TAL TECH

RANGEFORCE

CASE STUDY

How TalTech improved the quality of cybersecurity studies with the RangeForce CyberSkills Platform

Founded in 1918, Tallinn University of Technology (TalTech) is the flagship science and engineering university of Estonia. Located in a region where advanced cyberattacks against both public and private organizations are commonplace, the school provides one of the oldest curriculums for both undergraduate and graduate level cybersecurity studies in Europe.

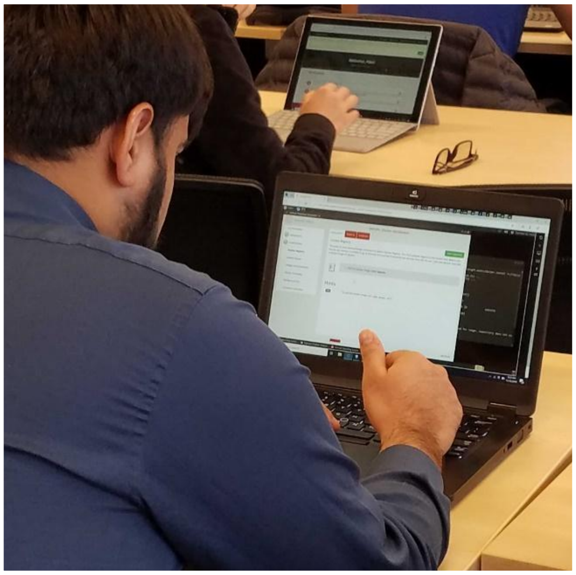
TalTech was forced to expand its cybersecurity curriculum to match the unprecedented growth in both computer technology and cyberattacks. This expansion created significant challenges for the school's professors and IT staff, who struggled to create lessons, hands-on learning tools, and supporting IT systems that could keep up with the pace of changing cyberattacks. The existing technology used by the school was limited in scale, required long setup times, lacked true hands-on capabilities, and was expensive. Professors spent so much time preparing lesson and evaluations, that little time remained to actually teach students.

This was clearly the wrong direction for the program, and if left unchanged, would hurt both student enrollment to the school, and the quality of training provided by the school. A change in direction was needed.

> "It's a scalable method for the university to evaluate skills and also assess levels of motivation and problem-solving. RangeForce is many times cheaper than building your own cyber range and I don't need to outsource technical help."
>
> TalTech Cybersecurity Lecturer

SOLUTION

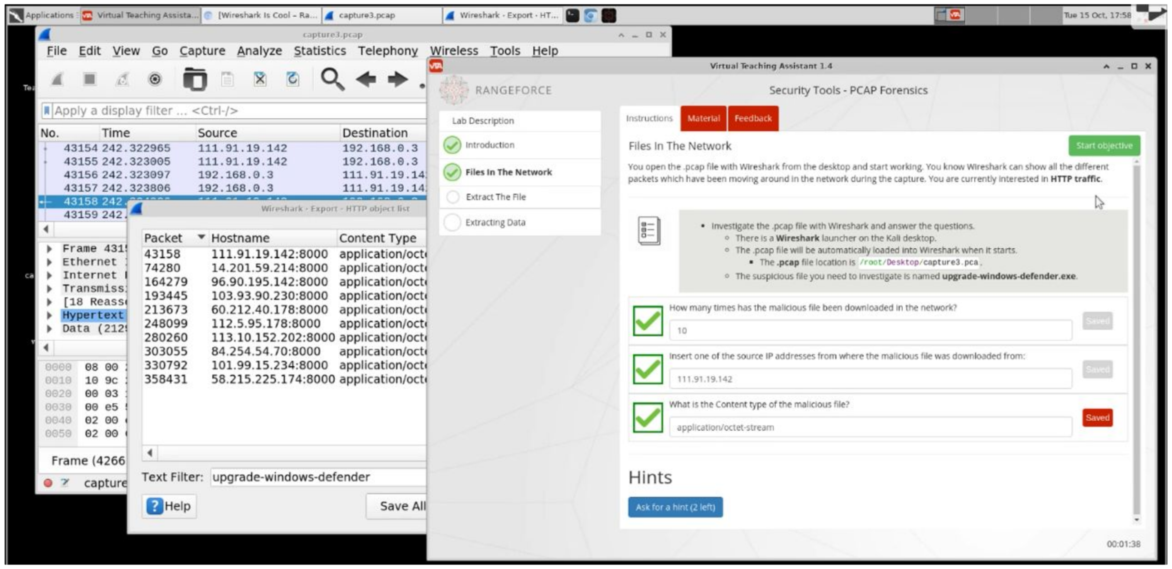
In 2016, TalTech made that change in direction. They implemented the RangeForce CyberSkills Training Platform. The university introduced RangeForce's virtual threat training modules to students as a new hands-on approach to teaching, motivating, and assessing the students cybersecurity skills. By using RangeForce's fully automated online learning capabilities, the school eliminated the factors that were degrading the professors teaching capabilities.



