Global Information Assurance Certification Paper

GIAC Certified Incident Handler
Practical Assignment v3

The Tactical Use of Rainbow Crack to Exploit Windows Authentication in a Hybrid Physical-Electronic Attack

Mike Mahurin

Submitted November 22, 2003

Statement of Purpose

The purpose of this paper is to examine how the RainbowCrack tool, a password cracking tool that uses a time-memory trade off technique, can be practically used during a physical intrusion. This tool uses flaws in Microsoft's network authentication scheme to rapidly compromise the password database of a Microsoft Windows 2000 network.

We will examine how the Microsoft LAN Manager (LM) authentication protocol operates and how the cryptographic method used to store passwords is flawed. Once this is complete, we will examine how RainbowCrack uses a faster time-memory trade-off cryptographic technique to rapidly decrypt LM password hashes faster then traditional cracking methods.

A fictitious scenario where a professional attacker is hired by organized crime to retrieve sensitive information from a police file server will be presented. Common social engineering, hacking methodologies, and tools will be used by the attacker to gain access to the network's password database. They will then use the RainbowCrack to decrypt the password of the user with the targeted information. Using this information the attacker will acquire the user's files from an encrypted file share on what is thought to be a secure file server. After this is complete the attacker will cover his tracks and provide himself with a method to access the network in the future.

The organization's security preparations and approach to incident handling will be discussed in detail. Once these are explained, the remainder of the incident handling process will be discussed. The underlying theme of this paper is that electronic and physical security must work hand in hand to provide a secure environment.

The Exploit

Tool Name

The RainbowCrack tool was released by Zhu Shuanglei in October 2003 [1]. This tool is based on the Advanced Instant NT Password Cracker developed by Luca Wullschleger and Cluade Hochreutiner [2]. The underlying cryptographic algorithm for all of the above tools is based on the Faster Time-Memory Trade-Off Technique developed by Philippe Oechslin at the Laboratoire de Cryptographie, EPFL [3].

This attack is possible due to the methods that Microsoft products use to store LM password hashes in the Security Account Manager (SAM) files on domain controllers and the local machine. This program uses pre-generated hashes to determine the user's password from pre-generated hash tables. The end result is

the ability to decipher passwords dramatically faster then older methods. This functionality will be covered in more detail.

Operating Systems Effected

The following operating systems maintain copies of the SAM database with both LM & NTLM hashes stored on the local machine and domain controllers. These systems include all Microsoft Active Directory implantations. This is important because, many administrators assume that newer versions of Windows only store passwords using a secure method by default in newer versions.

- Microsoft Windows Server 2003, Standard Edition
- Microsoft Windows Server 2003, Enterprise Edition
- Microsoft Windows Server 2003, 64-Bit Datacenter Edition
- Microsoft Windows Server 2003, 64-Bit Enterprise Edition
- Microsoft Windows Server 2003, Datacenter Edition
- Microsoft Windows XP 64-Bit Edition Version 2002
- Microsoft Windows XP 64-Bit Edition Version 2003
- Microsoft Windows XP Professional
- Microsoft Windows XP Tablet PC Edition
- Microsoft Windows 2000 Server SP2
- Microsoft Windows 2000 Server SP3
- Microsoft Windows 2000 Advanced Server SP2
- Microsoft Windows 2000 Advanced Server SP3
- Microsoft Windows 2000 Professional SP2
- Microsoft Windows 2000 Professional SP3
- Microsoft Windows 2000 Datacenter Server SP2
- Microsoft Windows 2000 Datacenter Server SP3
- Microsoft Windows Small Business Server 2003, Premium Edition
- Microsoft Windows Small Business Server 2003, Standard Edition
- Microsoft Windows NT Server 3.1
- Microsoft Windows NT Workstation 3.1
- Microsoft Windows NT Advanced Server 3.1
- Microsoft Windows NT Workstation 3.51
- Microsoft Windows NT Workstation 4.0
- Microsoft Windows NT Server 3.51
- Microsoft Windows NT Server 4.0

The following Operating Systems use LM for authentication and transmit the hashes during initial logon to the domain:

Microsoft Windows 95 All Editions
Microsoft Windows 98 All Editions

- Previous Versions of Microsoft Windows

By transmitting the LM hash during authentication, the attacker can intercept the transition and gain access to the hash for cracking using a packet capture utility.

