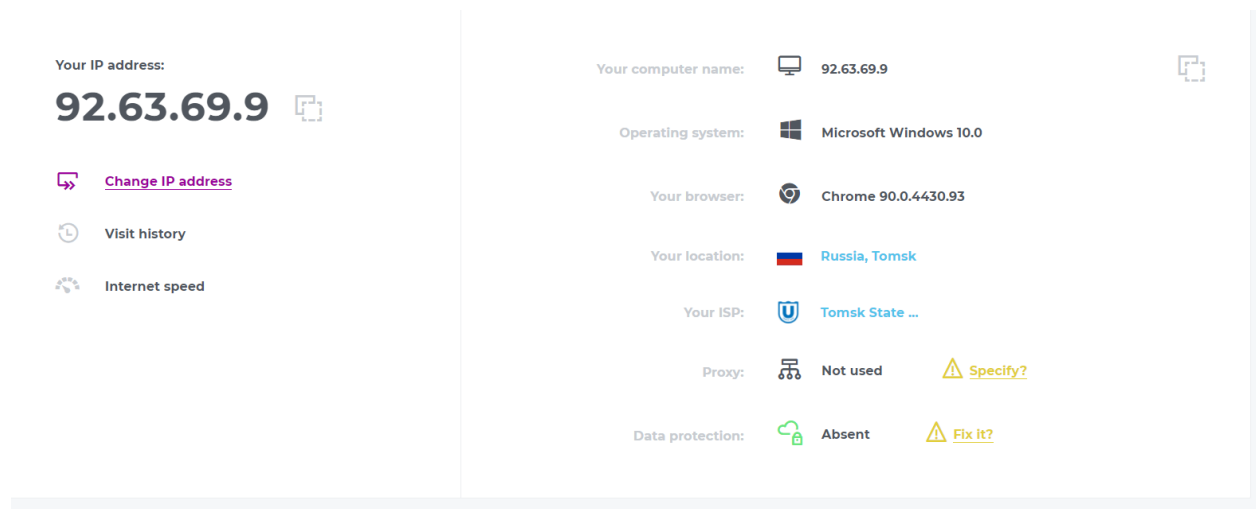


Report

Laboratory 1: Information Security

By: Sneha Shukla

Task1:Using the service <https://2ip.ru/>, determine your external network address (take a screenshot).



The screenshot displays the 2ip.ru website interface, which is divided into two main sections. The left section, titled "Your IP address:", prominently features the external IP address "92.63.69.9" in a large, bold font. Below this, there are three interactive links: "Change IP address" (with a purple icon), "Visit history" (with a clock icon), and "Internet speed" (with a speedometer icon). The right section, titled "Your computer name:", lists various system details. It includes the computer name "92.63.69.9", the operating system "Microsoft Windows 10.0", the browser "Chrome 90.0.4430.93", the location "Russia, Tomsk" (indicated by a Russian flag), the ISP "Tomsk State ...", the proxy status "Not used" (with a warning icon and a "Specify?" link), and the data protection status "Absent" (with a warning icon and a "Fix it?" link). Each item in the right section is accompanied by a small icon representing its category.

Category	Value
Your IP address:	92.63.69.9
Your computer name:	92.63.69.9
Operating system:	Microsoft Windows 10.0
Your browser:	Chrome 90.0.4430.93
Your location:	Russia, Tomsk
Your ISP:	Tomsk State ...
Proxy:	Not used
Data protection:	Absent

Task2:Using the service <https://2ip.ru/port-scanner/>, scan for open ports on your machine. Take a screenshot and analyze the test results.

Security of your computer

Our service allows you to quickly and easily check how secure your computer is on the Internet.

The system automatically detects your address and scans your computer for open ports that can be used for hacking or attacks. It will also scan the ports that open and use the most famous Trojans.

After checking the computer, the system will show you the open ports. Since we only check the most dangerous ports, we strongly recommend that you eliminate all problems detected by our system. To do this, you can use the Firewall program.

If you're ready, then we can get started. To do this, simply click on the "Check" button below and wait for the result. Depending on the speed of your internet connection, the test may take some time, please be patient.

Check

All potentially dangerous ports are closed.
Your system is safe !!!

