

cybersecurity

Introduction to bootCon

Lesson 24.1



Welcome

This week



bootCon

Presenter

Name
Company
Job Title

Email: name@company.com



000-000-000

This Week

This week, we will conclude our cohort by participating in a cyber conference, called bootCon.

Day 1:

We will:

- Highlight the value of communication in the cybersecurity industry.
- Review the bootCon conference and the rules for your presentations.
- Research and begin to piece together your presentations.

Day 2:

We will:

- Review some tips for a successful bootCon presentation
- Use the remaining class time to finalize your presentations.

Day 3:

We will:

- Present our projects.

Congratulations

You've learned a lot over the past 23 weeks:

01

Core fundamental skills of terminal, operating systems, networking, cryptography, and cloud

02

Offensive skills such as web application attacks and penetration testing

03

Defensive skills such as SIEM and attack defense

While proficiency with these skills is important for success in the cybersecurity industry, it is also imperative that cyber professionals can clearly communicate cyber issues to audiences, including:

- Customers
- Management
- Board members
- Peers

Often this audience is non-technical, and the ability to communicate complex cyber issues in layman's terms is crucial.



The Importance of Communication

Suppose an application security professional at a bank is tasked with finding vulnerabilities in their online-banking application.

If this AppSec employee discovers a SQL injection vulnerability on their bank's website that may have already been exploited, they may be tasked with several important communications:

01

Explaining the issue to their management team and executives at the organization and providing a high-level overview of the vulnerability and the risk/impact of not mitigating it quickly.

02

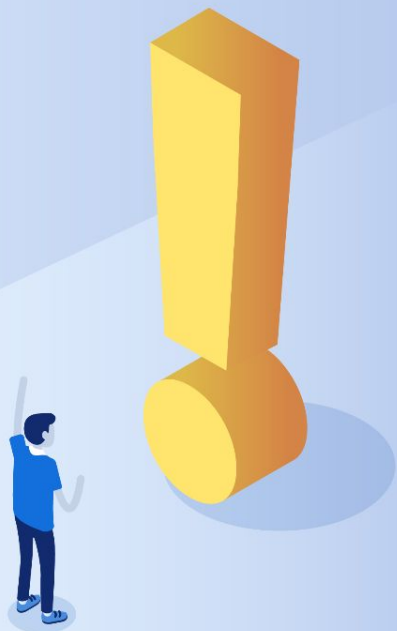
Explaining to the legal team what data may have been exposed so that they can begin to determine the legal implications.

03

Communicating to the developers where the vulnerability exists within the web application so they can implement a fix to their code.

Clear communication

can help lead to an efficient and quick resolution to a security issue.



Poor communication

could adversely impact the business by guiding business partners to make incorrect or ineffective decisions.



For example: If the AppSec developer doesn't clearly present the data that may have been exposed to their attorneys, the organization may not properly disclose breached data, which could have significant legal implications.

The Importance of Communication

While the ability to communicate complex cyber issues to a variety of stakeholders is one aspect of cyber communication, cyber professionals may also need to clearly communicate technical topics for other reasons, including:

01

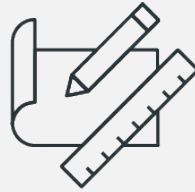
Presenting proposals for ordering new technology to management.

02

Explaining their InfoSec/technical experience in job interviews.

03

Presenting cybersecurity research to their peers.



Cybersecurity Research Presentations

Cybersecurity Research Presentations

Cybersecurity professionals commonly present the following to their peers:

1

Security research that they're conducting.

2

Newly discovered security vulnerabilities of products, devices, software, or hardware.

3

Demonstrations of the “hacks” that will exploit these vulnerabilities.

4

Mitigations to protect against these vulnerabilities.



