Tracer FIRE 8

Welcome to Tracer FIRE 8! Tracer FIRE is an incident response exercise and simulation designed by Sandia National Laboratories. This is an introduction to the Tracer FIRE 8 scenario as well as the tools that will be used during the workshop. This may be useful to refer back to during the workshop/competition.

The Scenario

Orko Electric Company in Verri Xikon has been hacked. You've been hired as an incident responder to triage the incident. As you perform your forensic investigation, knowing the key players and people invovled may help as you work with the artifacts you are given.

Major actors in this scenario:

```
*Amaya Labankada - CIO at Orko Electric Company
*Ella Beltzetan - Consultant at Orko Electric Company
*Antton Sarea - Head of IT at Orko Electric Company
*Others which will be revealed as you progress through the scenario
```

Certain challenges will provide a link to news articles from Tracer Line on the Tracer News Network (TNN). These articles will give you more insight into the state of affairs at Orko.

Your Laptop

You may be provided with a laptop for this scenario or you may be provided access to a virtual machine. You are welcome to use your own laptops, however, our laptops/VMs are guaranteed to have all the tools you need to solve the challenges. Also, the laptops/VMs contain the artifacts for the Tracer FIRE challenges in the Desktop\Artifacts folder. It is advised that you only operate on copies of the artifacts as opposed to the original artifacts so you avoid accidentally modifying or deleting them.

The artifacts include:

```
* Selected SMTP sessions of emails within employees of the company
* Disk images of three machines immediately after compromise
* Memory images of three machines immediately after compromise
* Packet captures of network traffic going into or out of the corporate netw
ork (note that this does not include traffic between machines in the networ
k)
```

**Please be aware that you will be dealing with active malware. Even if you accidentally run the malware, it won't communicate to any dangerous servers outside of the environment, however, you might ruin your laptop/VM and it will only hinder you from doing the challenges.

**All artifacts (except for the packet captures) are in Pacific Daylight Time (PDT), the timezone of Verri Xikon. Packet captures are timestamped in Mountain Daylight Time (MDT).

The following tools are provided to you to solve the challenges and can be found pinned to the Taskbar, via the Start Menu, or in your Desktop\Tools folder. This list is not exhaustive. There are other tools on the laptop/VM that may be useful:

```
* Wireshark
* Volatility
* Autopsy
* IDA 7.0
* Sublime Text 3
* Exif Tool
* Python 2.7 and Python 3
* carve.py (Python Script for carving out files of SMTP sessions)
* PDF Dissector
* JD Gui
```

You also have access to a Kali Linux 2018.3 VMWare Virtual Machine. Username: root / Password: toor

Live Enviroment

In addition to the static artifacts in the Artifacts folder on your Desktop, you may have access to the corporate environment via an Intel NUC device running a virtualized version of some of the corporate machines. You might want to access the ELK server which contains all the Bro logs indexed. Another server which may help you with the challenges is the GRR Server. Additionally, a network diagram is available to you below.

Remote Desktop Connection

Domain administrator credentials are available to you in order to initiate an RDP connection to the clients:

Username: DC\Administrator

Password: 0rk0@dm1n

The first time you log onto the machines, you'll be asked to change the above password as the passwords have expired since the scenario was enacted. Make sure to share this password with your teammates as they'll need it to RDP into the boxes as well.

Challege Categories

There are five categories in the main Tracer FIRE storyline:

```
* Erge
* Herensuge
* Tartalo
* Odei
* Lamia.
```

Each of these categories will walk you through a single attack chain in Orko Electric Company. The challenges are linear, meaning that you will usually only have one unsolved challenge in each category and will need to solve that challenge in order to unlock the next challenge in that category. The challenge page won't automatically refresh, therefore, you may need to refresh your page periodically as your team solves challenges.

It is recommended that you communicate with your teammates. Explain to them how you solved challenges that way each of you equally know the attack chains.

Scoring System

Tracer FIRE 8 uses a dynamic scoring system. For those who have played in CTFs before, this concept should be familiar.