Protocols/Services/Applications Involved

The RainbowCrack tool takes advantage of the Windows LM hashing scheme used to authenticate legacy clients. All versions of the Windows Operating System store LM & NTLM hashes on the local machine and domain controllers by default. This includes Windows 2000 & 2003 Active Directory implementations. LM is the weaker of the two protocols and the primary target of most cracking software. SANS defines this as one of the top 20 vulnerabilities for Windows based systems[1].

LM password hashing begins when the user enters their plain text password when they initially set their password. The password has to be exactly 14 characters, if the user's password is shorter than the 14 characters, the remaining characters are padded with null characters (0x00). All characters are then translated to all uppercase characters. The resulting string is then broken down into two sets of 7 characters. The first set of 7 characters is used to encrypt a set of numbers known as a 'magic number' using the DES Algorithm. After this is completed the second set of 7 characters is used as the DES key and the magic number is encrypted with the DES algorithm. The resulting two sets of ciphpertext are then appended to each other with a DES parity byte at the first byte of each set of 7 characters. The result is one 16 byte string made up of two 8 byte ciphertexts [4]. This value is then stored in the SAM database in conjunction with the users Relative ID (RID) and the NTLM hash.

One of the most glaring weaknesses of this method, is there are two 7 character 56-bit passwords instead of one 112-bit. This gives the attacker the ability to attack a significantly weaker password and the ability to attack two passwords at the same time. By having two separate processes the attacker can attack the passwords in parallel. This would allow multiple machines to be used to simultaneously attack a given password and speed up the attack process.

[1] http://www.sans.org/top20/#w3

To determine the password, the attacker can encrypt the 'magic number' with the DES algorithm using a key that is a guess of the password. When the resulting ciphertext is generated, it is compared to the original hash. If the two hashes are found to be equal, then the attacker has guessed the correct password. Two types of attacks can be used to attempt to determine the account's password. The dictionary attack and brute force are the two theoretical methods commonly used today.

A dictionary attack can take several forms, one being a common word list and the second being a directed word list attack. A common word list is a collection of words that have been found to be commonly used for passwords and are usually weak passwords. The directed word list would be a word list based on information gathered about the person whose password is being attempted to be broken. Information like social security number, birthdates, loved ones birthdates, favorite movies, artists, sports, or other interests are used to expand an existing word list or add entire new word lists. Often directed word list attacks are referred to as 'guerilla' password guessing. Information gathered for a directed password attack can be entered in the dictionary files for most password cracking utilities. An example of a utility that utilizes the directed password attacks is the Access Data Password Recovery Law Enforcement[2] edition. It also takes the concept one step further by indexing a forensic image for every word used on the hard disk, the resulting words are added to the dictionary used in the attack on the password. Most password guessing programs such as LC4[3] by @stake, John the Ripper[4], or Access Data Forensic Tool Kit include a mutation list for word list that add or remove characters and assemble words in unique positions. This method is frequently used in law enforcement forensic investigations. These methodologies can be used for many other types of password attacks that are beyond the scope of this paper.

The other method is to use brute force to attempt to guess all the possible keys in the key range. This will result in a guaranteed crack of the password, but it will take the most amount of time. Using this method all combinations of passwords are attempted against the hashes. Eventually the correct combination will be found and the password will be cracked. Time ranges for this are dependant on hardware, but @stake currently advertises 48 hours on a Pentium II/300 to crack

[2] http://www.accessdata.com/ultimate_overview.htm
[3] http://stake.com/products/lc/
[4] http://www.openwall.com/john/

90% of system passwords. Most software, including LC4, uses a hybrid attack where it first attempts a dictionary attack and then brute force. Personal experience has shown that over 60% of passwords on a 2,000 user network are broken in the first 5-10 minutes on a Pentium III 400 MHz machine using LC4.

