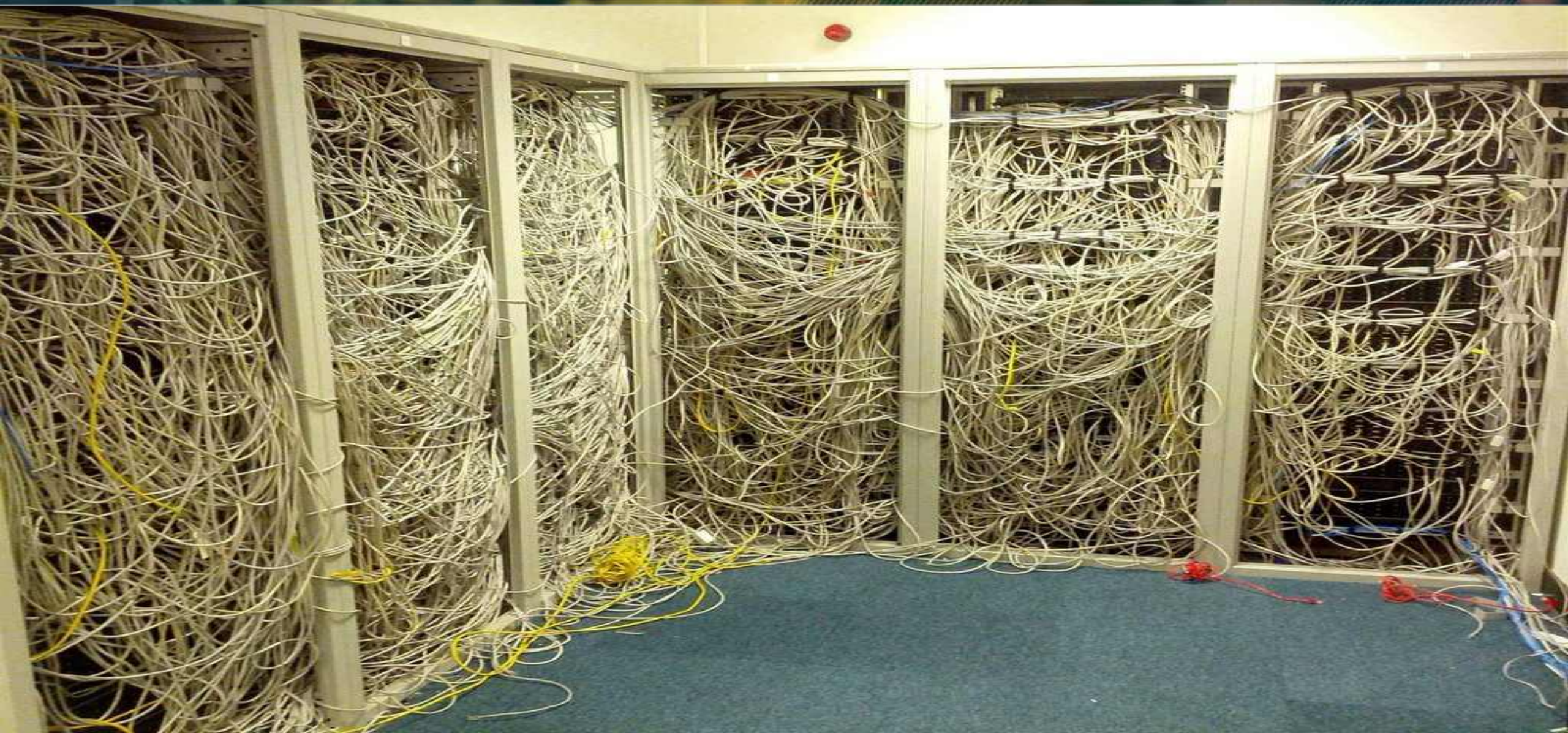
WAT JE TE ZIEN KRIJGT VERSUS DE WERKELIJKHEID

WAT JE TE ZIEN KRIJGT VERSUS DE WERKELIJKHEID



Tale of a Compliance Kettle. (Frank Breedijk)

¯_(ツ)_/¯

SHA2017

STILL HACKING ANYWAY

Are open fires allowed (bonfire, barbecue, ...)?

No, unfortunately not because of safety reason.
Open fire is anything that is not gas powered, allowed are (butane, propane) powered stoves and barbecue grills.

If u are cooking for 1 person we will allow small burners on fuel (like spirit of alcohol) , make sure u cook in the open air! There will however be a official sha2017 organized campfire near the beach, feel free to join.

Please make sure u have a fire-extinguisher in the area.

COMPLIANCE AND SECURITY

Tale of a Compliance Kettle. (Frank Breedijk)

EN DUS?

Introductie van de Compliance Kettle

Regels voor veiligheid tot op de letter gevolgd.

Compliance voegt vaak iets toe aan veiligheid!
Vaak ook niet.

CSX CYBERSECURITY NEXUS BY ISACA

2017 Cyber Security Skills Gap

Cyberattacks are growing, but the talent pool of defenders is not keeping pace.

Although attacks are growing in frequency and sophistication, the availability of sufficiently skilled cyber security professionals is falling behind. ISACA's Cybersecurity Nexus (CSX) is addressing this gap by creating a skilled global cyber security workforce. From the Cyber Security Fundamentals Certificate for university students to CSX Practitioner—the first vendor-neutral, performance-based cyber security certification—and new security training programs, CSX is enabling cyber security professionals at every stage of their careers, and helping enterprises develop strong cyber work forces.

Too Many Threats

MORE THAN 550 MILLION **RECORDS WERE BREACHED** IN THE FIRST HALF OF 2016 ALONE.[1]

$4 MILLION: AVERAGE COST OF A **DATA BREACH IN 2016.**[2]

32% OF ECONOMIC CRIME AFFECTING ORGANIZATIONS IS **CYBERCRIME** MAKING IT THE SECOND MOST REPORTED.[3]

201 DAYS WAS THE MEAN TIME TO **IDENTIFY A DATA BREACH IN 2016**, WHILE THE MEAN TIME TO **CONTAIN A DATA BREACH WAS 70 DAYS.**[4]

97% OF IT DECISION MAKERS SAY THEIR ORGANIZATION'S BOARD OF DIRECTORS NOW **VIEWS CYBER SECURITY AS IMPORTANT.**[5]

Too Few Professionals

THE DEMAND FOR **INFORMATION SECURITY PROFESSIONALS** IS EXPECTED TO GROW BY **53%** BY 2018.[6]

32% OF SECURITY PROFESSIONALS SAY IT TAKES **SIX MONTHS OR MORE TO FILL CYBER SECURITY POSITIONS** IN THEIR ORGANIZATIONS.[7]

MORE THAN 7 IN 10 DECISION MAKERS REPORT THE **SHORTAGE IN CYBER SECURITY SKILLS** DOES DIRECT AND MEASURABLE DAMAGE TO THEIR ORGANIZATIONS BY MAKING THEM **MORE DESIRABLE HACKING TARGETS.**[8]

48% OF ORGANIZATIONS GET **FEWER THAN 10 APPLICANTS FOR CYBER SECURITY POSITIONS.**

64% SAY FEWER THAN HALF OF THEIR CYBER SECURITY APPLICANTS ARE QUALIFIED.[9]

60% OF MEN & **72%** OF WOMEN REPORT THAT NO HIGH SCHOOL TEACHER OR COUNSELOR MENTIONED **CYBER SECURITY AS A CAREER.**[10]

