# *IT Security (420-F30-HR)*

# *Lab 13 – Business Practices I*

Date assigned: Thursday May 2

Date Due: Thursday May 2, end of lab (it’s a short lab)

**Objectives:**

Learn:

1. The purpose and functions of a honeypot
2. Phishing, phishing expeditions and metrics
3. Ethical hacking, pen testing and bug bounties
4. Canadian Cybersecurity recommendations

# Honeypot

Research honeypots [here](https://www.kaspersky.com/resource-center/threats/what-is-a-honeypot).

|  |  |
| --- | --- |
| What is the definition of a honeypot? | A honeypot baits hackers into attempting to intrude a sacrificial computer system (a decoy) to gain information about cybercriminals and the way they are operating or to distract them from other targets. |
| Explain how honeypots work | It looks like a real system with apps and data, tricking cybercriminals. Its not set up for a specific problem, but to study attackers’ tactics and using that information to further fortify your system. |
| How can spam be automatically detected using a honeypot? | Email traps or spam traps place a fake email address in a hidden location where only an automated address harvester will be able to find it. |
| What are the 5 things you can assess by monitoring the honeypot system? | where the cybercriminals are coming from  the level of threat  what modus operandi they are using  what data or applications they are interested in  how well your security measures are working to stop cyberattacks |