To use these tools, the attacker must get the SAM database from a local machine or domain controller. By default, all Windows based servers keep a copy of the LM hashes and the NTLM hashes stored on the local machines and domain controllers. Windows requires administrative or local system rights to allow the user to copy the SAM database. The attacker has several methods they can use to get the SAM database. The methods discussed here are running a SAM dump utility, from backup media, or from sniffing the network traffic.

The first and easiest method to gain the SAM database is to use a program such a samdump[5], pwdump, pwdump2[6], or pwdump3v2[7] to copy the SAM database to a text file. Pwdump3v2 is the current best option for acquiring the password hashes from a remote machine. These programs are run from the command line and must be run as administrator or a domain administrator. Many hacking techniques can be used to run the program as an administrator. A buffer overflow could be used to remotely gain administrator access and execute the program. A Trojan horse program could be used to hide the pwdump3v2 file and social engineering used to convince an administrator to run it. Yet another option could be to use a Unicode exploit on IIS to run a script file that runs pwdump3. The possibilities are endless to gain access and run the program under administrative context.

Other methods to gain access to the hash files are to gain access to the physical machine or backup media. Booting the system from a Linux boot disk or using a program like Winternals ERD Commander[8] can allow access to the SAM through booting on an alternate operating system. The SAM can be found on the system partition at %systemroot%\system32\config. If the attacker has access to backup media or Windows Backup can be used, a backup of the system state can acquired on Windows 2000/2003, and the SAM database acquired. In Windows NT 4.0, the emergency recovery disk can be acquired or the rdisk command can be executed to make an emergency repair disk. This disk contains a copy of the

[5] http://www.atstake.com/products/lc/dist/samdump.zip
[6] http://razor.bindview.com/tools/desc/pwdump2_readme.html
[7] http://www.polivec.com/Downloads/pwdump3v2.zip
[8] http://www.winternals.com/products/repairandrecovery/

SAM database. Many administrators fail to secure this media, making theft a real possibility.

The last method that can be used to gain access to the SAM database is through capturing network traffic using a packet capture utility such as Ethereal[9] to look at authentication traffic. LC4 has an integrated network sniffing tool that allows authentication traffic to be captured off the network. In a switched environment, this can be a difficult process. The attacker would have to find a way to get between a file share or domain controller during an authentication to capture the hashes. If the attacker used ARP Cache Poisoning they may have problems handling the traffic volume to the server as well as the processing overhead. Another method could be to flood the switch with ARP traffic to force the switch to behave like a hub. The switch will copy every packet transmitted and broadcast it to every port. This would allow the attacker to capture traffic that was being transmitted between a domain controller and a workstation. The attacker could get the hash by sending an email that had a link to a share on which they had a capture utility. When the user clicked on the link they will use pass-through authentication to the machine indicated in the URL and the attacker could intercept the hash [5].

Variants

The RainbowCrack tool is an off-shoot of the Advanced Instant NT Password Cracker developed by Luca Wullschleer and Claude Hochreutiner. RainbowCrack was released due to Advanced Instant NT Password being pulled from the website. Other password cracking utilities such as LC4 or John the Ripper are variations of password attacks, but RainbowCrack uses pre-generated Hash tables instead of guessing hashes from a dictionary or brute force attack. This change in technique makes it dramatically faster, up to a factor of over 12 times faster the traditional methods. This differentiates RainbowCrack from other previous password cracking tools and places it in its own category.