Task3:Using the service

<https://hidemy.name/en/port-scanner/>, perform a rescanning of ports by entering your network address in the appropriate field. Take a screenshot and analyze the test results. Which ports / protocols / services, in your opinion, are the most dangerous / vulnerable, and which are the most secure?

Enter your IP address or domain

92.63.69.9

[Insert my IP address](#)

Enter your IP address or domain

Popular ports ▼

Test result

Not shown: 999 filtered ports
PORT STATE SERVICE
1723/tcp open pptp
Nmap done: 1 IP address (1 host up) scanned in 20.36 seconds

Start scanning

If the result is "Host seems down", then the network screen or router of the IP address being checked blocks pings.

Enter your IP address or domain

92.63.69.9

[Insert my IP address](#)

Enter your IP address or domain

Found on proxy servers ▼

Test result

All 399 scanned ports on 92.63.69.9 are filtered
Nmap done: 1 IP address (1 host up) scanned in 81.33 seconds

Start scanning

If the result is "Host seems down", then the network screen or router of the IP address being checked blocks pings.

Task4: Review the current document and complete the tasks:

4.1. Select and research one of the list of free intrusion detection systems. Give the features of the IDS under investigation, and explore the interface.

Chosen Intrusion Detection Systems: Zeek

Zeek is a passive, open-source network traffic analyzer. Many operators use Zeek as a network security monitor (NSM) to support investigations of suspicious or malicious activity. Zeek also supports a wide range of traffic analysis tasks beyond the security domain, including performance measurement and troubleshooting.

Features:

- | |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none">• In-depth Analysis: Zeek ships with analyzers for many protocols, enabling high-level semantic analysis at the application layer. |
| <ul style="list-style-type: none">• Adaptable and Flexible: Zeek's domain-specific scripting language enables site-specific monitoring policies and means that it is not restricted to any particular detection approach. |
| <ul style="list-style-type: none">• Efficient: Zeek targets high-performance networks and is used operationally at a variety of large sites. |
| <ul style="list-style-type: none">• Highly Stateful: Zeek keeps extensive application-layer state about the network it monitors and provides a high-level archive of a network's activity. |

Functionalities:

1) The first benefit a new user derives from Zeek is the extensive set of logs describing network activity. These logs include not only a comprehensive record of every connection seen on the wire, but also application-layer transcripts. These include all HTTP sessions with their requested URIs, key headers, MIME types, and server responses; DNS requests with replies; SSL certificates; key content of SMTP sessions; and much more. By default, Zeek writes all this information into well-structured tab-separated or JSON log files suitable for post-processing with external software. Users can also choose to have external databases or SIEM products consume, store, process, and present the data for querying.

2) In addition to the logs, Zeek comes with built-in functionality for a range of analysis and detection tasks, including extracting files from HTTP sessions, detecting malware by interfacing to external registries, reporting vulnerable versions of software seen on the network, identifying popular web applications, detecting SSH brute-forcing, validating SSL certificate chains, and much more.

3) In addition to shipping such powerful functionality “out of the box,” Zeek is a fully customizable and extensible platform for traffic analysis. Zeek provides users a domain-specific, Turing-complete scripting language for expressing arbitrary analysis tasks. Think of the Zeek language as a “domain-specific Python” (or Perl): just like Python, the system comes with a large set of pre-built functionality (the “standard library”), yet users can also put Zeek to use in novel ways by writing custom code. Indeed, all of Zeek’s default analyses, including logging, are done via scripts; no specific analysis is hard-coded into the core of the system.

4) Zeek runs on commodity hardware and hence provides a low-cost alternative to expensive proprietary solutions. In many ways Zeek exceeds the capabilities of other network monitoring tools, which typically remain limited to a small set of hard-coded analysis tasks. Zeek is not a classic signature-based intrusion detection system (IDS); while it supports such standard functionality as well, Zeek’s scripting language facilitates a much broader spectrum of very different approaches to finding malicious activity. These include semantic misuse detection, anomaly detection, and behavioral analysis.

5) A large variety of sites deploy Zeek to protect their infrastructure, including many universities, research labs, supercomputing centers, open-science communities, major corporations, and government agencies. Zeek specifically targets high-speed, high-volume network monitoring, and an increasing number of sites are now using the system to monitor their 10GE networks, with some already moving on to 100GE links.

