University at Buffalo

Lockdown v12

Sponsored in part by Yahoo!®
& Sponsored by M&T Bank

April 30th, 2022

Blue Team Packet

Competition Schedule:

9:30 AM – 10:00 AM	CHECK-IN
10:00 AM – 10:30 AM	COMPETITION OVERVIEW
10:30 AM – 4:00 PM	COMPETITION
4:10 PM - 4:30 PM	CLOSING REMARKS

University at Buffalo

Competition Scenario

For generations, the Saccenti family restaurant, Vinny's, has been in business and kept their secret recipes hidden from other restaurants. These secret recipes led to the success and popularity of the Saccenti family restaurant. For years, the Saccenti family has been pestered to give up the secret recipes. The family continuously refused.

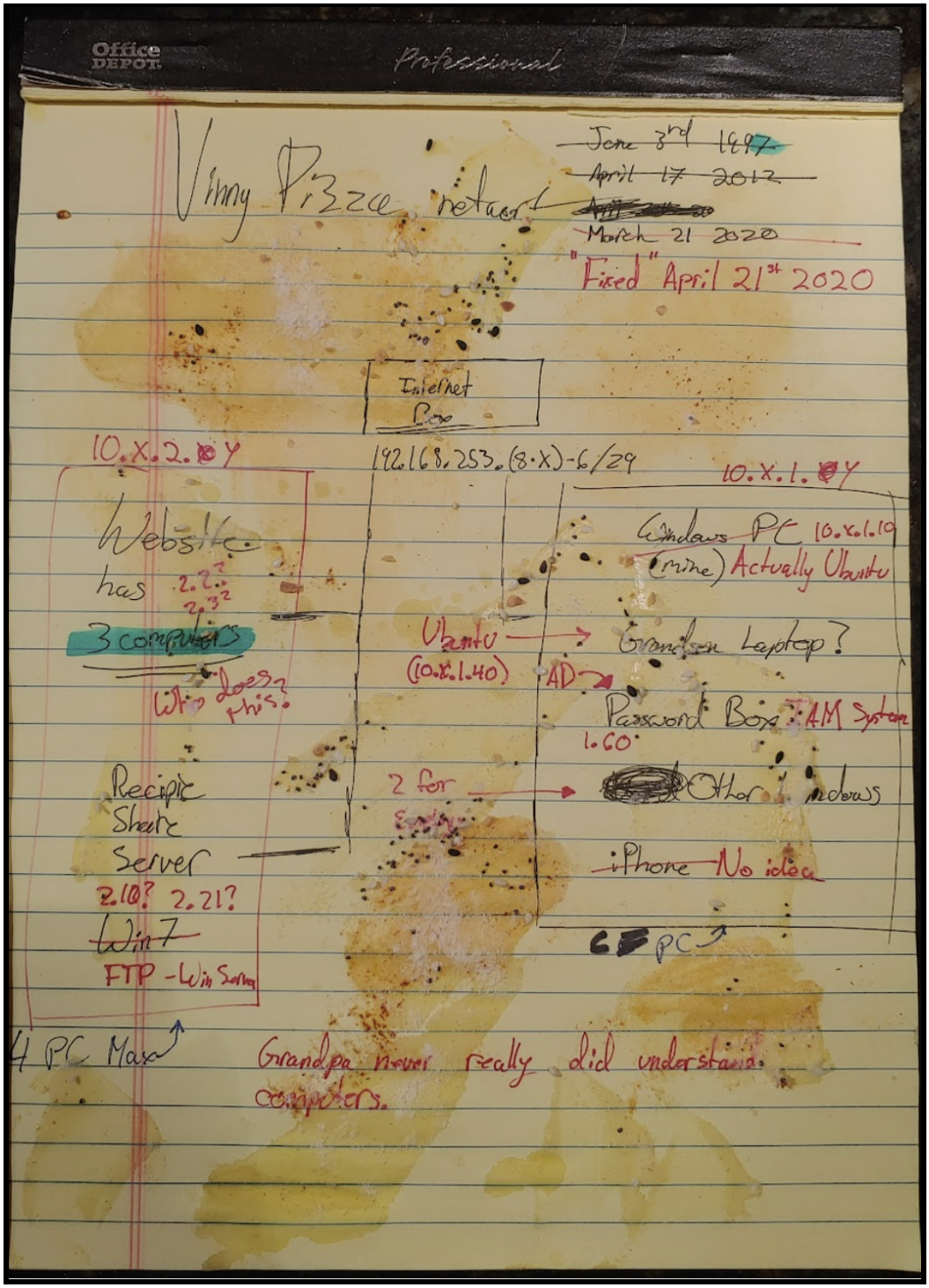
Recently, Vinny's restaurant website and infrastructure was attacked. The family is quite concerned that they are going to lose the family recipes and hurt the business. The family members are very embarrassed by the situation and do not want the public to know.

Vinny Saccenti, who is the current owner of Vinny's, does not know which competing restaurant might be trying to steal the secret recipes. In light of the situation, Vinny has hired your team to investigate the infected machines as well as assist in securing Vinny's network infrastructure. However, the family wants to ensure their systems stay up and running for normal operations.

Vinny Saccenti and the rest of the family welcome you to the team!

University at Buffalo

Network Topology Diagram



University at Buffalo

Scored Services:

Services	Points Per Check
ICMP	1
SSH	2
WinRM	2
LDAP	3
DNS	3
API	4
HTTP	4
MySQL	4
FTP	3

University at Buffalo

Team Identification

Blue Team

This group refers to you and your fellow team members. Your team's responsibility is to secure Vinny's computers and network to prevent attacks, while completing important tasks to keep the restaurant running. Your team must designate a dedicated Team Captain, who is accountable to management and provides direct communication with consultants and business leaders. While your team is rather new and may not have a subject matter expert in any or all of the business operations, you will have the aid (paid and unpaid) from the white team consultants.