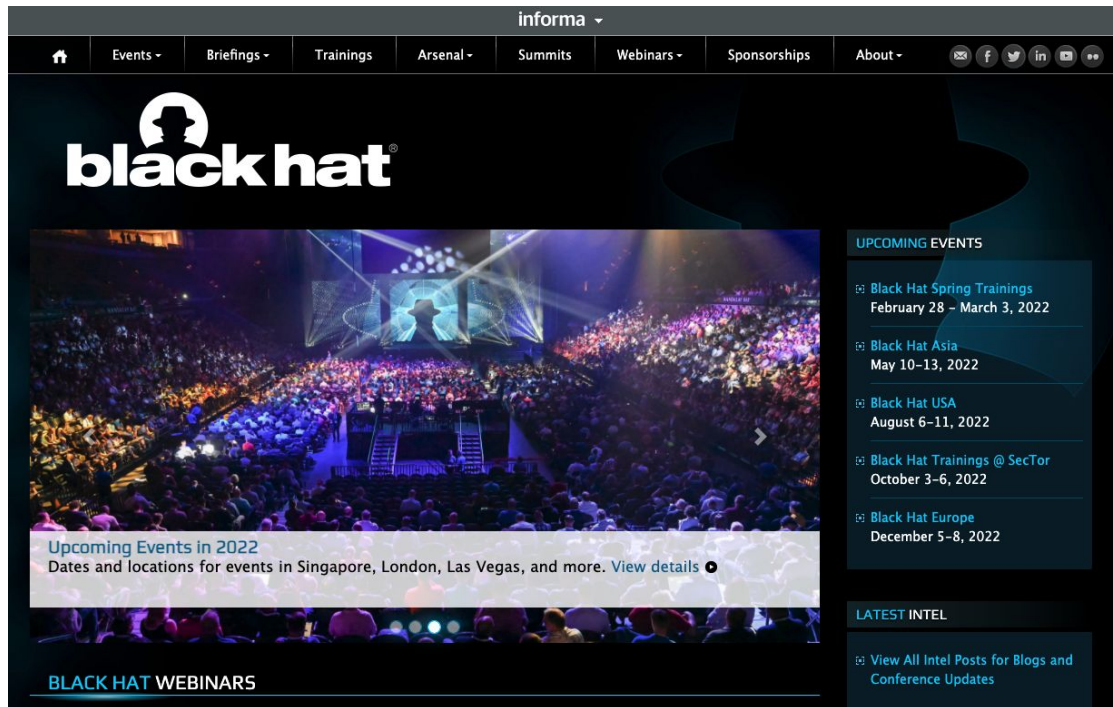
- These presentations often occur at security conferences, trade shows, and other industry events.
- Cybersecurity professionals commonly attend these events to remain up to date with new technological developments and techniques.
- These events can also provide good networking opportunities, which can help when job searching both early and later on in your career.

Cyber Conferences and Events: Black Hat

Black Hat is one of the largest cybersecurity events, typically held in Las Vegas every year in late summer.

This event brings executives, cyber practitioners, and cyber sales teams to show off their newest products to the industry.

Additionally, it includes many talks about cyber vulnerabilities and their mitigations.

