Sri sankanrs degree college kurnool

**BOYA ANITHA**

**Long term intership**

**Foot printing and reconnassiance**



* Footprinting in the context of cybersecurity refers to the process of gathering information about a target system or network to identify potential vulnerabilities and assess the security posture. Here are the key points:
* **Passive Footprinting**: Involves collecting information without directly interacting with the target system or network. This could include gathering data from public sources such as social media, company websites, search engines, and public databases.
* **Active Footprinting**: Involves directly interacting with the target system or network to gather information. This could include techniques such as port scanning, network mapping, and reconnaissance to identify active hosts, services, and potential vulnerabilities.
* **Open Source Intelligence (OSINT)**: Utilizing publicly available information to gather intelligence about the target. This includes information from websites, social media, online forums, job postings, press releases, and other public sources.
* **Tools and Techniques**: Various tools and techniques are used in footprinting, such as WHOIS lookup, DNS interrogation, network scanning tools like Nmap, web scraping tools, social engineering, and dumpster diving (physically going through trash for sensitive information).
* **Enumeration**: Involves extracting additional information about the target network, such as user accounts, shares, services, and system configurations. Enumeration is typically performed after initial information gathering and can involve techniques like querying DNS records, SNMP enumeration, and querying network services.
* **Ethical Considerations**: Footprinting should be conducted ethically and legally, adhering to all relevant laws and regulations. Unauthorized access to systems or networks is illegal and unethical.
* **Risk Assessment**: The information gathered during footprinting is used to assess the security posture of the target system or network. This includes identifying potential vulnerabilities, entry points, and areas of weakness that could be exploited by attackers.
* **Footprinting as a Phase in Penetration Testing**: Footprinting is often the initial phase in a penetration testing or ethical

hacking engagement. It provides the foundation for subsequent phases such as scanning, exploitation, and post-exploitation.

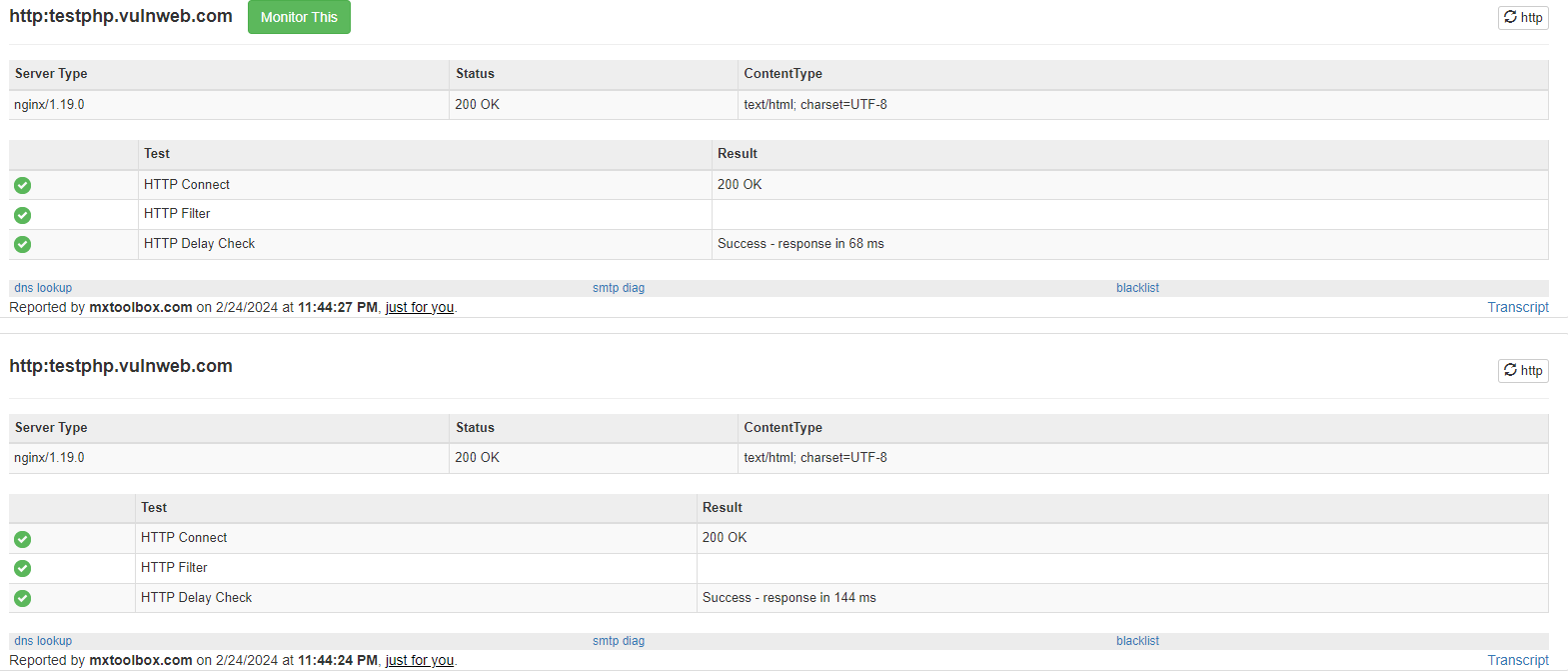
* By understanding the key points of footprinting, organizations can better protect their systems and networks by identifying and addressing potential security risks before they can be exploited by malicious actors.