SOURCES: 1. *2016 H1 Breach Level Index, Gemalto, September 2016.* 2. *2016 Cost of Data Breach Study: Global Analysis, IBM and Ponemon Institute, June 2016.* 3. *PwC Global Economic Crime Survey 2016.* 4. *2016 Cost of Data Breach Study: Global Analysis, IBM and Ponemon Institute, June 2016.* 5. *Hacking the Skills Shortage: A study of the International Shortage in Cybersecurity Skills, McAfee, May 2016.* 6. *Demand to Fill Cybersecurity Jobs Booming, Peninsula Press, March 2015.* 7. *ISACA's 2017 State of Cyber security Study.* 8. *Hacking the Skills Shortage: A study of the International Shortage in Cybersecurity Skills, McAfee, May 2016.* 9. *ISACA's 2017 State of Cyber security Study.* 10. *Securing Our Future: Closing the Cyber Talent Gap, Raytheon and NCSA, October 2016.*

CSX CYBERSECURITY NEXUS

ISACA Trust in, and value from, information systems

https://cybersecurity.isaca.org

CSX™
CYBERSECURITY NEXUS

CSX Fundamentals/Practitioner

ISACA®
Trust in, and value from, information systems

ISACA CYBER SECURITY CREDENTIALS

Our holistic program starts with the knowledge-based Cybersecurity Fundamentals Certificate for those who are new to the profession or looking to change careers, and centers on our performance-based CSX Practitioner certification.

For those looking to move into a more managerial role, our Certified Information Security Manager® (CISM) is an ideal solution.

CSX CYBERSECURITY NEXUS BY ISACA

CSX PRACTITIONER

CSX PRACTITIONER SERIES COURSES

The series consists of three unique, week-long courses aligned with existing global frameworks, including the NIST Cybersecurity Framework. Each course is 5 days and combines lecture with hands-on lab time, and includes a 6-month subscription to the labs used in the course.

CSX Practitioner Course 1: Identification and Protection

Focuses on concepts and skills needed to recognize, assess and remediate specific internal and external network threats, and to implement cyber security controls to protect a system from identified threats.

CSX Practitioner Course 2: Detection

Centered on building skills to levearge cyber security controls to identify system events and non-event level incidents, and to detect potential network events and incidents.

CSX Practitioner Course 3: Respond and Recover

This course focuses on skills required to draft and execute comprehensive incident response plans, including maintaining proper isolation and incident response information and documentation.

CSX PRACTITIONER LABS

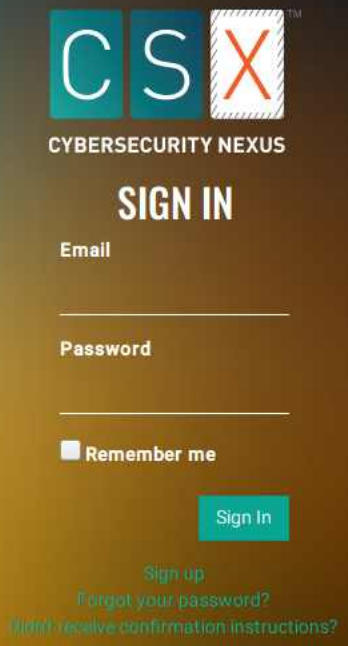
The same labs used in our CSX Practitioner Series training courses are also available for separate purchase, and are an ideal way to practice your technical skills and prepare for the CSX Practitioner certification exam. Access your labs and practice your skills from anywhere you have a high-speed internet connectivity, any time.

Skill to practice:

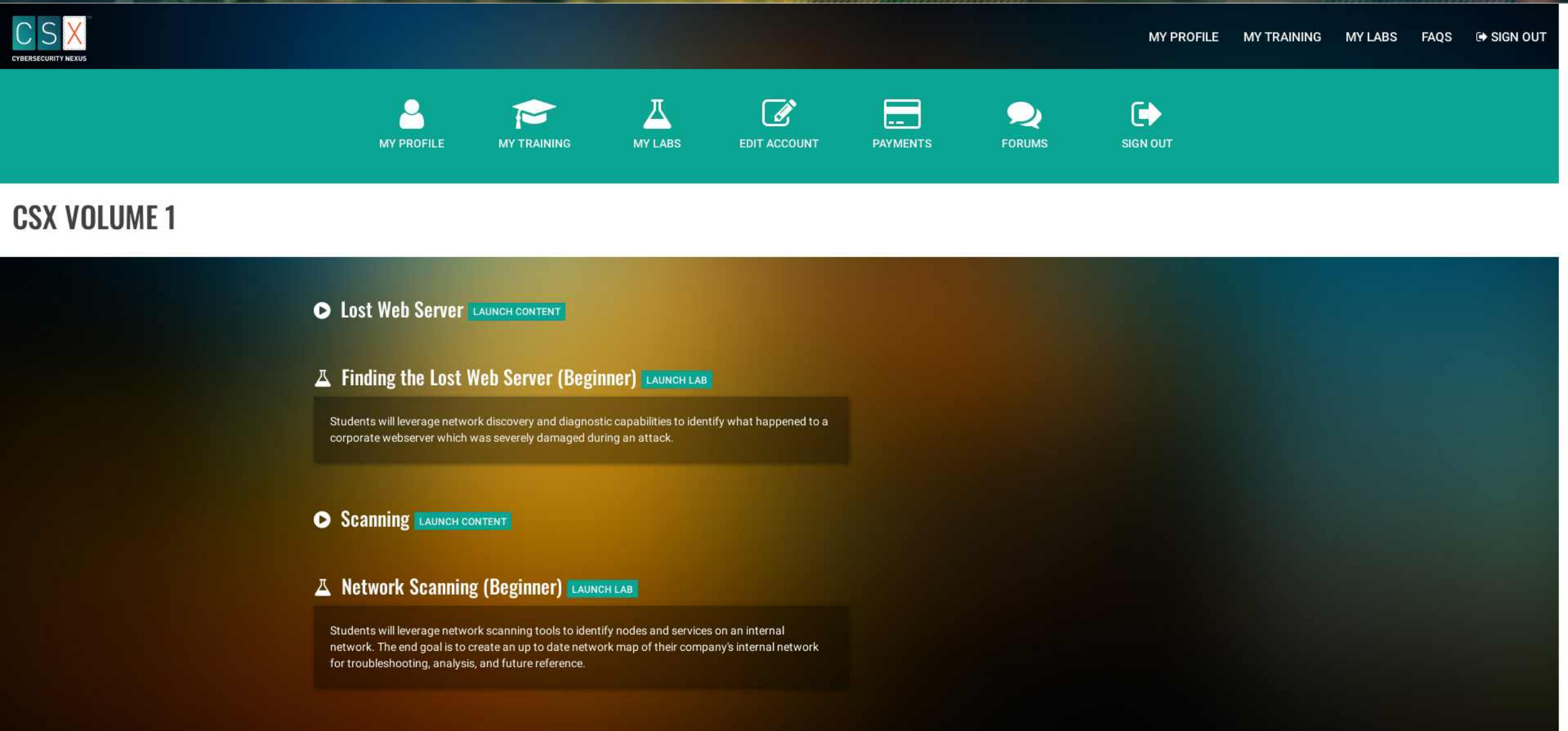
- Network Scanning
- Specialized Port Scans
- Network Topologies
- Network Log Analysis
- Centralized Monitoring
- Hotfix Distribution
- Vulnerability Scanning
- Traffic Monitoring
- Compromise Indicators
- False Positive Identification
- Packet Analysis
- User Account Controls