Description

RainbowCrack utilizes the concept of an optimized fast-memory trade-off developed by Philippe Oechslin using pre-generated hash tables known as Rainbow tables to decrease the decryption time of a Windows LM password

[9] http://www.ethereal.com

hash from 101 seconds to 13.6 seconds. The fast-memory trade-off theory by Oechlin is a refinement of the theory originally proposed by Martin Hellman in 1980 [6] and later refined by Rivest in 1982 [7].

Before the time-memory trade off was developed by Hellman, there were only two options that could be used to acquire a key from a cryptographic system that uses a key to encrypt a block of constant plaintext. The first method was to use all possible keys one at a time. Theoretically the time required to determine the key would be equivalent to the time required to attempt every possible key. In a Windows based system, this would require approximately 3 days to complete a full key space using a Pentium 4 1.5 GHz performing 700,000 attempts per second with a key space of 80,603,140,212 which is a 7 byte alphanumeric LM password if the password was 7 characters or less, it would be doubled for a password over 7 characters.[10] This is due to LM passwords being separated into two 7 byte passwords.

The second exhaustive search method would be to have all the possible password/hash combinations stored on disk. The plaintext key would be 7 bytes in length, the storage for the hash would be 8 bytes in length. The difference in size is due to the parity bit LM stores with the hash. This would result in a table that required approximately 564 Gigabytes of storage for the keys and approximately 644 Gigabytes for the ciphertext hashes with at least 1.20 Terabytes total space.[11] The look up time for they key would be limited by the input/output speed of hard disks where the table is located. On a modern machine, this would be less then 1 minute. Even by today's standards, over 1 Terabyte is an extreme amount of storage space to break LM hashed, but is theoretically possible.

Hellman introduced the Time-Memory Trade-Off technique in 1980 to address this problem [6]. This theory relies on the fact there are two key factors in finding a key, Memory used (M) and Operations or time (T). Either of these factors can be manipulated to strike a balance between an extreme amount of time or memory detailed previously in decrypting a LM password. His theory is probabilistic in nature, so the confines of time and memory have to be manipulated to set a desired success rate. Operationally, the theory works by generating a given number of chains (m) that contain a certain number of keys

[10] Found by the equation (Keyspace/Attempts per second) * 2 7-byte hashes
[11] Found by the equation Space for Keys = (Keyspace * 7 bytes) Space for Hashes=(Keyspace * 8) Total Space=Space for Keys + Space for Hashes

(t). A reduction function which is an arbitrary reduction function is run against the ciphertext to produce a key that is shorter then the ciphertext. The reduction (R) function is run repeatedly until the end of the chain (t) is reached. The reduction function is an arbitrary removal of a portion of the chain. The chains are then sorted and the beginning and end points of the chains are recorded in the table while the intermediate points in the chain are discarded. This creates a benefit in memory at the cost of time. Once these tables have been generated, we can create a chain for a given ciphertext and run it through the reduction function R with a chain length of t to generate keys. We then compare those to the endpoint point we have stored from the initial table generation. When a match is found the starting point for that chain is used to regenerate the complete chain for that row. The key is then located in that chain and should be the key used to encrypt the original ciphertext.

A problem with this technique is that due to the size of the tables and the fact R is an arbitrary reduction, the key spaces can collide and create non-unique keys and invalid keys that look the same after the reduction function. To compensate for loss in success probability from these collisions and merges, more tables each with a different reduction function have to be used. False alarms also happen with this method, this is where a matching end point is found, but the key is not in the chain. This slows the process down, because to detect this the program has to generate the full chain and test each key in the chain.

Rivest [2] suggested modifying this theory by implementing the concept of distinguished points. This idea states that a criterion for the key should be defined as being significant. Only items that are significant will be stored in memory, which would include the end points. The ciphertext would then be used to generate a set of keys until the criterion for the distinguished points is met, then it would be checked against the table. This would result in a lowering of the number of table lookups that would have to be performed.

The time-memory trade off method developed by Oechslin optimizes the previous theories by introducing the concept of rainbow chains and rainbow tables. Utilizing a successive reduction function that is related to t, the chains will not merge. Merging occurs when chains have the same endpoints, which causes the chains to be regenerated for comparison. Implementing changing reduction functions lowers the chance of a merge on the table and makes the lookups more efficient.