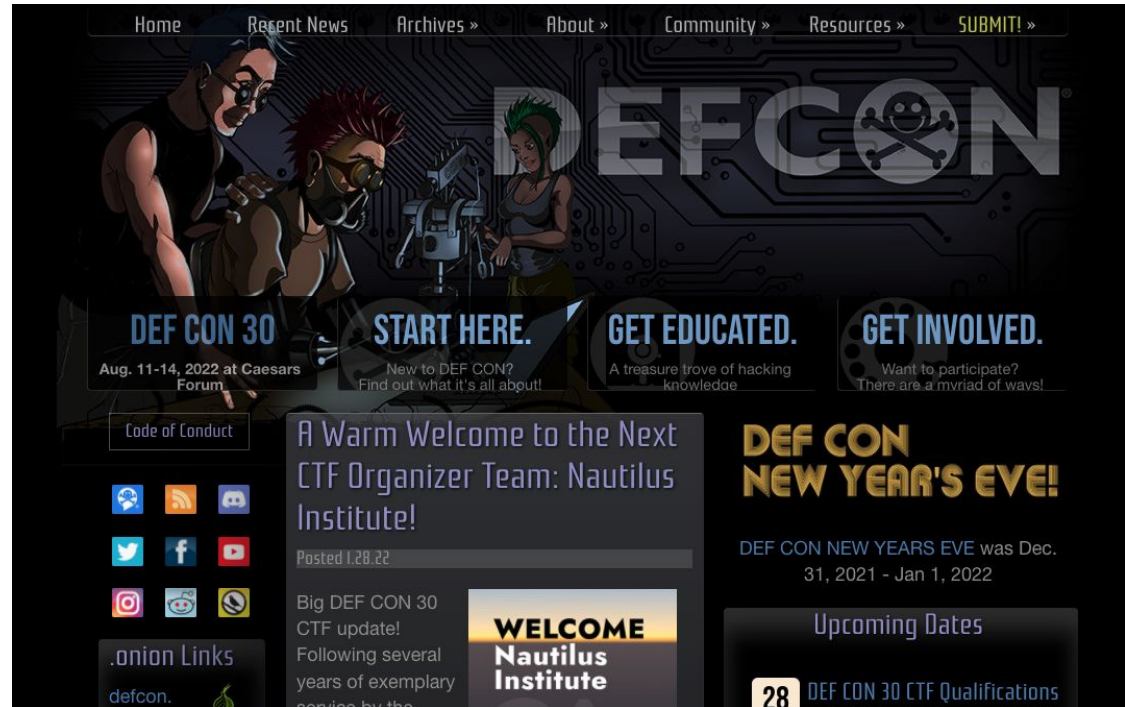


The screenshot displays the Black Hat website interface. At the top, a navigation bar includes links for Home, Events, Briefings, Trainings, Arsenal, Summits, Webinars, Sponsorships, and About, along with social media icons. The main header features the Black Hat logo, which consists of a silhouette of a person wearing a hat. Below the logo is a large, vibrant image of a crowded conference hall with a stage and bright lighting. A text overlay on the image reads "Upcoming Events in 2022" and "Dates and locations for events in Singapore, London, Las Vegas, and more. View details". To the right of the main image, a sidebar titled "UPCOMING EVENTS" lists several events: "Black Hat Spring Trainings" (February 28 - March 3, 2022), "Black Hat Asia" (May 10-13, 2022), "Black Hat USA" (August 6-11, 2022), "Black Hat Trainings @ SecTor" (October 3-6, 2022), and "Black Hat Europe" (December 5-8, 2022). Below this, a section titled "LATEST INTEL" includes a link to "View All Intel Posts for Blogs and Conference Updates". At the bottom of the page, a section titled "BLACK HAT WEBINARS" is visible.

Cyber Conferences and Events: DEF CON

DEF CON occurs in Las Vegas immediately after Black Hat. DEF CON is not only considerably less expensive (typically around \$300), it is also very informal.

Similar to Black Hat, DEF CON offers many talks about vulnerabilities and their mitigations.



Larger Cyber Conferences and Events: RSA

RSA is a formal cybersecurity conference held annually in winter in San Francisco. It is typically attended by cyber management and executives.

RSA also offers many talks about cyber vulnerabilities and mitigations.



The image is a screenshot of the RSA Conference website. The header is dark with the 'RSAConference' logo on the left and a navigation menu on the right containing links for 'Events', 'Library', 'Experts', 'Marketplace', 'RSAC Programs', 'About', and a search icon. Below the header, the main banner features a blue-tinted background image of a smiling man. The text on the banner reads: 'Where the world talks security' (small), 'RSAC 2022 Registration Has Reopened!' (large), and a paragraph of text: 'Great news! We've reopened registration and extended our Discount Period, so there's still time to save \$900* on a Full Conference Pass. While we finish updating our agenda, browse through our expanding list of inspirational Keynotes and speakers.' At the bottom of the banner are two buttons: 'VIEW SPEAKERS' (red) and 'REGISTER NOW' (blue).

RSAConference
Where the world talks security

Events ▾ Library ▾ Experts ▾ Marketplace ▾ RSAC Programs ▾ About ▾ 🔍

RSAC 2022 Registration Has Reopened!

Great news! We've reopened registration and extended our Discount Period, so there's still time to save \$900* on a Full Conference Pass. While we finish updating our agenda, browse through our expanding list of inspirational Keynotes and speakers.

[VIEW SPEAKERS](#) [REGISTER NOW](#)

Smaller/Local Cyber Events

Many smaller, local cyber conferences exist, and students may be able to find one that's available in their area.

Bsides:

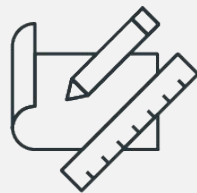
Per Bsides, “each BSides is a community-driven framework for building events for and by information security community members.” Bsides often hosts local conferences where speakers discuss security issues. The audience is typically local and smaller.

