CS 4404 - Network Security

Mission 3 (25 points)
Launched: Monday, Nov. 28, 2022
Due: Monday, Dec. 12, 2022 at 11:59:00pm

Mission 3: Novel IDS IDeaS

Many organizations are concerned that attackers will gain access to their networks and try to spread laterally or exfiltrate data. These organizations would like to deploy intrusion detection systems (IDSes) that will alert them to any suspicious behavior, and in the case of a breach, identify other systems that may have been affected.

In class, we just read about the Bro IDS and its design concepts, but there are other ways to monitor networks. The NetFlow feature from Cisco enables the logging of communication between endpoints using a flow tuple (typically including the source and destination IP addresses, source and destination ports, and the IP protocol field). This allows an administrator to figure out everyone communicating through the monitoring point (which is typically a border router).

With the advent of software-defined networking (SDN), the OpenFlow protocol (which is not related to NetFlow) allowed a centralized monitoring device to gain insight into network activities. When switches act in a "reactive mode" in OpenFlow, they essentially contact an OpenFlow controller for instructions on how to forward packets associated with any new connection. As a result, the OpenFlow controller can learn when each new connection is established between any endpoints communicating via a reactive OpenFlow switch.

In this mission, we will explore these three different monitoring techniques, identify their strengths and weaknesses, and deploy one of the techniques to discover attacks that previously went unnoticed.

Reconnaissance Phase

In this phase, we will first explore what tools are available and how we can use them. We will focus on the following three categories:

1. **Packet inspection tools:** Tools like Bro and Snort allow the deeper inspection of every packet they see and can apply rules or anomaly detection methods.

2. **Flow monitoring tools:** The popularity of NetFlow has resulted in a wide-range of flow collection and analysis tools.

3. **SDN-based monitoring:** Within the SDN paradigm, multiple techniques have been created to explore network communication on a controller and middleboxes.

Students should identify the sets of tools, their strengths and weaknesses, and how a defender would deploy them on a network for each of the above categories. Students should describe how performance and scalability goals may affect the technique's ability to ensure certain security goals. Students should also identify the goals an attacker may have in communication with compromised hosts and describe how these techniques may affect those goals.

Students are encouraged to explore research papers and other documents that can describe how to perform network monitoring effectively. For the SDN-based monitoring category, students must read and analyze the TLSDeputy paper[2] by Taylor and Shue. That paper describes how OpenFlow and IDSes can be combined to achieve detailed insights into communication.

[2] https://web.cs.wpi.edu/~cshue/research/cns16.pdf

Infrastructure Building Phase

Using the virtual machines on the isolated computer network in the Zoo lab, the students should create a client system that will simulate an “compromised” victim. Importantly, this compromised machine must run benign software that attempts to communicate as if it were compromised, but it **must not be malicious**, which precludes the use of real malware in this project. We will call this software a “bot” for simplicity despite its lack of malicious payload.

Based on the attack and defense the students choose to use, the rest of the VMs may be used for monitoring, for adversary coordination (e.g., “command and control” infrastructure), or may be infiltration targets (e.g., for lateral propagation).

Naturally, if the only traffic that appears on a network is malicious, it is trivial to prevent attacks by blocking everything. Accordingly, students should discuss what other traffic will exist on the network and any other legitimate infrastructure that may be present. Students will need to implement the other legitimate infrastructure along with a mechanism that generates this legitimate traffic. Students will also need to create appropriate infrastructure that will allow them to evaluate how effective any defense is at alarming on malicious traffic (a “true positive”) while avoiding false alarms (a “false positive”).

Attack Phase

Based on the insight gained from the reconnaissance phase, the students will implement a bot that has the ability to communicate with its command and control systems or propagate laterally. This bot must communicate on a periodic basis in order to give the defense opportunities to detect (or fail to detect) the communication. Students are encouraged to read about “covert channels” for covering bot communication to command and control infrastructure.

The design and sophistication of the bot’s communication strategy will directly influence the scoring for this component. A simple bot that is easy to detect will receive a low score whereas a sophisticated bot that is difficult to detect will earn a higher score. Naturally, since students are building both the attack and defense, they will know how to detect the bot’s traffic and design an appropriate defense. However, a bot is considered pretty sophisticated if can only be detected by a defender that knows the details of its communication. Since the defense phase described below is judged based on its ability to detect a sophisticated attack, a simplistic bot communication channel will limit a team’s ability to demonstrate a sophisticated defense and would affect the score in both the attack and defense phase.