Reconnassiance and key points

* Reconnaissance, often referred to as recon, is the initial phase of the hacking process where information is gathered about a target system or network. Here are the key points:
* **Purpose**: The primary goal of reconnaissance is to gather as much information as possible about the target to understand its structure, potential vulnerabilities, and the best approach for an attack.
* **Passive Reconnaissance**: Involves collecting information without directly interacting with the target system or network. This includes gathering data from public sources like social media, company websites, search engines, and public databases.
* **Active Reconnaissance**: Involves directly interacting with the target system or network to gather information. This could include techniques such as port scanning, network mapping, and reconnaissance to identify active hosts, services, and potential vulnerabilities.
* **Open Source Intelligence (OSINT)**: A significant part of reconnaissance involves utilizing publicly available information to gather intelligence about the target. This includes information from websites, social media, online forums, job postings, press releases, and other public sources.
* **Tools and Techniques**: Various tools and techniques are used in reconnaissance, such as WHOIS lookup, DNS interrogation, network scanning tools like Nmap, web scraping tools, social engineering, and dumpster diving (physically going through trash for sensitive information).
* **Information Gathering**: Reconnaissance involves gathering information about the target's infrastructure, including IP addresses, domain names, network topology, email addresses, employee names and roles, software versions, and potential entry points.

