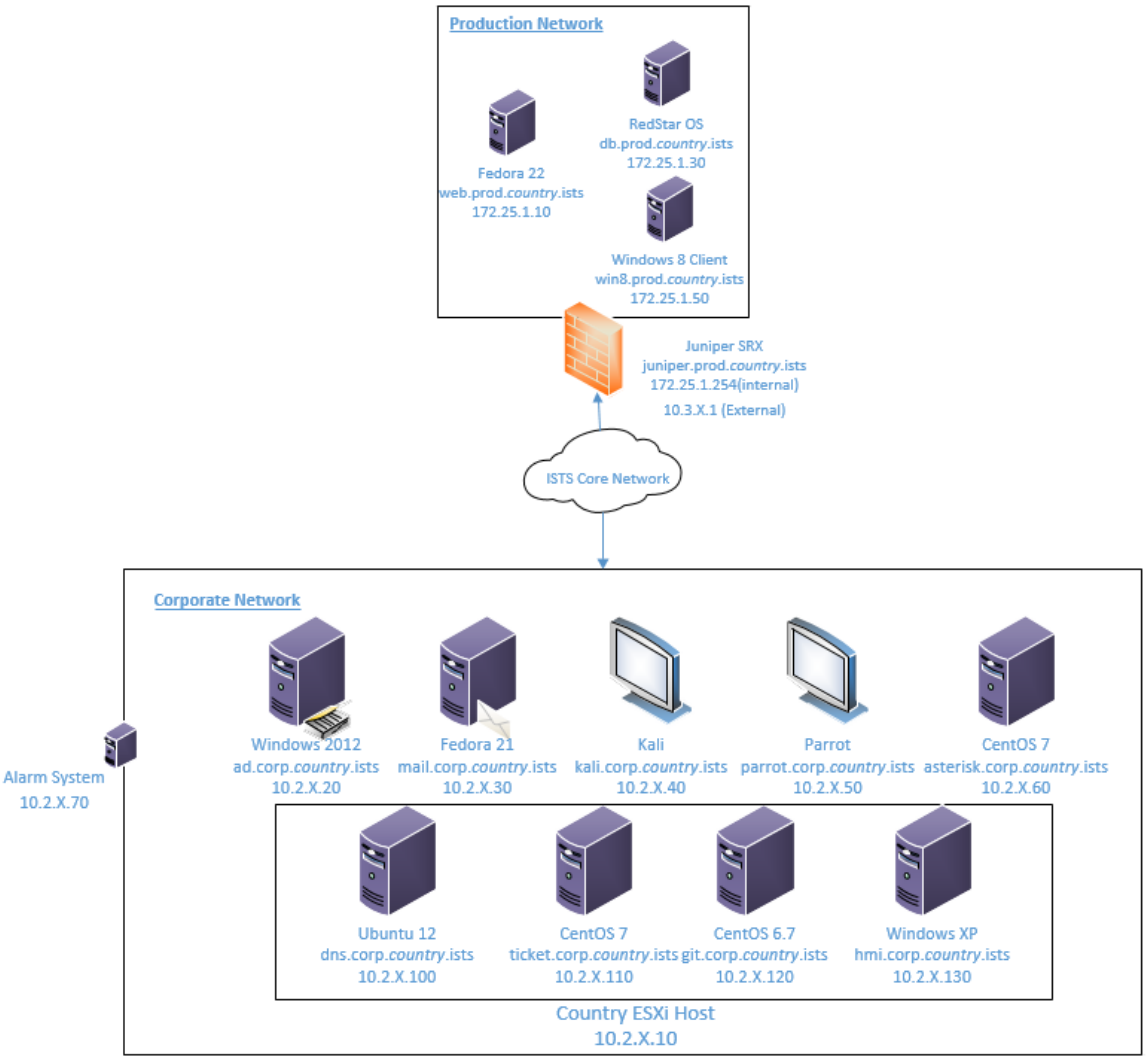
Sunday:

- Breakfast 8am
- Competition start 9am
  - Lunch 12 pm
  - *Competition breaks for lunch*
- Competition ends 2pm
- Ceremony of champions 2:30pm

Scoring Breakdown

- 25% Injects
    - You will be given tasks that must be completed within a given timeframe. Additionally, white team may verify that your functional services (listed below) are working. You will be given points for successful checks of functional services. Additionally, if white team is unable to verify that the functional service is working, you may receive a phone call and must be prepared to troubleshoot issues with the service.
- 15% Challenges
    - A Jeopardy style scoreboard will have challenges for teams to complete.
- 40% Service uptime
    - A scoring engine will verify that the scored services (listed below) are working at regular intervals. Teams will be awarded points for each successful check. Additionally, teams will be paid a percentage of money (directly transferred to their fed account) based on uptime. For example, if teams are paid $1000 every 20 minutes and that team has a combined uptime of 70% between all services over that period of time, the team will receive $700.
- 20% Attack challenges
    - An “attack bucket list” sheet will be provided to each team the day of the competition.