CSX CYBERSECURITY NEXUS BY ISACA

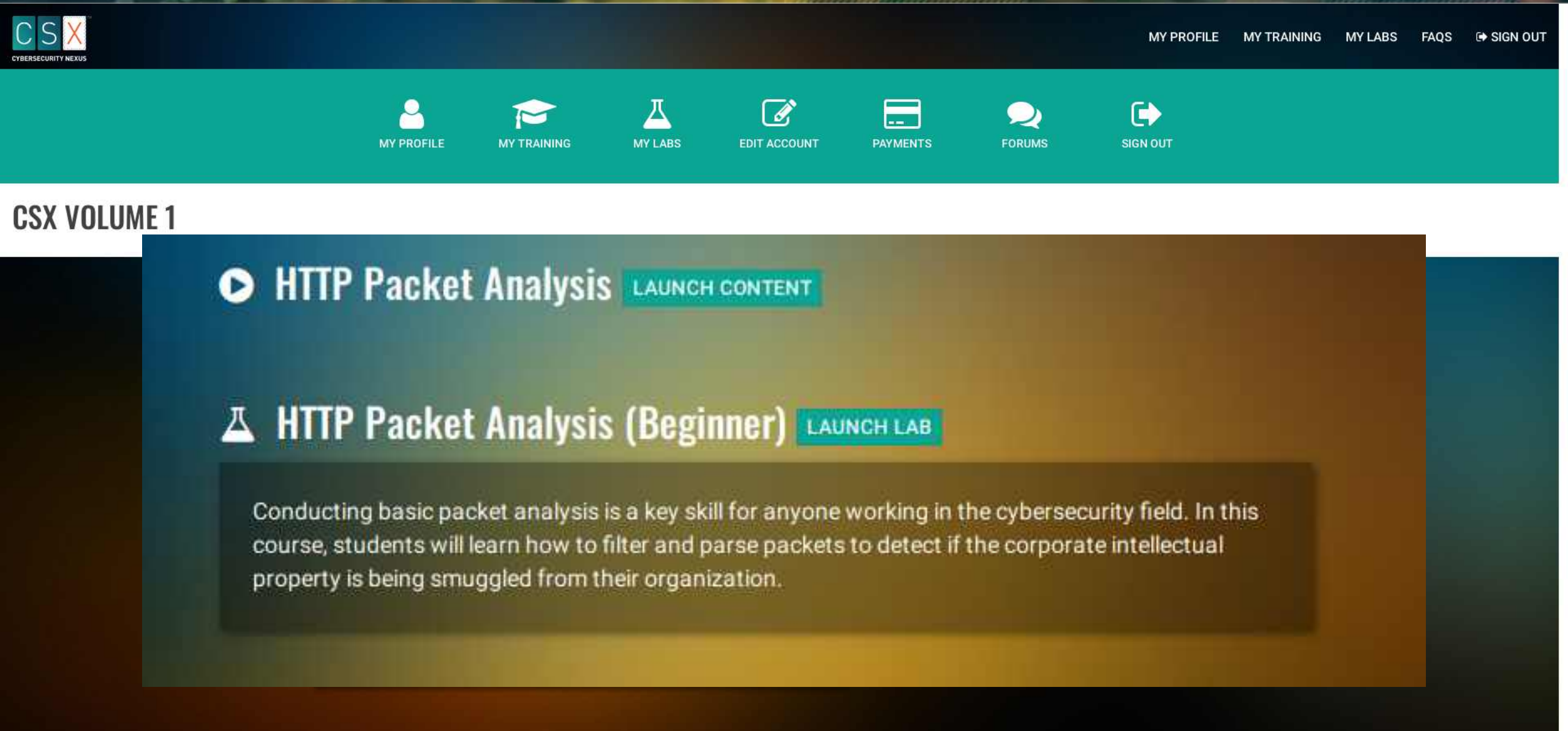
CSX PRACTITIONER / HTTP PACKET ANALYSIS



CSX PRACTITIONER / HTTP PACKET ANALYSIS



CSX PRACTITIONER / HTTP PACKET ANALYSIS



CSX PRACTITIONER / HTTP PACKET ANALYSIS

CSX CYBERSECURITY NEXUS

MY PROFILE MY TRAINING MY LABS FAQS SIGN OUT

Your lab environment is being built
This can take several minutes.