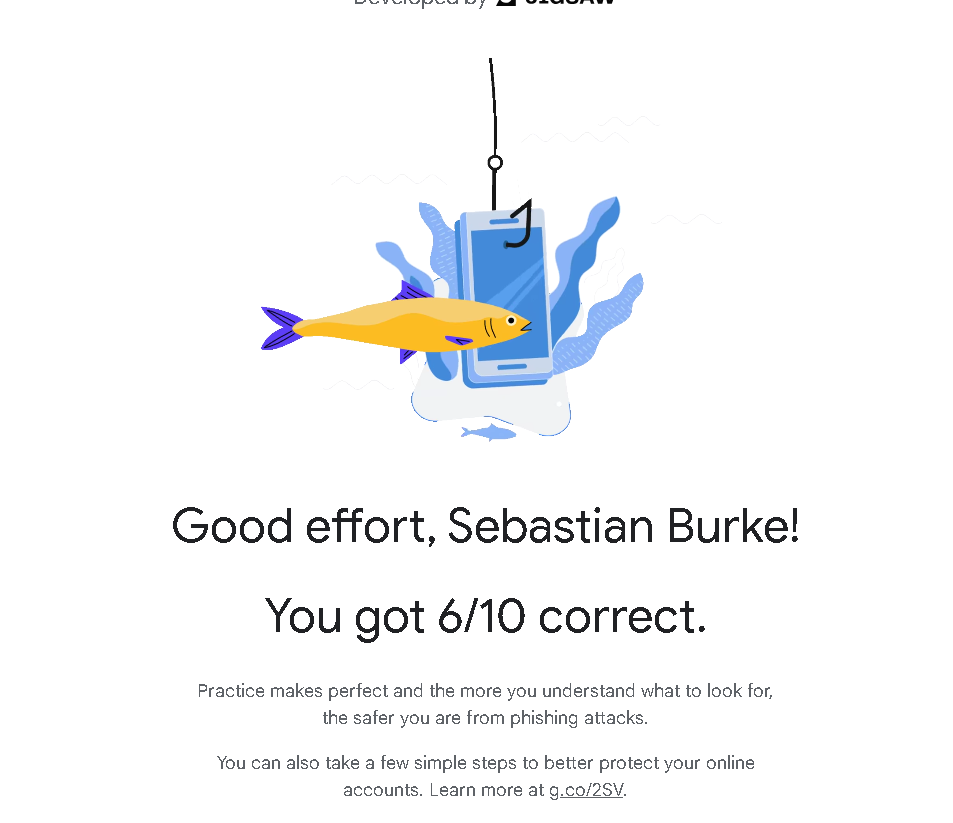
# Phishing

Research and answer

|  |  |  |
| --- | --- | --- |
| phishing | Define “phishing” and include URL | <https://www.cyber.gc.ca/en/guidance/dont-take-bait-recognize-and-avoid-phishing-attacks>  Phishing is a type of cyberattack where a scammer tries to trick you into giving them sensitive information, like your passwords, credit card numbers, or personal details.  Phishing can happen through:   * Emails * Text messages (SMS phishing or "smishing") * Phone calls (voice phishing or "vishing") * Fake websites that look real |
| spear phishing | Define “spear phishing” and include URL | <https://www.fortinet.com/resources/cyberglossary/spear-phishing>  Similar to a phishing attack but the intent is to go after a specific individual, whereas phishing takes a blanket approach targeting multiple victims. |
| [McGill](https://reporter.mcgill.ca/mcgills-phishing-expedition/) | What was the likelihood of a user getting fooled by a Phishing email? | 1 in 6 |
| [Phishing Activity](https://apwg.org/trendsreports/) | What was the Phishing trend for 2023?  How many attacks in the last quarter of 2023?  What is “vishing” | Worst year ever recorded for phishing attacks: almost 5 million attacks observed in 2023.  1,077,501 phishing attacks happened just in the 4th quarter (Oct–Dec 2023).  Attacks against social media platforms exploded in late 2023, making up 42.8% of all phishing attacks — a huge shift compared to previous years.  Voice phishing ("vishing") kept rising every single quarter of 2023.  Business Email Compromise (BEC) attacks involving wire transfers increased by 24% in Q4 compared to Q3, but the average amount stolen per attack decreased to $56,195. |

Do the [phishing test](https://phishingquiz.withgoogle.com/).

Paste in your result: (I got 7/8, but you can do better).



# Ethical hacking, Pen testing, Bug Bounty

Covered in the lecture and further research:

|  |  |  |
| --- | --- | --- |
| [Motivation](https://cisomag.com/whitepaper-bug-bounty-programs/) | What is the motivation for companies to have a bug bounty program.  What is the average bounty paid out. | The motivation is to incentivize developers to attempt to fix bugs for the company without them having to hire individually. It takes stress off the companies’ shoulders.  $505.79 |
| Intel | How much is the maximum bounty if you find a critical vulnerability in Intel hardware? (,  A critical bug in Intel software? | Critical vulnerability in Intel hardware $100,000  Critical vulnerability in Intel software $10,000 |
| Apple | How much is the bounty if you can figure out how to access someone’s iCloud account data on Apple Servers by them just clicking on a link/button | $10,000 – $100,000: For unauthorized access to iCloud account data associated with an Apple ID that doesn't belong to you. ​  [https://security.apple.com/bounty /categories/](https://security.apple.com/bounty/categories/?utm_source=chatgpt.com) |
|  | What is the difference between ethical hacking and pen testing? | Ethical hacking is broad – Practice of using hacking skills legally to find a fix security problem.  Pen Testing is specific type of ethical hacking – Focuses on simulating an actual cyberattack against a system to find weaknesses. |
|  | What does a pen tester do? | Acts like a hacker to test defenses, but with permission. |
|  | Explain in your own words, the difference between white hat, gray hat and black hat hackers. | White hat – good guys, have permission, protect, and secure systems.  Gray hat – in the middle, may hack w/o permission, but not for evil reasons.  Black hat – bad guys, break into systems illegally. |

# SIEM

Review a [sample product](https://cybersecurity.att.com/products/ossim) used for monitoring. Video overview: [AlienVault](https://www.youtube.com/watch?v=Z8u_Kls6WlE)

Collect information from each of the sections and fill in the table.

|  |  |
| --- | --- |
| Question | Answer |
| What does “SIEM” stand for ? | System information and event management |
| What is the primary functions of AlienVault. | Monitors, detects, and responds to security threats |
| Once an incident is detected, what are the possible responses? | General alarms, automatically notify security teams, provide investigation tools, and recommend specific response actions |
| How does the tool identify software versions that may be vulnerable? | Automated vulnerability scans that compare software version against known vulnerability databases. |

# Canadian Cybersecurity Best practices

Using content from [this page](https://www.cyber.gc.ca/en/guidance/baseline-cyber-security-controls-small-and-medium-organizations) and lecture slides provided, answer the following questions.