Local OWASP and DEF CON meetups:

Local chapters of groups such as OWASP and DEF CON may hold smaller monthly presentations.

Independent local security events:

There are also many independent conferences all over the world.

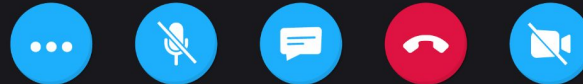


Introduction to bootCon

All of the conferences and events that we just discussed provide great learning opportunities.

During our final week of class:

We will get an opportunity to hold our very own class cyber conference called bootCon, where you will each present to your classmates!



bootCon Presentations

01

As discussed earlier in the course, on the last day of class, we will hold a cyber class conference called bootCon.

02

Each student will have an opportunity to showcase the skills that they learned during the boot camp with a presentation.

03

If students have elected to present as a group, each student must participate during the presentation.

04

Most cyber professionals present at conferences when they've found a brand-new vulnerability. However, for bootCon presentations, it is acceptable and recommended that you re-create a finding that has already been discovered.



A bootCon presentation
is **NOT** a research paper.



While research will be required, all presentations must be tangible and demonstrable.

A demonstration can either be:

- Conducted in person.
- A prerecorded video that accompanies the presentation (*if a live demonstration isn't practicable*).



bootCon Presentations

Each bootCon presentation should fall into one of the following three categories:

01

Category

Exploiting a vulnerability of an IoT device.

02

Developing code or a program that can complete a cybersecurity task.

03

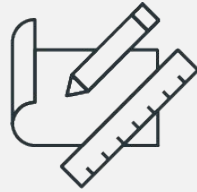
Demonstration of how a cybersecurity tool that was not covered in class can accomplish a specific goal.

Example

Hacking your personal Blu-Ray player.

Developing a Python script that can automate an Nmap scan.

Using SET to design a social engineering campaign



bootCon Rules and Requirements

bootCon Rules and Requirements

If you haven't yet received approval for your project, make sure to submit your project summary to your instructor for approval before proceeding.

Your project summary should include:

01

Topic and title of your presentation

02

End goal or vulnerability being exploited

03

List of devices and/or technologies that will be used to accomplish the goal

04

Summary of how the devices and technologies will be used to accomplish the goal

bootCon Rules and Requirements



Under no circumstances may any aspect of your **bootCon** presentation be unethical or illegal.

You must:

01

Perform all hacks and tests in simulated environments.

02

Complete any network connections in your own home and/or controlled environments.

03

Only perform IoT hacks on devices that you personally own.

bootCon Rules and Requirements

Presentations must have a goal whose achievement you can demonstrate.

For example:

Goal:

Cracking WEP wireless traffic from your home router.



Demonstration:

How you captured and cracked your wireless traffic.



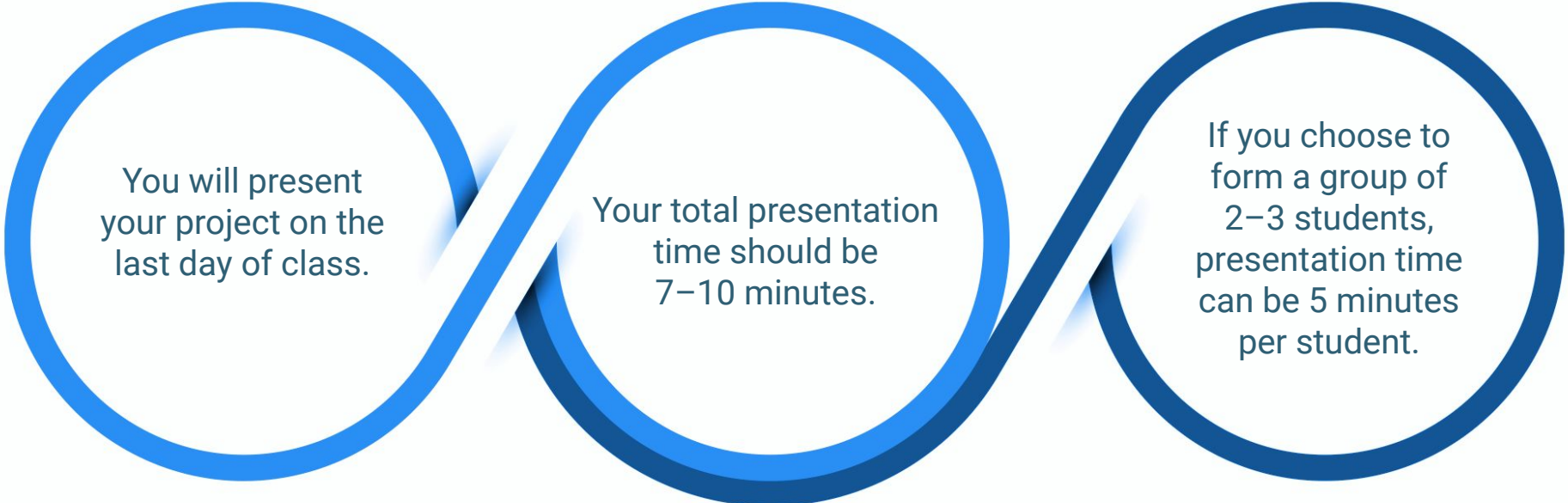
You can either conduct your demonstration live or record it and present it while you walk through what has taken place.