Defense Phase

Regardless of the stealthiness of the bot design, it must communicate and that means that the bot can be detected from the network’s perspective. With advanced knowledge of the bot they built in the attack phase, students should design an intrusion detection and prevention system that can detect the traffic to and from the bot and block then it. The students must then create a defense that is capable of blocking similar bots in as robust a fashion as possible.

The design and sophistication of the defense will directly influence the scoring for this component. A trivial solution, such as simply blocking all traffic from the host running the bot would be effective, but would not earn points for this component because it would block all legitimate traffic as well. The goal is not to achieve a perfectly accurate and comprehensive IDS that can stop all malicious communication; such a system remains elusive for the network security community. Instead, the goal should be to develop a solution that would be effective even against a particularly sophisticated malicious communication channel.

Mission Debriefing Report

The Mission Debriefing Report is the team’s opportunity to demonstrate their understanding of covert channels and sophisticated IDS techniques. The report should include all the results from the reconnaissance phase. The report should then focus one approach to constructing a stealthy communicating bot, the metrics used for determining success at remaining covert, along with the relevant evaluation results. The report should then provide a feasible solution that detects such a sophisticated bot.

The Mission Debriefing Report should be comprehensive and provide conclusive supporting evidence. It is likely that such a report will be at least five pages of write-up and any figures, followed by an appendix of supporting evidence (e.g., screenshots, output of terminal windows, log file output). In addition to the write-up, the debriefing report should include additional supporting files, such as source code or configuration files. For the report to be scientifically valid, enough detail must be provided that would enable the grader or another member of the class to create and run the experiment without the need to ask questions.

Mission Rubric

The mission score can be broken down into five components, each of which are scored independently. The total score is out of 25 points. The following are the components:

1. Reconnaissance: 4 points
2. Infrastructure Building: 5 points
3. Attack: 5 points
4. Defense: 5 points
5. Mission Debriefing: 6 points

When working together, teams are required to evaluate their partners. While no additional credit is awarded for completion of these evaluations, a **3 point penalty** will be assessed to the project grade for any student working in a team who fails to complete a project partner evaluation.

We now describe each of the project components and how they are graded.

Reconnaissance: 4 points

Rubric:

- 4 points: The team has identified a comprehensive set of security goals for the targeted system. Each security goal is described in detail and the impact of not achieving the security goal is clearly stated. The description includes at least one realistic attack vector for each security goal. The countermeasures for each attack vector are likely to be effective and realistic to deploy.
- 3 points: The reconnaissance phase is generally good, but a key security goal may be missing. Alternatively, one or more security goals is not described in sufficient detail or the attack vectors or countermeasures are not fully developed or are unrealistic. This score reflects solid work with relatively minor deficiencies.
- 2 point: The reconnaissance phase omits two or more key security goals. Alternatively, multiple security goals lack detail or attack vectors or countermeasures are poorly formulated or unrealistic. This score reflects work with moderate deficiencies.
- 0 points or 1 point: The reconnaissance phase has significant limitations. The work does not demonstrate a comprehensive review of the problem or the analysis is severely flawed.

Infrastructure Building: 5 points

Rubric:

- 5 points: The infrastructure is realistic and appropriate for the scenario evaluated. The details of the design are obvious with clear configuration files and step-by-step instruction on how the team built the infrastructure. An independent party would clearly be able to follow these instructions to quickly replicate the experimental setup. There is clear evidence that the team learned how to use the provided infrastructure and gave serious consideration into the best configuration that would enable a clear demonstration of the attack and its defense.
- 4 points: The infrastructure setup is generally good, but some details may be missing or some steps in the instructions may have minor errors. With some problem-solving efforts and additional time, an independent party would likely be able to replicate a close approximation of the experimental setup. The team used the provided infrastructure and designed a configuration that adequately enables a demonstration of an attack and defense.

- 3 points: The infrastructure setup has flaws or significant omissions in its instructions or design documentation. An independent party would have trouble recreating the experimental setup. The team used the provided infrastructure, but the configuration limits the effectiveness of an attack or defense demonstration.
- 2 points: The infrastructure setup is flawed and/or is inadequately described to allow replication. The team deviated from the provided infrastructure or the application of the infrastructure has the potential to undermine the validity of the attack or defense experiments.
- 0 points or 1 point: The infrastructure setup has severe flaws that greatly undermine its utility.