6) Zeek accommodates high-performance settings by supporting scalable load-balancing. Large sites typically run “Zeek Clusters” in which a high-speed front end load balancer distributes the traffic across an appropriate number of back end PCs, all running dedicated Zeek instances on their individual traffic slices. A central manager system coordinates the process, synchronizing state across the back ends and providing the operators with a central management interface for configuration and access to aggregated logs. Zeek’s integrated management framework, ZeekControl, supports such cluster setups out-of-the-box.

7) Zeek’s cluster features support single-system and multi-system setups. That’s part of Zeek’s scalability advantages. For example, administrators can scale Zeek within one system for as long as possible, and then transparently add more systems when necessary.

8) Zeek is best known for its transaction data. By default, when run and told to watch a network interface, Zeek will generate a collection of compact, high-fidelity, richly-annotated set of transaction logs. These logs describe the protocols and activity seen on the wire, in a judgement-free, policy-neutral manner. This documentation will spend a considerable amount of time describing the most common Zeek log files such that readers will become comfortable with the format and learn to apply them to their environment.

9) Zeek can also easily carve files from network traffic, thanks to its file extraction capabilities. Analysts can then send those files to execution sandboxes or other file examination tools for additional investigation. Zeek has some capability to perform classical byte-centric intrusion detection, but that job is best suited for packages like the open source Snort or Suricata engines. Zeek has other capabilities however that are capable of providing judgements in the form of alerts, through its notice mechanism.

10) Zeek is also attractive because of its ability to run on commodity hardware, giving users of all types the ability to at least try Zeek in a low-cost manner.

Task4.2: Review the documentation of any of the commercial intrusion detection systems and compare the functionality with the previously investigated IDS.

Chosen Commercial Intrusion Detection System: **Check Point IPS**

Check Point IPS is an Intrusion Prevention System (IPS). Whereas the Security Gateway firewall lets you block traffic based on source, destination and port information, IPS adds another line of defense by analyzing traffic contents to check if it is a risk to your network. IPS protects both clients and servers, and lets you control the network usage of certain applications. The new, hybrid IPS detection engine provides multiple defense layers which allows it excellent detection and prevention capabilities of known threats, and in many cases future attacks as well. It also allows unparalleled deployment and configuration flexibility and excellent performance.

Check Point IPS is available in two deployment methods:

- **IPS Software Blade** - integrated with the Check Point Security Gateway to provide another layer of security in addition to the Check Point firewall technology.
- **IPS-1 Sensor** - installed without the Check Point Firewall and dedicated to protecting network segments against intrusion.

Layers of Protection

The layers of the IPS engine include:

- Detection and prevention of specific known exploits.
- Detection and prevention of vulnerabilities, including both known and unknown exploit tools, for example protection from specific CVEs.
- Detection and prevention of protocol misuse which in many cases indicates malicious activity or potential threat. Examples of commonly manipulated protocols are HTTP, SMTP, POP, and IMAP.
- Detection and prevention of outbound malware communications.
- Detection and prevention of tunneling attempts. These attempts may indicate data leakage or attempts to circumvent other security measures such as web filtering.
- Detection, prevention or restriction of certain applications which, in many cases, are bandwidth consuming or may cause security threats to the network, such as Peer to Peer and Instant Messaging applications.
- Detection and prevention of generic attack types without any pre-defined signatures, such as Malicious Code Protector.

In all, IPS has deep coverage of dozens of protocols with thousands of protections. Check Point constantly updates the library of protections to stay ahead of the threats.

Capabilities of IPS

The unique capabilities of the Check Point IPS engine include:

- Clear, simple management interface.
- Reduced management overhead by using one management console for all Check Point products.
- Unified control of both the IPS-1 Sensors and the integrated IPS Software Blade.
- Easy navigation from business-level overview to a packet capture for a single attack.
- Up to 15 Gbps throughput with optimized security, and up to 2.5 Gbps throughput with all IPS protections activated.
- #1 security coverage for Microsoft and Adobe vulnerabilities.
- Resource throttling so that high IPS activity will not impact other blade functionality.
- Complete integration with Check Point configuration and monitoring tools, such as SmartEvent, SmartView Tracker and SmartDashboard, to let you take immediate action based on IPS information.