CSX PRACTITIONER / HTTP PACKET ANALYSIS

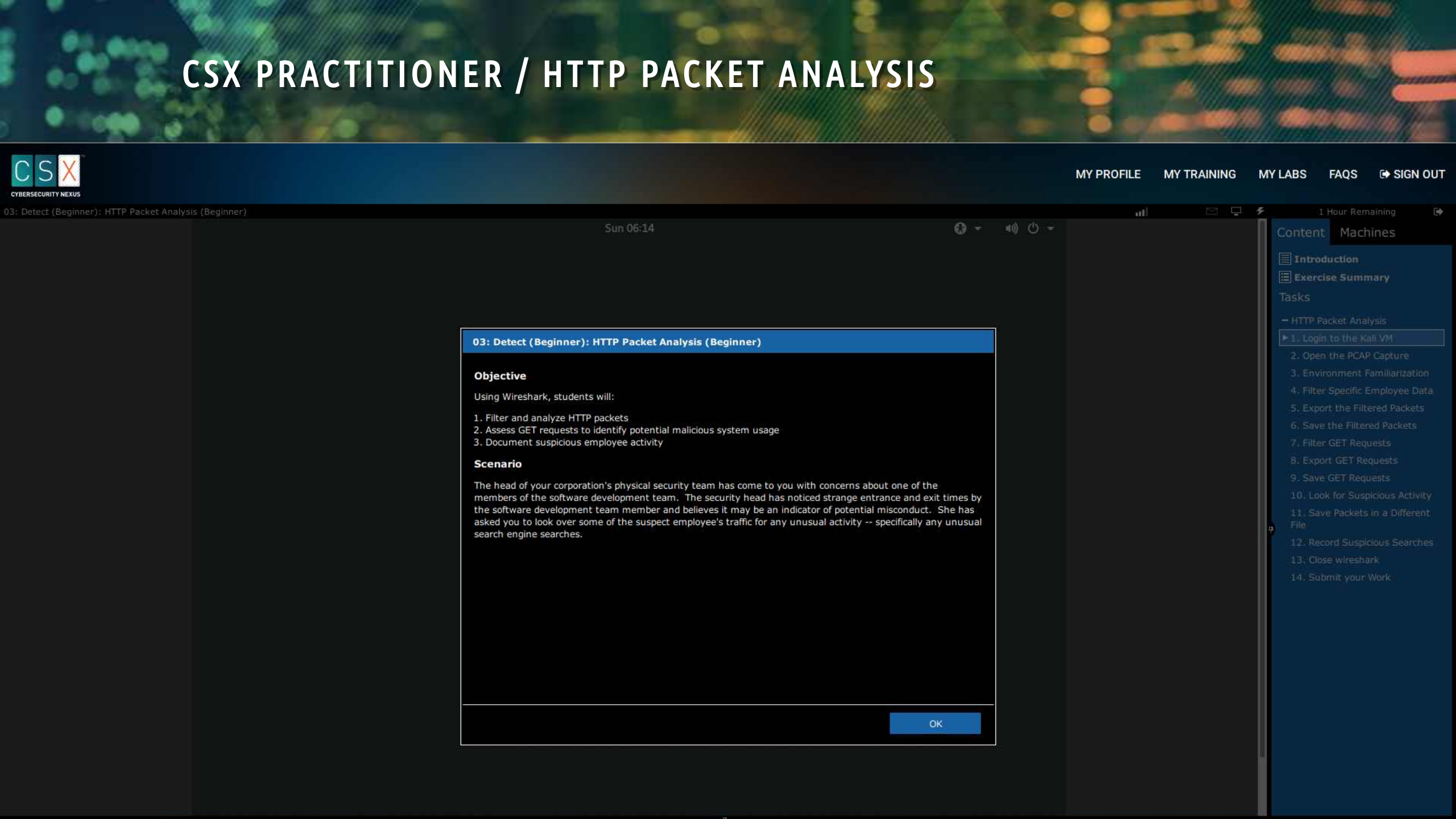
CSX CYBERSECURITY NEXUS

MY PROFILE MY TRAINING MY LABS FAQS SIGN OUT

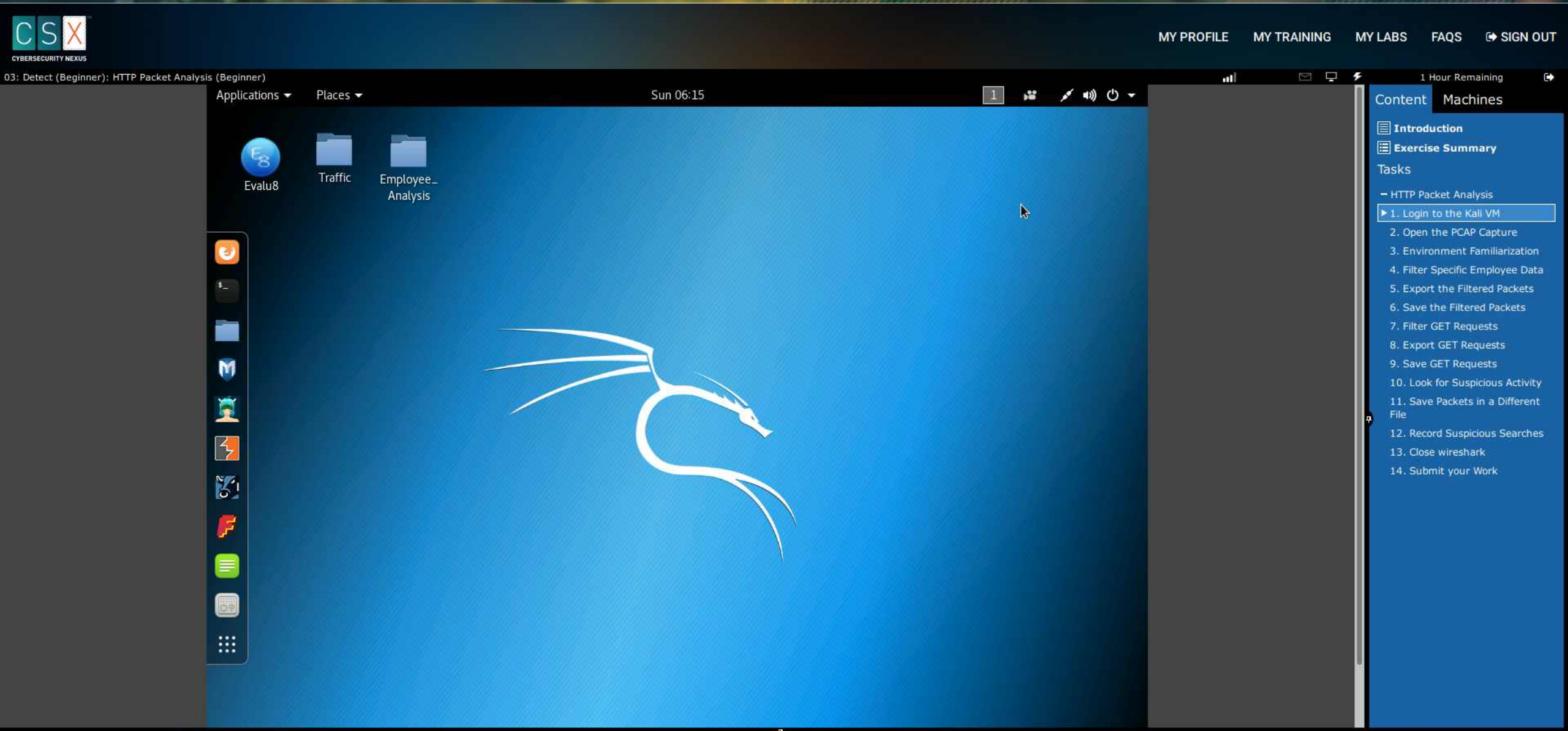
Your virtual machines are starting

This can take several minutes.

CSX PRACTITIONER / HTTP PACKET ANALYSIS



CSX PRACTITIONER / HTTP PACKET ANALYSIS



CSX PRACTITIONER / HTTP PACKET ANALYSIS

Applications Places Wireshark Sun 06:17

employee_traffic_sample.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression... +

No.	Time	Source	Destination	Protocol	Length	Info
66	6.071321	192.168.2.204	192.168.2.1	DNS	72	Standard query 0xf818 AAAA www.bing.com
67	6.071329	192.168.2.204	13.107.21.200	HTTP/X…	1681	POST /fd/ls/lsp.aspx HTTP/1.1
68	6.073587	192.168.2.1	192.168.2.204	DNS	183	Standard query response 0x36af A www.bing.com CNAME www-bing-com.a-0001.a-mse…
69	6.075304	192.168.2.1	192.168.2.204	DNS	151	Standard query response 0xf818 AAAA www.bing.com CNAME www-bing-com.a-0001.a-…
70	6.087239	13.107.21.200	192.168.2.204	TCP	66	80 → 44146 [ACK] Seq=1 Ack=1616 Win=514 Len=0 TSval=227191862 TSecr=1064307
71	6.093273	13.107.21.200	192.168.2.204	HTTP	305	HTTP/1.1 204 OK
72	6.093502	192.168.2.204	13.107.21.200	TCP	66	44146 → 80 [ACK] Seq=1616 Ack=240 Win=5159 Len=0 TSval=1064313 TSecr=227191863
73	6.104148	8.8.8.8	192.168.2.204	DNS	164	Standard query response 0x36af A www.bing.com CNAME www-bing-com.a-0001.a-mse…
74	6.104433	192.168.2.204	8.8.8.8	ICMP	192	Destination unreachable (Port unreachable)

```
▸ Frame 67: 1681 bytes on wire (13448 bits), 1681 bytes captured (13448 bits)
▸ Ethernet II, Src: Microsof_8b:01:09 (00:15:5d:8b:01:09), Dst: BelkinIn_30:1a:75 (14:91:82:30:1a:75)
▾ Internet Protocol Version 4, Src: 192.168.2.204, Dst: 13.107.21.200
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    [Total Length: 1667 bytes (reported as 0, presumed to be because of "TCP segmentation offload" (TSO))]
    Identification: 0x2057 (8279)
  ▸ Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (6)
    Header checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.2.204
    Destination: 13.107.21.200
    [Source GeoIP: Unknown]
  ▸ [Destination GeoIP: United States, Redmond, WA, AS8068 Microsoft Corporation, 47.680099, -122.120598]
▾ Transmission Control Protocol, Src Port: 44146, Dst Port: 80, Seq: 1, Ack: 1, Len: 1615
    Source Port: 44146
    Destination Port: 80
    [Stream index: 11]
    [TCP Segment Len: 1615]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 1616    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    Header Length: 32 bytes
  ▸ Flags: 0x018 (PSH, ACK)
    Window size value: 5159
```

```
0000  14 91 82 30 1a 75 00 15  5d 8b 01 09 08 00 45 00   ...0.u.. ].....E.
0010  00 00 20 57 40 00 40 06  00 00 c0 a8 02 cc 0d 6b   .. W@.@. .......k
0020  15 c8 ac 72 00 50 ac 95  7c 40 5d ce db ef 80 18   ...r.P.. |@].....
0030  14 27 e6 ad 00 00 01 01  08 0a 00 10 3d 73 0d 8a   .'...... ....=s..
0040  a8 9a 50 4f 53 54 20 2f  66 64 2f 6c 73 2f 6c 73   ..POST / fd/ls/ls
0050  70 2e 61 73 70 78 20 48  54 54 50 2f 31 2e 31 0d   p.aspx H TTP/1.1.
```