Today, TalTech uses RangeForce to teach and test undergraduate and graduate level students. The system is popular among students who enjoy the interactive gaming nature of the platform and love the challenge of facing off against real cyberattacks. Prior to RangeForce, cyberattacks were merely theoretical discussions based on threat intelligence reports.

Training modules used by TalTech include:

- WASE learning: Path Traversal, Commend Injection, Cookie Security, Insecure Direct Object References, Unrestricted File Upload, XSS, and CSRF Defense.
- Security Tools: PCAP Forensics, NoSQLMap, Password Cracking, Brute-force Defense, and Malware Analysis.
- SOC Learning: System Compromise, Backdoors, and Botnet Takedown.


Applications
Virtual Teaching Assista...
[Wireshark Is Cool – Ra...
capture3.pcap
Wireshark · Export · HT...
Tue 15 Oct, 17:58
capture3.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Wireshark · Export · HTTP object list
Help
Save All
Virtual Teaching Assistant 1.4
RANGEFORCE
Lab Description
Introduction
Files In The Network
Extract The File
Extracting Data
Instructions
Material
Feedback
Start objective
Saved
Ask for a hint (2 left)
00:01:38

```
No.    Time        Source         Destination
 43154 242.322965  111.91.19.142  192.168.0.3
 43155 242.323005  111.91.19.142  192.168.0.3
 43156 242.323097  192.168.0.3    111.91.19.14
 43157 242.323806  192.168.0.3    111.91.19.14
 43158 242.
 43159 242.

▸ Frame 431
▸ Ethernet
▸ Internet
▸ Transmiss
▸ [18 Reass
▸ Hypertext
▸ Data (212

0000  08 00
0010  10 9c
0020  00 03
0030  00 e5
0040  02 00
0050  02 00

Frame (4266
capture
```

```
Packet  Hostname              Content Type
43158   111.91.19.142:8000    application/octe
74280   14.201.59.214:8000    application/octe
164279  96.90.195.142:8000    application/octe
193445  103.93.90.230:8000    application/octe
213673  60.212.40.178:8000    application/octe
248099  112.5.95.178:8000     application/octe
280260  113.10.152.202:8000   application/octe
303055  84.254.54.70:8000     application/octe
330792  101.99.15.234:8000    application/octe
358431  58.215.225.174:8000   application/octe

Text Filter: upgrade-windows-defender
```

Security Tools - PCAP Forensics

Files In The Network

You open the .pcap file with Wireshark from the desktop and start working. You know Wireshark can show all the different packets which have been moving around in the network during the capture. You are currently interested in **HTTP traffic**.

- Investigate the .pcap file with Wireshark and answer the questions.
  - There is a **Wireshark** launcher on the Kali desktop.
  - The .pcap file will be automatically loaded into Wireshark when it starts.
    - The **.pcap** file location is `/root/Desktop/capture3.pca`.
  - The suspicious file you need to investigate is named **upgrade-windows-defender.exe**.