White Team

This White Team consists of the consultants that will assist you with your operations. The consultants are available to provide you with advice when needed. The consultants are always available to help, and they do not charge a fee for simple questions. For more involved questions or requests, White Team consultants will potentially charge a fee for their services. Feel free to ask them anything - they are more than happy to help you out to the best of their ability!

University at Buffalo

Red Team

The Red Team is composed of both professional and hobbyist penetration testers. They conduct adversarial operations to the best of their ability and within the context of the competition environment. They have volunteered their time to be your main adversary. Their goal is to assess and exploit the configuration of Blue Team networks and capture specific data items on the targeted devices of each Blue Team. The main aim of the Red Team is to provide a rich educational experience by simulating incidents that may be encountered “in the wild”.

Black Team

The Black Team deploys and manages the underlying competition infrastructure. They set up all of the virtual machines used in the competition, document the configuration settings, tune the scoring engine, ensure the competition network is and stays functioning properly, and test the environment. They are in constant contact with the White Team throughout the competition, coordinate injects, answer blue team questions, and maintain the overall stability of the competition environment.

University at Buffalo

Competition Rules and Guidelines

1. All participants (competitors, organizers, and volunteers) are expected to behave professionally at all times throughout the duration of the competition. This means treating others with dignity and respect and fostering an open and welcoming environment for all involved. Anyone found to be violating this stipulation will be penalized at the discretion of the competition organizers.

2. All network traffic during the competition is captured and logged. Do not enter any personal credentials unless you are comfortable sharing them with the world.

3. All university and local/state/federal government rules, policies, regulations and laws apply and ultimately supersede competition rules and regulations.

4. You are free to come and go from the competition room, but no outside assistance regarding competition is allowed. What happens in the competition room stays in the competition room (until the event is over, then by all means talk about and review whatever you wish)!

5. All COVID-19 guidelines implemented by the University at Buffalo, the State University of New York (SUNY) and the Erie County Health Department are required to be followed.

University at Buffalo

Scoring

1. Service Uptime: 50% of the Blue Team score will be determined by the uptime of various services within their network and configuration of new services and systems, via inject request. These services *could* include but are not limited to AD, DNS, Web Server, Database Server, and GitLab. Teams will all have access to the scoreboard, which will show which services are currently "up" (meaning reachable and usable) and which are "down" (unreachable and/or unusable). Scoring engine checks occur in a synchronous fashion – each service will be checked once every 20 seconds. System misconfiguration, failure to follow security best practices and red team exploits will most likely result in loss of service uptime points.
    - Remember to update the Scoring Engine with your updated passwords to ensure proper scoring. Red team will NOT attack the Scoring Engine, and it can be freely accessed from your host machines.

2. Injects: An inject is a scored task assigned to your team during the competition. 50% of the Blue Team score will be determined by the successful and quality completion of the injects they are given by the White Team throughout the competition. Completeness counts as does quality. It is expected that written inject submissions will be typed in a professional report/documentation format. Anything you submit inject-wise should be something that you would feel comfortable submitting to your boss at work.

University at Buffalo

Infrastructure

1. The University at Buffalo owns all infrastructure – this includes hardware, software, the hypervisor/VMs, etc. Treat it with respect and take due care to not cause any damage outside the scope of the competition.

2. You are not authorized to revert any VMs to a previous snapshot or template or create your own snapshots or templates. Doing so will result in a significant team penalty. You may ask for this service from the White Team during the competition, however. The White Team will inform you of any penalties at the time of the request.

3. All software used by Blue Teams in the competition must be free and open-source (FOSS) and publicly available to anyone. No personal use or commercial trial software is allowed.

4. Blue team members are restricted from uploading artifacts from the competition to VirusTotal or similar websites.

5. Blue team members are prohibited from the “pre-staging” of scripts or software prior to the start of the competition (i.e. creating a .zip archive and hiding it on Dropbox) unless they are publicly available and free for any competitor and have been publicly published 3 months prior to the competition date. The exceptions to this rule are scripts that are written during the competition and scripts written on paper.

6. You may not touch another team’s infrastructure. Doing so will result in immediate disqualification for your team. If something doesn’t belong to your team, don’t touch it!

7. **Competitors are not allowed to attack other teams in this competition, but certain injects may require tools such as Nmap. You must only use these tools on your own team's network. Any activity that could be construed as attacking or reconnaissance against another team, the University, or an outside entity will result in immediate disqualification for your team.**

8. **You are allowed to collaborate with other teams participating in the competition. All teams will still be individually scored.**

University at Buffalo

Reference Material

- **You will have access to the Internet on your host machines during the competition to use for looking up reference material. You may only use free and publicly available resources. I.e., you may not use paid resources such as support forums or private resources such as unregistered Git repositories or public resources published after three months prior to the competition date.**

- **<u>In-person competitors:</u> Regarding Internet on your host machines – you may not use the host machine Internet for anything unrelated to the competition. This means no Facebook, Reddit, Twitter, etc. (unless specifically allowed by the white team for the purpose of an inject).**

- **Any and all paper-based reference materials (cheat sheets, books, printed PDFs, etc.) are allowed and encouraged. You may use scripts printed on paper for competition..**

- **You are allowed to use scripts, executables, tools, and programs that have been published as a publicly available resource on a public site such as GitHub for at least 3 months prior to the competition date.**

No electronic media are allowed in the competition environment, namely USB drives, external hard drives, CDs/DVDs/BDs, etc. Cell phones and their usage are not allowed during the competition time.

University at Buffalo

Sponsored in part by:

yahoo!

Sponsored by:

M&T Bank