Topology Information



Corporate Network

Domain: corp.*country*.ists

Host (Hostname)	IP Address
ESXi (esxi)	10.2.X.10
AD/DNS (ad)	10.2.X.20
Mail (mail)	10.2.X.30
Kali (kali)	10.2.X.40
Parrot (parrot)	10.2.X.50
VoIP (asterisk)	10.2.X.60
Bind DNS (dns)	10.2.X.100
Ticket System (ticket)	10.2.X.110
Git Lab (git)	10.2.X.120
Human Machine Interface (hmi)	10.2.X.130

Production Network

Domain: prod.*country*.ists

Host (Hostname)	External IP Address	Internal IP Address
Web Server (web)	10.3.X.10	172.25.1.10
Database (db)	10.3.X.30	172.25.1.30
Windows 8 Client (win8)	10.3.X.50	172.25.1.50
Juniper SRX (juniper)	10.3.X.1	172.25.1.254

Theme Explanation

Inspired by your favorite turn based strategy game, Civilization. We present to you Sid Meier's ISTS XV. You are a country. You must defend your country from foreign adversaries, while also ensuring your population is safe. Once every hour a natural disaster will hit your country. These will vary and be specific to a resource. For example, a famine may hit, if you don't have the food resource, your country will incur a monetary penalty. These penalties will start small and then increase as the competition goes on. These natural disasters will be announced with a 10-minute warning, so you will have some time to prepare. The overall goal is to get all 5 resources so that you are safe from all natural disasters.

Resources:

- Water
- Gas
- Food
- Electricity
- Luxury

You start off with 2 random resources. Other resources can be obtained through creating alliances or stealing from other teams. These resources are represented by a randomly generated code that is displayed in your web application.

Allies:

As a country, you can become allies with other countries *(teams)*. If you see that a country has a resource you don't, and you have a resource they don't, you can become allies. You then have the option to share your resource with them, as they do with you. You can have a maximum of 2 allies, once you are no longer allies however, you also no longer share the resource. **Note:** you can share a max of one resource per ally

Declaring War:

To attack another country without chance of penalty you must declare war on them. If you did not declare war on a country, and that country can prove that you were the ones who attacked them, you will lose a random resource, and the team that you attacked will gain it.

When attacking countries, an option you have is to try to steal a resource from a team. If you can find out one of their resource codes, you can add it to your web application and it will become yours, the team you steal it from will lose it.

Important Topology Information

- The alarm sensor monitor MUST be able to poll the modbus sensor.
    - If a check is missed, your alarm system will be turned off
    - <u>You do not manage the alarm sensor. You do not have console access to the alarm sensor.</u>

- Everything is authenticating with your domain controller. You probably don't want to firewall that off completely.

- Git Lab hosts the repository for your web app, if you need to make changes to it do so there. The changes will be pushed to production via Jenkins.

- You do not have console access to the Juniper SRX. You must remotely manage it.
    - Try not to reboot it, it can take up to 15 minutes to come back on.

- You manage your own local ESXi server (esxi.corp.*country*.ists). The hosts on that hypervisor are:
    - dns.corp.*country*.ists
    - ticket.corp.*country*.ists
    - git.corp.*country*.ists
    - hmi.corp.*country*.ists

- You will manage your own call server. Your phone number is NN01 where NN is your team number. **Note:** *All calls are recorded.*

Virtual Machine Credentials

(Administrator / root) / changeme15

Bank Account Information

You will be provided a magnetic stripe ATM card. This ATM card has an account number associated with it at the core federal reserve (“fed”). The fed keeps track of the amount of money that your bank can spend. You may query your balance from the fed to see the amount of funds you have available. These funds can be used to purchase various benefits discussed by the white team during the opening talks.

Alarm System Information

You will have an alarm system next to your workstations. Its status will be signified by 2 LEDs on the system, green for on and red for off. This alarm system will protect the “sensitive” document located next to your alarm system. While the system is on, you are safe. When it is off, Red Team is free to steal the documents one at a time. Each document stolen will result in a deduction of points at the end of the competition. 10 documents stolen equates to missing a inject, giving you a reference for how much its worth. You can view the logs/status of the alarm system through the HMI server in your corporate network.

Important Addresses

Core DNS: 10.0.1.6
Scoring Engine: scoring.whiteteam.ists
Alarm Sensor Monitor: alarm.whiteteam.ists

Functional Services

Hostname	Public IP	Service	Purpose
ad.corp.*country*.ists	10.2.X.20	Active Directory	Active Directory Auth
asterisk.corp.*country*.ists	10.2.X.60	VoIP	VoIP
git.corp.*country*.ists	10.2.X.120	GitLab & Jenkins	Host web app code and push updates to web server
alarm.prod.*country*.ists	10.2.X.70	Modbus	Alarm Sensor Polling
web.prod.*country*.ists	10.3.X.10	HTTP & SSH	Hosts web application and allows for code to be pushed from Jenkins
hmi.corp.*country*.ists	10.2.X.130	Modbus	Displays info from Alarm Sensor

Scored Services

Hostname	Public IP	Service
ad.corp.*country*.ists	10.2.X.20	AD
mail.corp.*country*.ists	10.2.X.30	SMTP, POP3
parrot.corp.*country*.ists	10.2.X.50	SSH
dns.corp.*country*.ists	10.2.X.100	DNS
web.prod.*country*.ists	10.3.X.10	HTTP
win8.prod.*country*.ists	10.3.X.50	FTP
db.prod.*country*.ists	10.3.X.30	MySQL

If you have any questions about the packet, email us at eboard@sparsa.org

See you soon!