Content Machines

- Introduction
- Exercise Summary

Tasks

- HTTP Packet Analysis
  - ✓ 1. Login to the Kali VM
  - ✓ 2. Open the PCAP Capture
  - ✓ 3. Environment Familiarization
  - ▸ 4. Filter Specific Employee Data
  - 5. Export the Filtered Packets
  - 6. Save the Filtered Packets
  - 7. Filter GET Requests
  - 8. Export GET Requests
  - 9. Save GET Requests
  - 10. Look for Suspicious Activity
  - 11. Save Packets in a Different File
  - 12. Record Suspicious Searches
  - 13. Close wireshark
  - 14. Submit your Work

CSX PRACTITIONER / HTTP PACKET ANALYSIS

Applications Places Wireshark Sun 06:19

employee_traffic_sample.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr==192.168.2.204 && http.request.method=="GET"

No.	Time	Source	Destination	Protocol	Length	Info
133	11.562887	192.168.2.204	13.107.21.200	HTTP	773	[TCP Previous segment not captured] GET / HTTP/1.1
204	11.830119	192.168.2.204	13.107.21.200	HTTP	958	GET /fd/ls/l?IG=71F4017F4D9E4646A64C3EAE267784F7&Type=Event.CPT&DATA={%22pp%2…
220	12.091011	192.168.2.204	13.107.21.200	HTTP	983	[TCP Previous segment not captured] GET /notifications/render?bnptrigger=%7B%…
226	12.133446	192.168.2.204	13.107.21.200	HTTP	827	GET /hpm?IID=SERP.1000&IG=71F4017F4D9E4646A64C3EAE267784F7 HTTP/1.1
228	12.153985	192.168.2.204	13.107.21.200	HTTP	858	GET /HPImageArchive.aspx?format=js&idx=0&n=1&nc=1477235941541&pid=hp&video=1&…
261	12.387202	192.168.2.204	13.107.21.200	HTTP	901	GET /fd/ls/l?IG=71F4017F4D9E4646A64C3EAE267784F7&Type=Event.PPT&DATA={%22S%22…
289	13.887217	192.168.2.204	13.107.21.200	HTTP	903	GET /AS/Suggestions?pt=page.home&mkt=en-us&qry=&cp=0&o=hs&css=1&cvid=71F4017F…
320	14.045985	192.168.2.204	13.107.21.200	HTTP	835	GET /Passport.aspx?popup=1 HTTP/1.1
326	14.144012	192.168.2.204	65.202.58.87	HTTP	1087	[TCP Previous segment not captured] GET /fd/ls/l?IG=71F4017F4D9E4646A64C3EAE2…

```
▸ Frame 204: 958 bytes on wire (7664 bits), 958 bytes captured (7664 bits)
▸ Ethernet II, Src: Microsof_8b:01:09 (00:15:5d:8b:01:09), Dst: BelkinIn_30:1a:75 (14:91:82:30:1a:75)
▾ Internet Protocol Version 4, Src: 192.168.2.204, Dst: 13.107.21.200
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 944
    Identification: 0x4887 (18567)
  ▸ Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (6)
    Header checksum: 0x081a [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.2.204
    Destination: 13.107.21.200
    [Source GeoIP: Unknown]
  ▸ [Destination GeoIP: United States, Redmond, WA, AS8068 Microsoft Corporation, 47.680099, -122.120598]
▾ Transmission Control Protocol, Src Port: 44156, Dst Port: 80, Seq: 709, Ack: 34830, Len: 892
    Source Port: 44156
    Destination Port: 80
    [Stream index: 10]
    [TCP Segment Len: 892]
    Sequence number: 709    (relative sequence number)
    [Next sequence number: 1601    (relative sequence number)]
    Acknowledgment number: 34830    (relative ack number)
    Header Length: 32 bytes
  ▸ Flags: 0x018 (PSH, ACK)
    Window size value: 3123
```

```
0000  14 91 82 30 1a 75 00 15  5d 8b 01 09 08 00 45 00   ...0.u.. ].....E.
0010  03 b0 48 87 40 00 40 06  08 1a c0 a8 02 cc 0d 6b   ..H.@.@. .......k
0020  15 c8 ac 7c 00 50 ee 86  82 a8 cc b8 c5 b2 80 18   ...|.P.. ........
0030  0c 33 ea 49 00 00 01 01  08 0a 00 10 43 13 0d a4   .3.I.... ....C...
0040  67 a9 47 45 54 20 2f 66  64 2f 6c 73 2f 6c 3f 49   g.GET /f d/ls/l?I
0050  47 3d 37 31 46 34 30 31  37 46 34 44 39 45 34 36   G=71F401 7F4D9E46
```

Content Machines

- Introduction
- Exercise Summary

Tasks

- HTTP Packet Analysis
  - ✓1. Login to the Kali VM
  - ✓2. Open the PCAP Capture
  - ✓3. Environment Familiarization
  - ✓4. Filter Specific Employee Data
  - ✓5. Export the Filtered Packets
  - ✓6. Save the Filtered Packets
  - ✓7. Filter GET Requests
  - ✓8. Export GET Requests
  - ✓9. Save GET Requests
  - ▸10. Look for Suspicious Activity
  - 11. Save Packets in a Different File
  - 12. Record Suspicious Searches
  - 13. Close wireshark
  - 14. Submit your Work

CSX PRACTITIONER / HTTP PACKET ANALYSIS

CSX CYBERSECURITY NEXUS

MY PROFILE | MY TRAINING | MY LABS | FAQS | SIGN OUT

03: Detect (Beginner): HTTP Packet Analysis (Beginner)

53 Minutes Remaining

Applications | Places | Wireshark | Sun 06:22

employee_traffic_sample.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr==192.168.2.204 && http.request.method=="GET"