Attack: 5 points

Rubric:

- 5 points: The team identifies a realistic, high-impact attack vector. The attack is implemented flawlessly and the description of the attack and its supporting documentation allows an independent party to replicate the attack. The documentation provides evidence that conclusively shows that the team mounted the attack and that the attack was successful. To earn this score, the attack and/or the implementation of the attack must demonstrate significant independent learning or creative thinking by the team. The attack must be sufficiently complex that the students needed to invent or configure existing tools to effectively launch it.
- 4 points: The team identifies a realistic attack vector. The attack is implemented well and the supporting documentation is solid, but may be missing minor details that are needed to replicate the attack. The supporting documentation generally shows the attack was implemented and was likely successful. The attack showed that the students learned about a new way to launch an attack, but the team may have used an obvious or straightforward methodology to launch the attack.
- 3 points: The team identifies an attack vector, but it may be low impact or may be less realistic. The attack implementation or its supporting documentation may have small flaws. The supporting evidence suggests the attack was implemented and may have been effective, but the support is not conclusive. The attack itself may not have been sophisticated or provided significant learning opportunities for students.
- 2 points: The students identified an attack vector, but it may be low impact or unrealistic. The supporting documentation or evidence of the attack is lacking. The attack itself is trivial and there is little evidence the students learned much from the exercise.
- 0 points or 1 point: The attack has severe flaws that greatly undermine its utility.

Defense: 5 points

Rubric:

- 5 points: The team identifies a realistic, high-impact defense. The defense is implemented flawlessly and the description of the defense and its supporting documentation allows an independent party to replicate the defense. The documentation provides evidence that conclusively shows that the team mounted an effective attack and that the defense prevented the attack from being successful. To earn this score, the defensive approach and/or the implementation of the defense must demonstrate significant independent learning or creative thinking by the team. The defense must be sufficiently complex that the students needed to invent or configure existing tools to effectively deploy it.
- 4 points: The team identifies a realistic defensive strategy. The defense is implemented well and the supporting documentation is solid, but may be missing minor details that are needed to replicate the defense. The supporting documentation generally shows the defense was implemented and was likely

successful. The defense showed that the students learned about a new way to protect a system, but the team may have used an obvious or straightforward methodology to deploy the defense.

- 3 points: The team identifies a defensive strategy, but it may be low impact or may be less realistic. The defense implementation or its supporting documentation may have small flaws. The supporting evidence suggests the defense was implemented and may have been effective, but the support is not conclusive. The defense itself may not have been sophisticated or provided significant learning opportunities for students.
- 2 points: The students identified a defensive strategy, but it may be low impact or unrealistic. The supporting documentation or evidence of the defense is lacking. The defense itself is trivial and there is little evidence the students learned much from the exercise.
- 0 points or 1 point: The defense has severe flaws that greatly undermine its utility.

Mission Debriefing Document: 6 points

The mission debriefing document includes the write-up associated with the reconnaissance, attack, and defense. The primary grading of those sections are described above. The mission debriefing document includes overall communication strategy, organization of the information, and interpretation of the data. It also includes supporting appendices and related files.

Rubric:

- 6 points: The report has an introduction and a conclusion section that clearly explain the scenario being evaluated, its importance, the key components that require evaluation, and the results of the specific attack and defense the team evaluated. The report makes use of figures or tables where appropriate to succinctly inform the reader of results. Key supporting information is placed in an easy to read appendix to the report. Additional files are clearly labeled and easy to understand. A README file is provided describing each of the supporting files. All tools are described and the mechanism to obtain the tools (e.g., URLs, relevant repository names) are provided. Where necessary, appropriate academic or technical sources are referenced and cited. The document is compelling, accurate, and leaves little doubt about the attack, defense, and recommendations.
- 5 points: The report has an adequate introduction and conclusion that describe the scenario, its importance, key components, and results. The report is understandable and makes the appropriate points, but the presentation may be suboptimal. The appendix contains supporting information but may have only basic explanation or description of the information. All the supporting files and evidence are included, but it may take extra time to locate. The tools are described, but information on how to obtain them may be missing in some cases. Some academic and technical sources are cited, but there may be instances in which additional citations would be useful. The document is accurate and descriptive, but the document may not be as convincing due to writing limitations or insufficient evidence.
- 4 point: The report has some flaws or omits some of the important points described above. The report may be unclear or unconvincing in places and supporting evidence may be missing, hard to find, or inconclusive. The report is generally accurate, but with apparent flaws or omissions.
- 0-3 points: The report has deficiencies that hinder understanding, omits important data, or provides inadequate support. One of the report sections may be missing or incomplete.