Collect information and fill in the table.

|  |  |
| --- | --- |
| Question | Answer |
| Why are these considered “Baseline cyber security controls” and how is it tied to the 80/20 rule? | They aim to achieve 80% of the benefit with 20% of the effort, helping small and medium organizations get strong protection with limited resources. |
| What is the size of the intended organizations for the baseline cyber security control recommendations? i.e. how is “small and medium organizations” defined? | Organizations with fewer than 500 employees (less than 499 employees). |
| What is the recommended cloud certification? | Cloud Service Providers should have certifications like ISO 27001 or similar recognized standards. |
| What standard is recommended for securing websites | Use HTTPS for websites and follow secure website configuration best practices. |
| What principle should be followed when implementing Access Control and Authorization | The Principle of Least Privilege — users should have the minimum access necessary to do their jobs. |
| What is the recommendation for USB Flash drives? Are they to be banned? | Not banned outright, but organizations should secure portable media (e.g., encrypt USB drives and control their use). |
| What is the recommendation for organizations that want to go beyond the baseline practices? (Hint: a framework you already know) | Follow a full framework like ITSG-33 (Canada’s version of NIST Cybersecurity Framework or ISO 27001). |
| What is the plan on how to respond and recover from cyber security incidents called? | An Incident Response Plan. |
| How often should passwords be changed? Monthly, annually? | Only when there is suspicion or evidence of compromise — not monthly or annually by default. |

Map the Canadian controls to the NIST framework lifecycle steps:

Diagram

Description automatically generatedS

|  |  |  |
| --- | --- | --- |
| Section | Section Title | NIST Lifecycle stage |
| 2.2 | Determine what information technology is in scope | Identify |
| 2.3 | Determine the value of information systems and assets | Identify |
| 2.4 | Confirm the cyber security threat level | Identify |
| 2.5 | Confirm cyber security investment levels | Identify |
| 3.1 | Develop an incident response plan | Protect |
| 3.2 | Automatically patch operating systems and applications | Protect |
| 3.3 | Enable security software | Protect |
| 3.4 | Securely configure devices | Protect |
| 3.5 | Use strong user authentication | Protect |
| 3.6 | Provide employee awareness training | Protect |
| 3.7 | Backup and encrypt data | Protect & Recover |
| 3.8 | Secure mobility | Protect |
| 3.9 | Establish basic perimeter defences | Protect & Detect |
| 3.10 | Secure cloud and outsourced IT services | Protect |

**Marking Scheme**

|  |  |
| --- | --- |
|  | **Out of** |
|  |  |
| **Part A: Honeypot** |  |
| 1 | 2 |
| 2 | 2 |
| 3 | 2 |
| 4 | 5 |
|  |  |
| **Part B: Phishing** |  |
| 1 | 2 |
| 2 | 2 |
| 3 | 2 |
| 4 | 2 |
|  |  |
| **Part C: Ethical hacking, Pen Testing, Bug bounty** |  |
| 1 - Motivation | 4 |
| 2 - intel | 4 |
| 3 - apple | 2 |
| 4- ethical hacking vs pen testing | 2 |
| 5 – Pen tester | 2 |
| 6 – hackers {white,gray, black} | 6 |
|  |  |
| **Part D: SIEM** |  |
| 1 | 2 |
| 2 | 2 |
| 3 | 2 |
| 4 | 2 |
|  |  |
| **Part E: Canadian Baseline** |  |
| Table 1 (8x2) | 16 |
| Table 2 (14x1) | 14 |
|  |  |
| Handed in properly | 4 |