Expression... | Apply this filter

No.	Time	Source	Destination	Protocol	Length	Info
553	26.124183	192.168.2.204	13.107.21.200	HTTP	936	GET /search?q=how+to+sell+secrets&qs=n&form=QBLH&pq=how+to+sell+secrets&sc=6-…
592	26.251630	192.168.2.204	13.107.21.200	HTTP	879	GET /sa/simg/sw_nh_smallidentitycf.png HTTP/1.1
604	26.279262	192.168.2.204	13.107.21.200	HTTP	881	GET /sa/simg/sw_nh_nlog_cct3_optimal.png HTTP/1.1
652	26.999256	192.168.2.204	13.107.21.200	HTTP	1094	GET /fd/ls/l?IG=EA139520BBF94B88A387CF2F10F55B06&Type=Event.CPT&DATA={%22pp%2…
680	27.056077	192.168.2.204	13.107.21.200	HTTP	975	GET /th?id=Ac8b7ec32459ef26251b4900b726f46ad:A63497ba894d2470126377d4d1275af2…
682	27.059561	192.168.2.204	13.107.21.200	HTTP	974	GET /rms/rms%20serp%20shareWebResults_c.source/jc,nj/14377375/0f4b3475.js HTT…
686	27.068631	192.168.2.204	13.107.21.200	HTTP	990	[TCP Previous segment not captured] GET /rms/rms%20answers%20SegmentFilters%2…
687	27.068636	192.168.2.204	13.107.21.200	HTTP	990	[TCP Previous segment not captured] GET /rms/rms%20answers%20WebResult%20Blue…
695	27.073184	192.168.2.204	13.107.21.200	HTTP	989	GET /rms/rms%20answers%20VisualSystem%20Footer$IPv6TestScript/jc,nj/154b61c8/…

```
    Header Length: 32 bytes
  ▸ Flags: 0x018 (PSH, ACK)
    Window size value: 1224
    [Calculated window size: 1224]
    [Window size scaling factor: -1 (unknown)]
    Checksum: 0xea33 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  ▸ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  ▸ [SEQ/ACK analysis]
▾ Hypertext Transfer Protocol
  ▸ GET /search?q=how+to+sell+secrets&qs=n&form=QBLH&pq=how+to+sell+secrets&sc=6-19&sp=-1&sk=&cvid=71F4017F4D9E4646A64C3EAE267784F7 HTTP/1.1\r\n
    Host: www.bing.com\r\n
    User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:49.0) Gecko/20100101 Firefox/49.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Referer: http://www.bing.com/\r\n
  ▸ [truncated]Cookie: SRCHD=AF=NOFORM; SRCHUID=V=2&GUID=13388AEBD0B54887968166A4876D4777; SRCHUSR=DOB=20161023; _SS=SID=380FAAF4CBE169E01BB5A343CA0D6885&R=0&b
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    \r\n
    [Full request URI: http://www.bing.com/search?q=how+to+sell+secrets&qs=n&form=QBLH&pq=how+to+sell+secrets&sc=6-19&sp=-1&sk=&cvid=71F4017F4D9E4646A64C3EAE267
    [HTTP request 2/13]
    [Prev request in frame: 220]
    [Response in frame: 641]
    [Next request in frame: 661]
```

```
01c0  74 65 0d 0a 52 65 66 65  72 65 72 3a 20 68 74 74   te..Refe rer: htt
01d0  70 3a 2f 2f 77 77 77 2e  62 69 6e 67 2e 63 6f 6d   p://www. bing.com
01e0  2f 0d 0a 43 6f 6f 6b 69  65 3a 20 53 52 43 48 44   /..Cooki e: SRCHD
01f0  3d 41 46 3d 4e 4f 46 4f  52 4d 3b 20 53 52 43 48   =AF=NOFO RM; SRCH
0200  55 49 44 3d 56 3d 32 26  47 55 49 44 3d 31 33 33   UID=V=2& GUID=133
0210  38 38 41 45 42 44 30 42  35 34 38 38 37 39 36 38   88AEBD0B 54887968
```

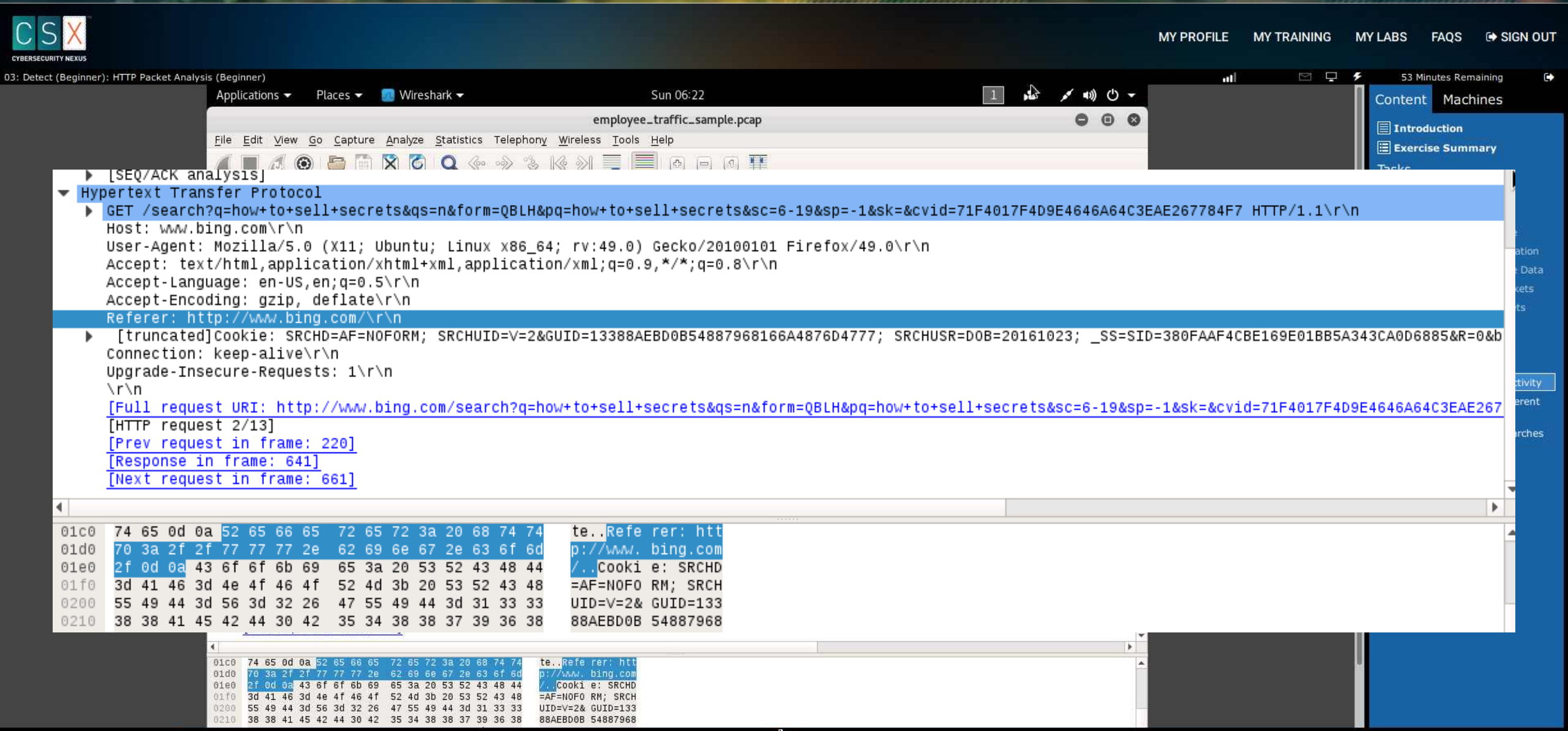
Content | Machines

- Introduction
- Exercise Summary

Tasks

- HTTP Packet Analysis
  - ✓1. Login to the Kali VM
  - ✓2. Open the PCAP Capture
  - ✓3. Environment Familiarization
  - ✓4. Filter Specific Employee Data
  - ✓5. Export the Filtered Packets
  - ✓6. Save the Filtered Packets
  - ✓7. Filter GET Requests
  - ✓8. Export GET Requests
  - ✓9. Save GET Requests
  - ▸10. Look for Suspicious Activity
  - 11. Save Packets in a Different File
  - 12. Record Suspicious Searches
  - 13. Close wireshark
  - 14. Submit your Work

CSX PRACTITIONER / HTTP PACKET ANALYSIS



CSX FUNDAMENTALS

Cybersecurity Introduction and Overview
Topic 1—Introduction to Cybersecurity
Topic 2—Difference Between Information Security and Cybersecurity
Topic 3—Cybersecurity Objectives
Topic 4—Cybersecurity Roles
Topic 5—Cybersecurity Domains

Cybersecurity Concepts
Topic 1—Risk
Topic 2—Common Attack Types and Vectors
Topic 3—Policies and Procedures
Topic 4—Cybersecurity Controls

Security Architecture Principles
Topic 1—Overview of Security Architecture
Topic 2—The OSI Model
Topic 3—Defense in Depth
Topic 4—Firewalls
Topic 5—Isolation and Segmentation
Topic 6—Monitoring, Detection and Logging
Topic 7A—Encryption Fundamentals
Topic 7B—Encryption Techniques
Topic 7C—Encryption Applications

Security of Networks, Systems, Applications and Data
Topic 1—Process Controls—Risk Assessments
Topic 2—Process Controls—Vulnerability Management
Topic 3—Process Controls—Penetration Testing
Topic 4—Network Security
Topic 5—Operating System Security
Topic 6—Application Security
Topic 7—Data Security

Incident Response
Topic 1—Event vs. Incident
Topic 2—Security Incident Response
Topic 3—Investigations, Legal Holds and Preservation
Topic 4—Forensics
Topic 5—Disaster Recovery and Business Continuity Plans

Security Implications and Adoption of Evolving Technology
Topic 1—Current Threat Landscape
Topic 2—Advanced Persistent Threats
Topic 3—Mobile Technology—Vulnerabilities, Threats and Risk
Topic 4—Consumerization of IT and Mobile Devices
Topic 5—Cloud and Digital Collaboration

CSX CYBERSECURITY NEXUS BY ISACA

CSX FUNDAMENTALS / Penetration Testing Phases

1. **Planning:** In the planning phase, the goals are set, the scope is defined and the test is approved and documented by management. The scope determines if the penetration test is internal or external, limited to certain types of attacks or limited to certain networks or assets.