The rules for scoring are simple:

```
* All challenges start at 100 points each
* As more teams solve a particular challenge, the value of that challenge wi
ll go down
* The minimum value of a challenge is 50 points
```

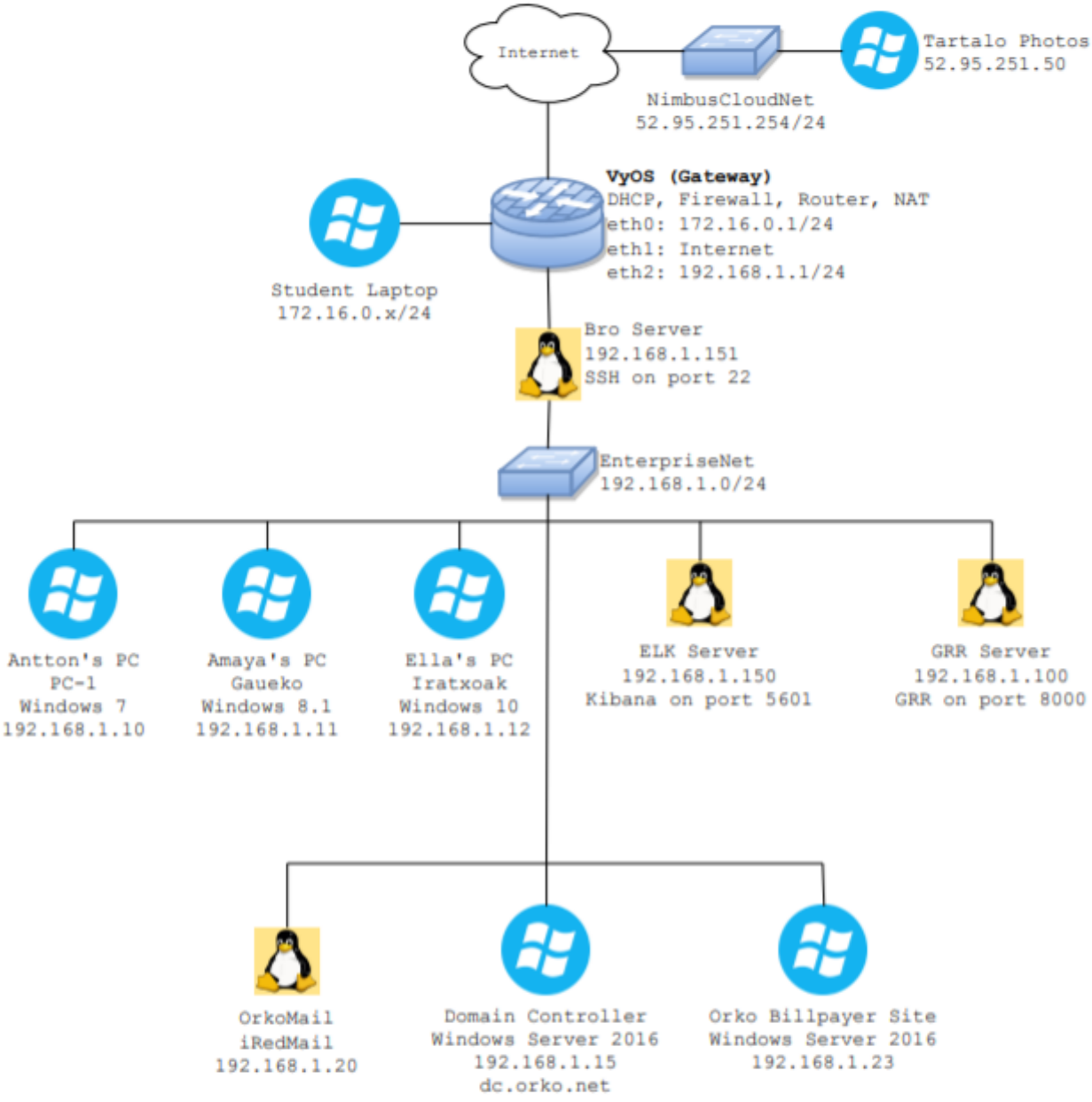
Example:

```
1. Team Gryffindor is first team to solve Herensuge 1. Now Team Gryffindor h
as 100 points.
2. Team Slytherin is second team to solve Herensuge 1. They solved it about
 10 minutes after Team Gryffindor. Now Herensuge 1 is worth 87 points. Team
 Gryffindor and Team Slytherin are now both tied in
point value at 87 points. However, Team Gryffindor is technically in the lea
d since they reached 87 points before Team Slytherin.
```

Final Note

Don't forget to have fun! While Tracer FIRE is run as a competition, you're here to learn. If you get stuck or don't know where to start, don't be afraid to ask someone for help. Be sure to communicate with your team and work together to solve the challenges! Take notes as you solve challenges and make sure you understand what is

TracerFIRE 8 NUC Setup



Orko Domain Users/Passwords:
asarea@dc1.orko.net/LtZsbt5p
ebeltzetan@dc1.orko.net/mWFz9QXF
alabankada@dc1.orko.net/9QQrgLKF

BroServer SSH: ubuntu/Br0R0ck$
GRR Server Web Interface: admin/##0rk0GrrR