bootCon Rules and Requirements

You must submit your presentation in the form of a Google Slides deck that, at a minimum, includes the following:

Cover slide:	Presentation title and team member(s) presenting.
Technical background:	<ul style="list-style-type: none">• Explanation of why you selected the topic that you are presenting.• Networking, cryptographic, or security concepts applied.• Research steps taken.
Demonstration preview:	Preview of the steps that you'll take in the upcoming demonstration.
Demonstration:	A live or recorded demonstration is conducted here.
Demonstration summary:	Summary of the demonstration that you just conducted and any impact that it may have.
Mitigation:	Recommendations for mitigating against the attack that you just conducted. If your presentation isn't about an attack, this is not required.

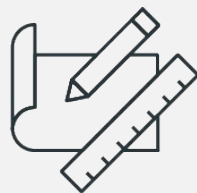
bootCon Rules and Requirements



You will present
your project on the
last day of class.

Your total presentation
time should be
7–10 minutes.

If you choose to
form a group of
2–3 students,
presentation time
can be 5 minutes
per student.



Example bootCon presentation

DHCP Starvation Attack with Yersinia

Slide 1 – Cover Slide:

This is the cover slide, with the presentation title and team members presenting.

What is DHCP?



- Dynamic Host Configuration Protocol (DHCP) is a network management protocol used to automate the process of dynamically configuring devices on IP networks, which allows them to use network services such as DNS, NTP, and many other communication protocols.
- A DHCP server hands out configuration data, based on the administrator's policy, to a requesting client.
- Common network parameters requested include subnet mask, router, domain name server, hostname, and domain name.

Slide 2, 3, 4 – Technical Background:

These slides explain the technical background of the project. They cover any protocols, cryptographic concepts, or network diagrams that are used in the upcoming demonstration.