☑ How many times has the malicious file been downloaded in the network?
10

☑ Insert one of the source IP addresses from where the malicious file was downloaded from:
111.91.19.142

☑ What is the Content type of the malicious file?
application/octet-stream

Hints

Existing System

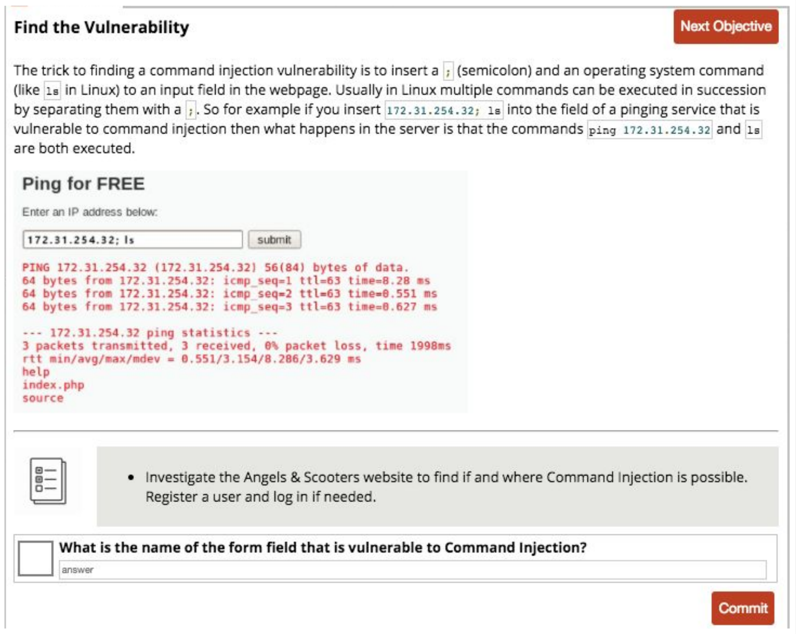
- Long IT setup time
- Limited scale
- Heavy class preparation
- Limited hands-on interaction
- Skills assessment through written tests

RangeForce Platform

- Cloud based virtual machine
- Highly scalable, setup in less than an hour
- Over 80+ training modules ready to deliver
- Totally interactive lessons and skills training
- Integrated assessments reporting

ADMISSION ASSESSMENTS

TalTech is also using RangeForce to assess the skills of incoming graduate students. To be accepted into the prestigious Masters in Cybersecurity program, students must show cyber skills competency by completing two of RangeForce's foundation modules. RangeForce assessments show the student's true capabilities and offer an objective way to evaluate and accept only the best candidates.



Find the Vulnerability

The trick to finding a command injection vulnerability is to insert a `;` (semicolon) and an operating system command (like `ls` in Linux) to an input field in the webpage. Usually in Linux multiple commands can be executed in succession by separating them with a `;`. So for example if you insert `172.31.254.32; ls` into the field of a pinging service that is vulnerable to command injection then what happens in the server is that the commands `ping 172.31.254.32` and `ls` are both executed.

Ping for FREE

Enter an IP address below:

172.31.254.32; ls

```
PING 172.31.254.32 (172.31.254.32) 56(84) bytes of data.
64 bytes from 172.31.254.32: icmp_seq=1 ttl=63 time=8.28 ms
64 bytes from 172.31.254.32: icmp_seq=2 ttl=63 time=0.551 ms
64 bytes from 172.31.254.32: icmp_seq=3 ttl=63 time=0.627 ms

--- 172.31.254.32 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.551/3.154/8.286/3.629 ms
help
index.php
source
```

- Investigate the Angels & Scooters website to find if and where Command Injection is possible. Register a user and log in if needed.

□ **What is the name of the form field that is vulnerable to Command Injection?**

answer

> "Using modules at admissions and in the classroom was a positive experience. It's a transparent and objective approach for showing my cyber skills and assessing my motivation"
>
> Student, Masters of Cybersecurity Program, TalTech

RESULTS

Since 2016, The RangeForce Platform has been used to train over 625 TalTech students. In the days before RangeForce, a professor would spend roughly 80 hours to prepare a cybersecurity course for a class of 100 students. That number dropped by 75% or to less than 20 hours once RangeForce was deployed. The time to assess and grade students also dropped dramatically from around 16 hours per 100 students to under an hour as RangeForce automated the testing and grading process. Today, it only takes a TalTech professor 20 minutes to score and then add student grades to the TalTech reporting portal.

ABOUT RANGEFORCE

RangeForce delivers the industries only integrated cybersecurity simulation and skills analysis platform that combines a virtual cyber range with hands-on advanced cyber defense training. Security and I.T. professionals use RangeForce to qualify their new-hires, training up there DevOps, IT and Security Staff, and run CyberSiege simulations of the latest attack methods to evaluate team.