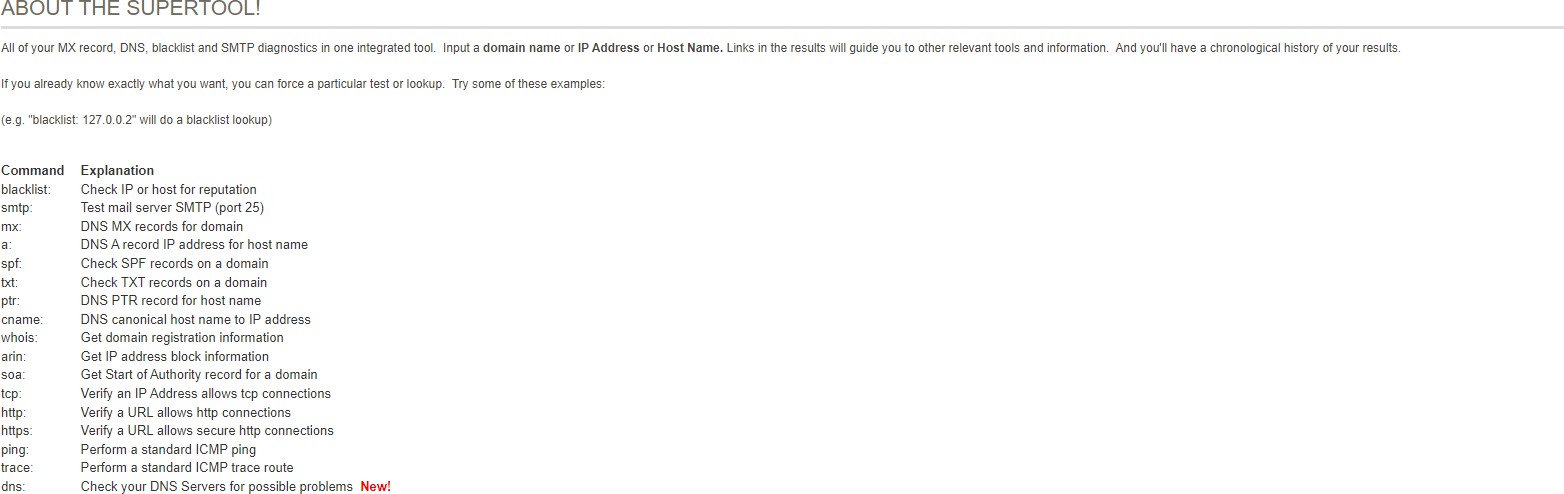
Domain name “Testphp” look up

service

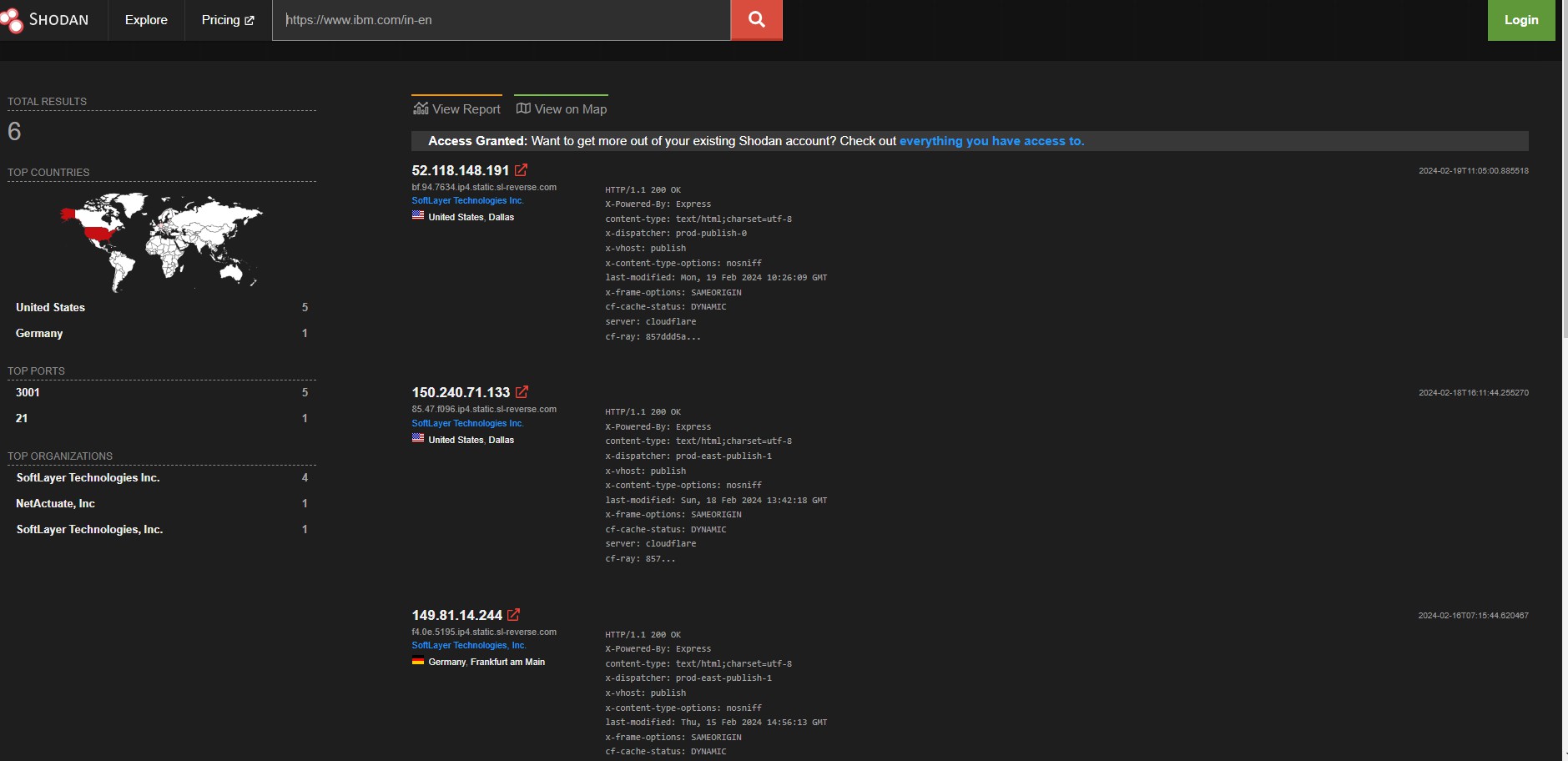


Domain spcefied web site particular

service



Shodan dns we can use web site



Ibm and web site with ip address