2. **Discovery:** In the discovery phase, the penetration tester gathers information by conducting research on the organization and scans the networks for port and service identification. Techniques used to gather information include:
   a. DNS interrogation, WHOIS queries and network sniffing to discover host name and IP address information
   b. Search web servers and directory servers for employee names and contact information
   c. Banner grabbing for application and service information
   d. NetBIOS enumeration for system information
   e. Dumpster diving and physical walk-throughs of the facilities to gather additional information
   f. Social engineering, such as posing as a help desk agent and asking for passwords, posing as a user and calling the help desk to reset passwords or sending phishing emails

   A vulnerability assessment is also conducted during the discovery phase. This involves comparing the services, applications and operating systems of the scanned host against vulnerability databases.

3. **Attack:** The attack phase is the process of verifying previously identified vulnerabilities by attempting to exploit them. Metasploit® hosts a public database of quality-assured exploits. They rank exploits for safe testing.

   Sometimes exploit attempts do not provide the tester with access, but they do give the tester additional information about the target and its potential vulnerabilities. If a tester is able to exploit a vulnerability, they can install more tools on the system or network to gain access to additional systems or resources.

   A payload is the piece of software that lets a user control a computer system after it has been exploited. The payload is typically attached to and delivered by the exploit. Metasploit's most popular payload is called Meterpreter, which enables a user to upload and download files from the system, take screenshots and collect password hashes. The discovery and attack phases are illustrated in **exhibit 4.7**.

In a basic Internet type of computer configuration using multiple computers, a site server is installed behind a firewall and its databases are installed on a second computer behind a second firewall. Other configurations are possible, of course. In some cases, there is a corporate intranet with internal users and a database server behind a firewall, a site server, another firewall and external users (it is also useful to have external site server tools access). Each firewall would allow access to ports set open by the site server software. With many server software applications, a number of ports are set by default, for example, HTTP-80, HTTPS-443 (the standard secure web server port number), SMTP-25 and others. Commonly exploited ports and services are listed in **exhibit 4.9**.

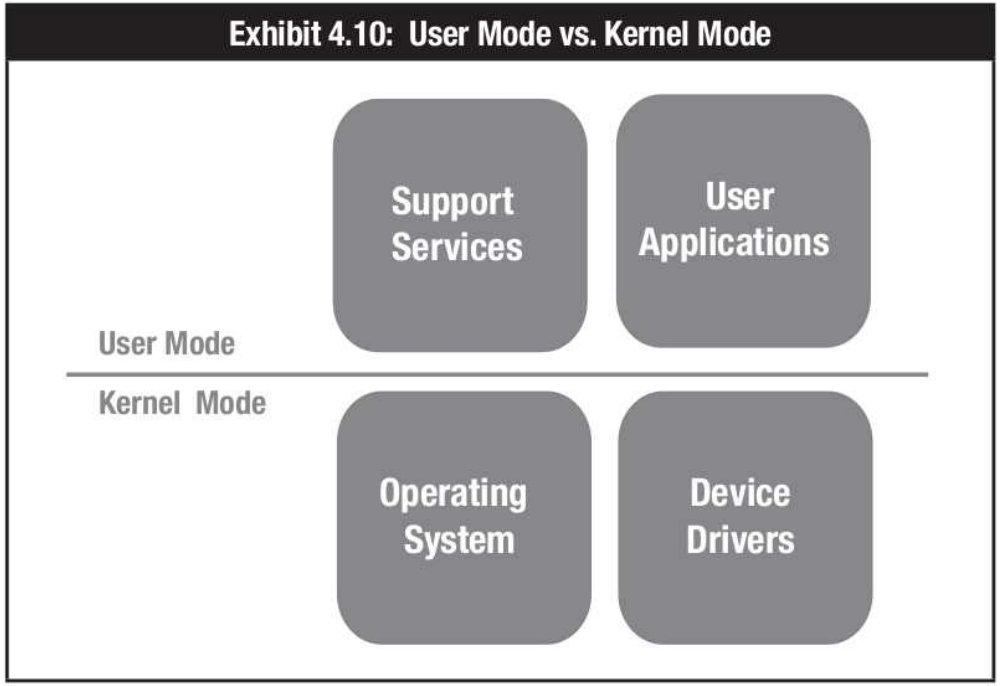
Exhibit 4.9: Commonly Exploited Ports and Services

Port #	Service	Protocol	Port #	Service	Protocol
7	Echo	TCP/UDP	110	POP3 (post office protocol)	TCP
19	chargen	TCP	111/2049	SunRPC (remote procedure calls)	TCP/UDP
20-21	FTP (file transfer protocol)	TCP	135-139	NBT (NetBIOS over TCP/ IP)	TCP/UDP
23	Telnet (remote login)	TCP	161, 162	SNMP (Simple Network Management Protocol)	UDP
25	SMTP (simple mail transfer)	TCP	512	Exec	UDP
43	Whois	TCP/UDP	513	Login	TCP
53	DNS (domain name system)	TCP	514	Shell	TCP/UDP
69	TFTP (trivial file transfer	6000-xxxx		protocol)	UDP
xxxx	X-Windows	TCP			
79	Finger	TCP	8000	HTTP	TCP/UDP
80	HTTP-low	TCP	8080	HTTP	TCP/UDP
107	Rtelnet	TCP/UDP	31337	Back Orifice	UDP

MODES OF OPERATIONS

Most operating systems have two modes of operations—**kernel mode** for execution of privileged instructions for the internal operation of the system and **user mode** for normal activities. In kernel mode, there are no protections from errors or malicious activity and all parts of the system and memory are accessible. See **exhibit 4.10**.

Exhibit 4.10: User Mode vs. Kernel Mode



Operating systems allow controlled access to kernel mode operations through system calls that usually require privileges. These privileges are defined on a user or program basis and should be limited under the principle of least privilege.

Most attacks seek to gain privileged or kernel mode access to the system in order to circumvent other security controls.

BEVINDINGEN WERKGROEP CSX

De werkgroep CSX ISACA Nederland heeft na een try-out geconstateerd dat er onder leden 2 uiteenlopende behoeftes leven:

1. Enerzijds zijn er leden die willen opgaan voor de formele CSX Fundamentals en Practitioner certificering, zij hebben behoefte aan een degelijke examentraining.

2. Anderzijds zijn er leden en dan met name Auditors, die net als het ISACA NL bestuur dat ziet, denken dat er een behoefte is aan (bij)scholing om hun bijdrage aan de Weerbaarheid van hun organisatie te verhogen.

De werkgroep richt haar aandacht op het ontwikkelen van een lesprogramma om te voldoen aan de behoefte bij punt 2.