To further enhance this process multiple rainbow tables can be created to increase the probability of success. Probability of success will dictate the size and the number of the tables that will need to be used. In the case of breaking LM passwords we would want a 99.99% chance of breaking any given password. The primary purpose is the administrator account is the primary target of the attack, since it has the most authority on the system. If any user account would due for the attacker the size and number of the rainbow tables could be reduced. The end result of this method is decryption of LM passwords at a factor of 12 times faster then the traditional methods of password cracking.

The operation of the RainbowCrack program is straight forward, but requires some understanding of the cryptographic process behind the program to get the best results. Pre-computation of the rainbow tables is the first step of the process of using the attack tool. The character set to be used is the first step; this can be alpha, alpha-numeric, alpha-number-symbol, or all characters. This also determines the key space you will be searching. Increasing the characters in the character set exponentially increases the key space. The next three items in the configuration are the chain size (t), number of chains in a table (m), and the number of tables (l). The author has provided the optimized settings for standard numeric and alpha numeric keyspace tables. Customized settings can be configured using the equations provided in [3] that requires advanced calculations. The disk space needed for the tables will be the product of the number of chains, number of tables, and the chain size.

Once these configuration options have been determined, the generation of the chains can begin. Syntax for the command is as follows:

Rgen.exe <Table Index> <Rainbow Chain Length> <Rainbow Chain Count> <Comments>

For each rainbow table created, the command must be executed again with the table index incremented by one. The pre-computation of the rainbow chains can take several hours or weeks depending on the speed of the machine generating the chains, chain length, number of chains, number of tables, and the size of the keyspace. Using the developers recommended settings for alphanumeric password cracking generating the required 5 rainbow tables took 40 hours each to generate on Pentium 4 2.0 GHz machines. The trade off of time in the time-memory trade off is the time to pre-compute the tables. A benefit for the attacker is they can generate these tables at their own leisure on their own equipment.

Once the tables are generated they can be used on different attacks of different systems. Each table is approximately 640 MB which makes it ideal to store each table on CDR for transport. Larger tables can be generated to provide higher accuracy rates. These tables can be over 1 GB in size; this would require a portable hard drive or DVD-R media to store the tables. With the availability of large storage devices and the low cost of these devices, an attacker could maintain large rainbow tables for different keyspaces and use them as needed.

Once the tables have been generated, the attacker will have several files in the directory they executed the rgen.exe command. These files will be labeled:

lm_<index number>_<chainlength>x<number of chains>_<comments>.rt

The attacker will then need to run the rsort utility against each of the rainbow tables which will increase the attacking speed by organizing the chains. Once this is complete the attacker is ready to attack the actual LM hashes. This would also be the point where the attacker would want to back up the rainbow table files so they could use them in future attacks.

Cracking the passwords requires the user to have the raw LM hashes or a pwdump file with the password hashes in it. As mentioned earlier, this requires the attacker to dump the hashes from the SAM or sniff them from the network. These hashes need to be stored in a text file in the RainbowCrack directory. The syntax for running rcrack is:

Rcrack <location of table files>*.rt <-h for raw has or –f for pwdump file> <text file with hashes>

The program will then run and look for the hashes the rainbow tables one table at a time. As the program finds the passwords they will be displayed on the screen. When all the tables have been searched a list of the programs operating statistics, usernames, and passwords will be displayed. The attack can dump this output to a text file for future reference by directing the output to a text file in the command shell. This command is show below:

```
E:\rainbow\rainbowcrack-1.1-win>rcrack e:\tables\*.rt -f pass.txt >> dump.txt
```

Signatures of Attack

Several signatures of this attack could be left behind depending on the mechanism used to acquire the LM hashes. The only signs that the RainbowCrack tool would leave behind would be the large table files that have to be generated. These tables will be in excess of 640 MB and there should be multiple tables of this size. Under almost all circumstances the attacker would run the actual cracking program from a machine not on the network. This would be due to the large file sizes and the difficulty in moving the rainbow table files. The attacker would want to run the RainbowCrack tool from a machine with a very large amount of RAM so the tables could be loaded directly into memory and not hindered by hard disk input/output times. The type and speed of the processor of the system has little impact on the decryption time of the hash.