As an example, some malware can be downloaded by a user unknowingly when browsing to a legitimate web site, also known as a drive-by-download. The malware may exploit a browser vulnerability by creating a special HTTP response and sending it to the client. IPS can identify and block this type of attack even though the firewall may be configured to allow the HTTP traffic to pass.

Task4.3: Investigate any of the vulnerability scanners listed in the document. Check out the software documentation on the official website and describe the functionality and features of the scanner.

Chosen Vulnerability Scanner: **XSpider**

XSpider is a professional vulnerability scanner that allows you to assess the security status of your IT infrastructure. XSpider reveals network components, analyzes them for vulnerabilities and provides detailed recommendations for elimination.

Identifies vulnerabilities

The main purpose of XSpider is to detect vulnerabilities in a timely manner in the company's infrastructure and thereby prevent possible attacks using them before negative consequences occur

Reduces labor costs of information security experts

XSpider allows you to automate the process of monitoring network security, eliminating the need for manual verification of each individual component of the information system. XSpider can be configured to automatically start scanning tasks at the right time. After the scan is complete, the system scheduler can report on the email address or save it to a specified network folder.

Analyzes test results

XSpider provides data on scan results in a convenient and structured form for detailed analysis of the current situation in the system. In XSpider, you can filter and group data, compare the results of different scans, get general status estimates systems and build regulated reports. For all discovered vulnerabilities can receive detailed information and clear recommendations for their elimination. For the convenience of the user, generation and delivery of reports at a specified time is available.

Allows for changes in infrastructure

XSpider mechanisms allow you to conduct a detailed inventory and track changes in the state of the information system. Control over the emergence of new network nodes, changes in the composition of open ports, available services and the operating system makes the IT infrastructure transparent for the IS operator.

Features of Xspider

- **Discovers hosts:**

workstations, servers, network hardware.

- **Scans TCP / UDP ports:**

For a quick check can be manually configured to scan often used ports.

- **Discovers vulnerabilities** in services SMB, RDP, HTTP, SNMP, FTP, SSH

- **Picks up passwords for services** requiring authentication.

- **Analyzes web applications** for presence vulnerabilities (SQLi, XSS, launching arbitrary programs).

- **Carries out an inventory:**

allows you to get basic system information (OS, open ports, available services)

Benefits

Extensive knowledge base

- Specialists from PT Expert Security Center and Positive R&D departments Technologies are constantly researching new threats and regularly submitting data on how to detect them into a unified knowledge base.
- It also supports vulnerabilities from the Information Security Threat Bank (BDU) of the FSTEC of Russia

Low false positive rate

Specially designed algorithms in XSpider allow you to refine the relevance of the identified vulnerabilities, due to which it is possible to achieve high accuracy of the product.

Fast installation and setup

XSpider does not require the deployment of program modules on nodes, which simplifies the operation of the system. All checks are carried out remotely.

Convenient licensing model

XSpider is licensed per verifiable nodes. Users have the ability to independently add the required nodes to the license. There is a possibility of expanding the license.

Low hardware requirements

It is possible to install XSpider both on a hardware platform and in a virtual environment.

Complies with legal requirements

Helps to comply with the requirements of Law No. 152-FZ, orders FSTEC # 21, 17, 31 and 239, PCI DSS international standard.

Conclusion

After doing all the four tasks, I understood the importance of Intrusion Detection System(IDS). No firewall is foolproof, and no network is impenetrable. Attackers continuously develop new exploits and attack techniques designed to circumvent your defenses. Many attacks leverage other malware or social engineering to obtain user credentials that grant them access to your network and data. A network intrusion detection system (NIDS) is crucial for network security because it enables you to detect and respond to malicious traffic.

The primary benefit of an intrusion detection system is to ensure IT personnel is notified when an attack or network intrusion might be taking place. A network intrusion detection system (NIDS) monitors both inbound and outbound traffic on the network, as well as data traversing between systems within the network. The network IDS monitors network traffic and triggers alerts when suspicious activity or known threats are detected, so IT personnel can examine more closely and take the appropriate steps to block or stop an attack.