CSX CYBERSECURITY NEXUS BY ISACA

KENMERKEN CSX FUNDAMETALS/PRACTITIONER

Kenmerken eerste categorie:

CSX Certificering (Foundation en Practitioner) [hoog technisch]

1. Technische knowhow netwerken, ip configuratie, subnetting etc al.
2. Inhoudelijke netwerk verkeer analyse, zoals gezien in de demo.
3. Malware herkenning en analyse, disassemblen van programmatuur en code review.
4. Netwerk penetratie testen, scanning technieken en aanvalmethodieken.
5. Technisch configuratie operating systems Windows, Linux etc.
6. Operating System Hardening, minimale service exposure, juiste rechtenstructuur etc.
7. Praktische ervaring met IDS/IPS, hoe analyseer ik meldingen en plaats ik deze in context.
8. Etc. etc. etc.

KENMERKEN FOCUS VAN DE CSX WERKGROEP

Kenmerken tweede categorie:

Kennisverbreding t.b.v. weerbaarheid [laag technisch, algemene termen en verbanden]

1. Wat is een vulnerability en hoe werkt dat (uitleg bufferoverflow en input validatie)
2. Diverse smaken log management tot aan SIEM functionaliteit
3. Wat kan je nu eigenlijk met een IDS doen?
4. Hoe werkt netwerksegmentatie en wat heb je er aan
5. Hoe verhouden diverse maatregelen zich tot elkaar
6. Hoe verrijken diverse maatregelen elkaar

Deze uitleg wil de werkgroep plotten op bekende modellen zodat duidelijk wordt hoe technische oplossingen kunnen helpen en welke maatregelen helpen in welk onderdeel. Een dergelijk theoretisch model geeft zodoende handvatten om op diverse plaatsen in de organisatie de juiste vragen te kunnen stellen.

De verkregen kennis over de onderlinge verhoudingen/verrijkingen tussen de context/fase/model en maatregelen stellen de Auditor in staat de verkregen antwoorden nog beter op waarde te kunnen schatten.

VOORBEELD KILLCHAIN-MODEL / DEFINITIE VAN DE FASES

Dit is de fase waarin kwaadwillenden proberen te beslissen wat goed en slechte doelen zijn om aan te vallen.

De hoeveelheid en de kwaliteit van de informatie die men kan vinden over uw organisatie en de wijze waarop dit gebruikt kan worden, kan u verrassen.

In deze fase wordt een op het doel afgestemde methode bedacht en software gemaakt om tot het doelsysteem te kunnen doordringen.

Dit kan in technische vorm (software vulnerabilities), echter ook in andere vormen. (Social engineering)

De bewapening kan ook specifiek gericht zijn op een persoon bijvoorbeeld.

Nadat de bewapening is gekozen en gemaakt, dient het wapen ook nog afgeleverd te worden op de locatie.

In deze fase wordt een methode bepaald waarmee deze aflevering plaats gaat vinden.

Dit kan wederom een technische methode zijn, maar ook gericht op personen. Vaak een combinatie daarvan.

De exploitatie is het uitbuiten van zwakheden in de infrastructuur om zodoende de payload die bij aflevering is binnen gekomen te kunnen uitvoeren.

Deze payload hoeft niet het uiteindelijke product te zijn dat ook geïnstalleerd wordt!

De payload wordt op diverse plekken in de infrastructuur verstopt en zodanig geïnstalleerd dat deze ontdekking probeert de voorkomen.

Daarnaast is het van belang dat de payload zo resistent mogelijk wordt geplaatst. Verwijdering is moeilijk en herstart apparatuur heeft geen invloed.

Er wordt contact gezocht met de Command and Control servers die ingericht zijn om de payloads te voorzien van instructies.

Het doel is om dit verkeer ondetecteerbaar te krijgen. Veel gebruikte protocollen worden hiervoor misbruikt die niet van toegestane verkeer te onderscheiden zijn.

Hier worden de opdrachten van de Command en Control servers uitgevoerd.

Encryptie data, exfiltratie gegevens, beïnvloeden processen, subtiele wijziging gegevens, te veel mogelijkheden om op te noemen.

CSX CYBERSECURITY NEXUS BY ISACA

VOORBEELD KILLCHAIN-MODEL / PLOTTEN MAATREGELEN

Houdt verkeer op uw publieke infrastructuur in de gaten.

Technische maatregelen
- Log Management
- DLP oplossingen
- Actieve monitoring media
- Maak gebruikers bewust dat ze kunnen melden als er iets raars op hun social media accounts gebeurt en dat zij daar niet alles zomaar moeten plaatsen.

In deze fase helpen maar weinig maatregelen.

In de uiterste gevallen kan op het “dark web” op marktplaatsen b.v. gekeken worden naar rekrutering van mensen voor een bepaalde opdracht.

Breng attack vectors in kaart en monitor deze.

Technische maatregelen
- Mail filtering
- Web filtering
- Behaviour analysis
- End point protection
- Goede end point policies
- IDS/HIDS
- Log Management van alle bovenstaande oplossingen om events te kunnen correleren.

Houdt systemen uit de attack vectorlijst goed in de gaten.

Technische maatregelen
- Patching van Vulnerabilities
- End Point Protection
- Log Management om uitzonderlijke situaties in kaart te brengen
- Monitoring systemen, b.v. hoge CPU load of andere vreemde zaken

Houdt systemen uit de attack vectorlijst goed in de gaten.

Technische maatregelen
- HIDS
- End Point Protection
- Goede policies op endpoints
- Log Management om uitzonderlijke situaties in kaart te brengen
- Monitoring systemen, b.v. hoge CPU load of andere vreemde zaken

Communicatie-mogelijkheden dienen bewaakt te worden.

Technische maatregelen
- IDS
- Firewalling
- Filtering Proxy
- DLP
- Log Management om uitzonderlijke situaties in kaart te brengen

Communicatie-mogelijkheden dienen bewaakt te worden.

Technische maatregelen
- IDS
- Firewalling
- Filtering Proxy
- DLP
- Mail Filtering
- Toegangscontrole
- Log Management om uitzonderlijke situaties in kaart te brengen

CSX CYBERSECURITY NEXUS BY ISACA

MEER INFORMATIE

De werkgroep CSX binnen ISACA NL bestaat uit:

1) *Jan van Kemenade, Inf. Security Officer RABObank, CSX Liaison bestuur* *jan.vankemenade@isaca.nl*
2) *Jeroen Visser, Senior Consultant Cyber-/Infosecurity DPA B-Able* *jeroen.visser@dpa.nl*

3) *Een Senior Consultant CyberSecurity, KPN*
4) *Een Auditor RE en RA, niet technisch*
5) *Senior IT Auditor en Business Consultant*
6) *Chief Security Officer en zeer betrokken Privacy/Cybersecurity lid*
7) *Onderwijs specialist op gebied van Cyber Security*
8) *Een bekende ex WOB-er*

Tijdens de NOREA IT-Auditors dag hebben diverse mensen zich aangemeld om in de werkgroep plaats te nemen. Daarvoor hartelijk dank!

CSX CYBERSECURITY NEXUS BY ISACA

AFSLUITEN

Hartelijk dank voor uw aanwezigheid. Als er nog vragen zijn kunt u ze in de resterende tijd stellen. De rest van de dag ben ik aanwezig en nog aanspreekbaar.

Wilt u achteraf nog contact?

Mijn naam is Jeroen Visser,
Cyber/Informatie Security Consultant bij DPA B-Able.
Email: jeroen.visser@dpa.nl
LinkedIn: https://linkedin.com/in/jeroenvisservm

CSX CYBERSECURITY NEXUS BY ISACA