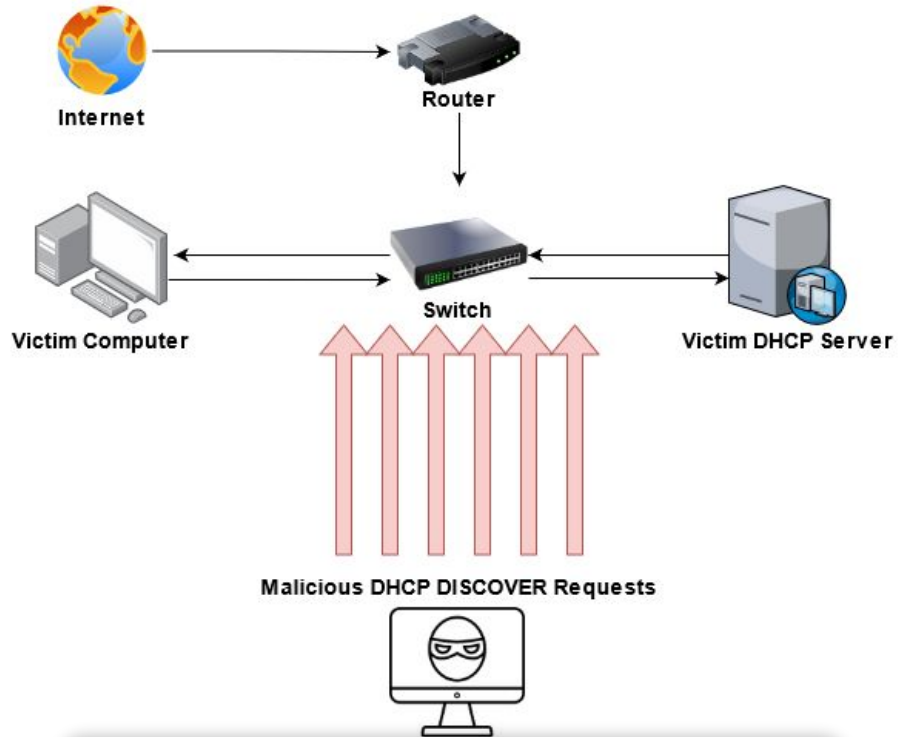
DHCP Starvation Attack

- During a DHCP attack, a hostile actor floods a DHCP server with DISCOVER packets and fake MAC addresses.

```
Source Dest Source Dest Packet
MAC addr MAC addr IP addr IP addr Description
-----
Client Broadcast 0.0.0.0 255.255.255.255 DHCP Discover
DHCPsrvr Broadcast DHCPsrvr 255.255.255.255 DHCP Offer
Client Broadcast 0.0.0.0 255.255.255.255 DHCP Request
DHCPsrvr Broadcast DHCPsrvr 255.255.255.255 DHCP ACK
```

- The DHCP server can't successfully send back OFFER packets and holds reservations for every DISCOVER packet sent until it exhausts its supply of IP addresses.

Visualization



Slide 2, 3, 4 – Technical Background

Installing and Using Yersinia

- Yersinia does not come with Kali by default, so the following command should be run:

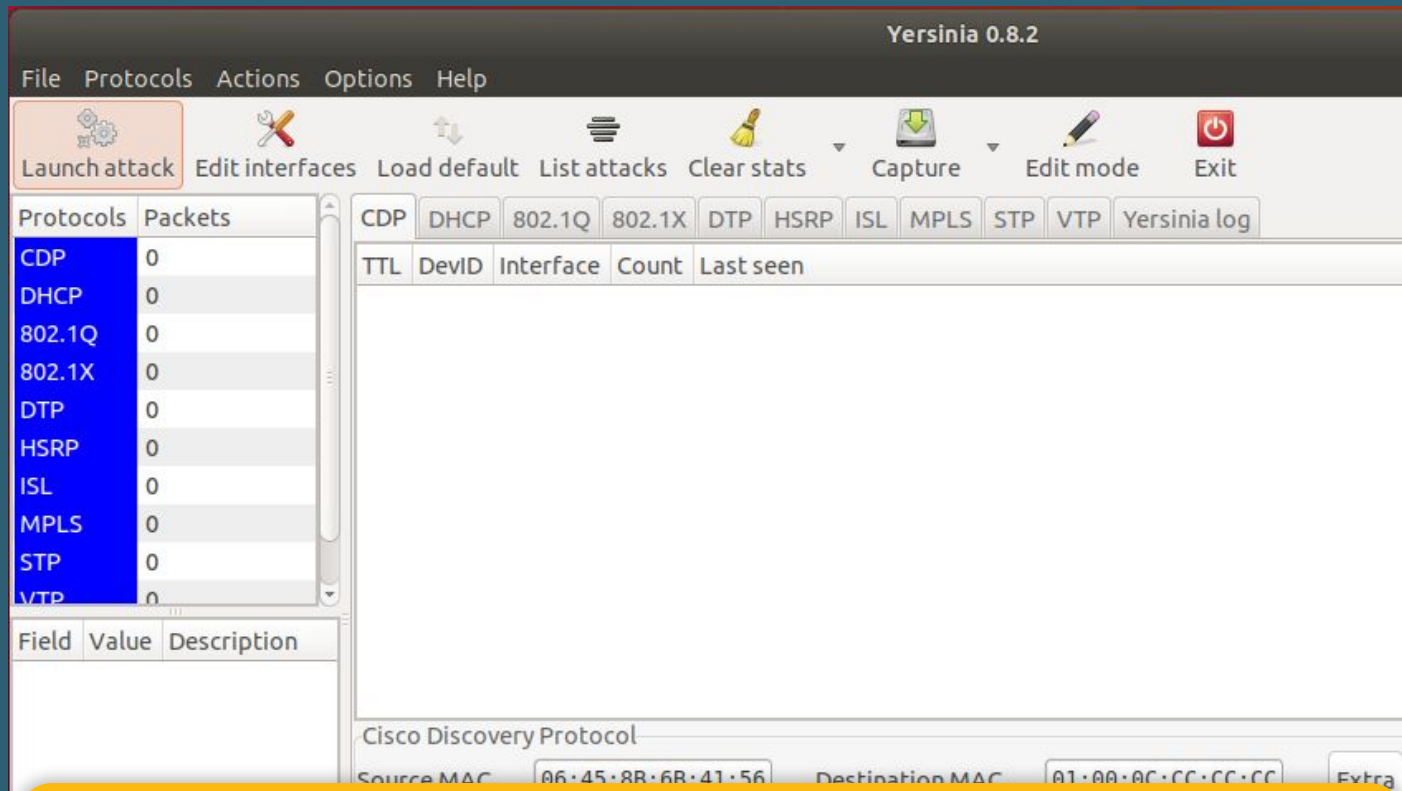
```
sudo apt-get install yersinia
```

- To open a graphical interface version of Yersinia, the '-G' option can be used:

```
yersinia -G
```

Slide 5, 6 – Demonstration Preview:

These slides cover the tool that you'll use to conduct the demonstration, essentially previewing the steps that you'll take in the upcoming demonstration.



Slide 5, 6 – Demonstration Preview:

These slides cover the tool that you'll use to conduct the demonstration, essentially previewing the steps that you'll take in the upcoming demonstration.

Yersinia DHCP Starvation Demo

Slide 7 – Demonstration:

This slide marks where the demonstration takes place. At this point, you will either demonstrate live or play a recorded video of your demonstration.

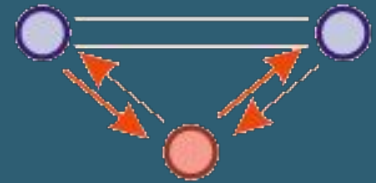
(This presentation has a placeholder slide where the presenter showed the class how to use Yersinia to conduct a DHCP attack.)

Effects of the Attack

- Legitimate clients are unable to lease IP addresses.
- The attacker can deny legitimate network users service, resulting in a Denial of Service.
- Attackers can then supply an alternate DHCP connection that leads to a Man-in-the-Middle (MITM) attack using a rogue DHCP server.
- When a rogue DHCP server is established, all network traffic between devices on the effected network can be snooped on.

Slide 8 – Demonstration Summary:

This slide summarizes the demonstration that was just conducted and any impact that such an attack may have.

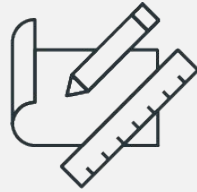


Mitigating DHCP Starvation Attacks

- Port security allows you to specify MAC addresses for each port or to permit a limited number of MAC addresses.
- Another solution is to manually pre-register MAC addresses of allowed devices before their first connection into the network.
- In cases where an attacker uses the same MAC address in the Ethernet packet and changes it in the DHCP payload packet, DHCP snooping can be utilized to make sure the MAC addresses match up.
- Additionally, a policy can be created to limit the amount of MAC addresses allowed to be registered over a period of time.

Slide 9 – Mitigation:

This slide provides recommendations for mitigating the attack if the demonstration was an attack.



Daily Schedules, Objectives, and Deliverables

Daily Structure

Like previous project weeks, class will run differently than usual this week.

The first two days will proceed as follows:

Part 1:

A brief lecture (we've already done today's).

Part 2:

Students will use the remaining class time to work on their presentations.

Project Deliverables

For this project, you will develop and submit the following deliverables, which you can take with you and discuss at job interviews:

Deliverable 1

Each student must submit the presentation slides that their team uses for Day 3's presentation.

Deliverable 2

Any additional resources or documents created or prepared for the presentation, such as:

- Recordings
 - GitHub code
-



Activity:

Project Presentation Preparation

For the remainder of today's class, you'll work on researching and completing your presentations.

Suggested Time:
End of Class





Questions?





The End