Other signatures would be the same as those for traditional password compromises. These could be event log entries indicating the user was logged into the system at times that were not consistent with the person's job functions. Other signs could be the user's files and file shares have audit logs that indicate abnormal access times. Other signs could be audit logs of the user logging on from machines that are not normally used by the user. Many other subtle signatures of a system wide password compromise could be unauthorized configuration changes, unauthorized file changes, backdoor software appearing, or information leaks outside the organization. This would be a worst case scenario, as the organizations primary authentication system would be compromised and the attacker would have almost unlimited access to the network.

Theoretical Network Targeted

A fictional scenario has been created that reflects a real network and real security vulnerabilities of that network. We will look at how a professional attacker could use a combination of physical and electronic attacks to acquire specific confidential information. Once we have seen how the attack is carried out, we will look at how the incident handling process would respond to this attack.

The city of Zion is a mid-sized city with 500,000 citizens in the metro area, and provides standard city services such as Water, Taxing, Policing, and other functions that keep the city operational. City Hall is the primary location for all of the city's administrative activity and houses the Zion Cities Police Departments investigative, administrative, and operations divisions. This facility also houses

the IT department including the data center, help desk, and IT administration for the city.

During the past month Zion City Police Department arrested Bob Soprano the kingpin of a decent sized organized crime family in the city. Detectives have linked him to various crimes through eyewitnesses and several people in the crime organization that turned states witnesses. Detective Vic Mackey is the lead detective for the case. The crime organization would like to know who the individuals testifying are so they could "convince" them not to testify. To accomplish this, they hire John Doe who is a hacker with script kiddie skills who can use tools that others have created, but lacks the ability to create his own tools. John however is experienced at social engineering and has worked as a con-artist, before moving up to corporate espionage. They agree to pay him a large sum of money in exchange for getting the names and other information about the witnesses.

The Zion city network is a 1,500 node switched network that is separated into 5 VLANS that are routed through a central router for inter-VLAN routing. All servers and management stations are on a separate VLAN with no user workstations. There are no Access Control Lists (ACL) configured on the router and any workstation can communicate with any other workstation on the network.

The city maintains a very high level of security for its external network to prevent attacks from outside of the network. Only port 25 SMTP traffic is allowed through the firewall to the Microsoft Exchange 2000 Server that is located on the DMZ of the network. All SMTP traffic is monitored using a SMTP analysis routine that is built into the firewall's operating system. SMTP traffic is then transferred from the DMZ Exchange server to the internal Exchange Server. The perimeter router, firewall, and Exchange server are updated with the latest vendor security patches as they are released. To further enhance security of the network the city has installed intrusion detection sensors on each side of the firewall. Due to staffing limitations the monitoring of the IDS has been outsourced to a 3rd party monitoring company. Figure 1 shows a diagram of the Zion City network.

Windows 2000 with Active Directory operating in native mode is the primary network operating system for the organization. The city has one domain named ZION under one contiguous name space. All servers are patched with the latest service pack and the latest security patches from Microsoft. Logon and failed logon attempts are audited in the event logs on all servers. Users are required to

change the password every 30 days, but there are no complexity requirements and the minimum password length is 6 characters. Accounts are configured to lockout the account for 30 minutes if an incorrect password is entered 5 times. Null sessions have not been disabled and the LM hash storage has not been removed to allow backward compatibility with Windows 95/98 machines.

One of the file servers on the network has been designated a high security file server. This file server stores information that is considered to be of a sensitive nature. The file shares on this system have the Microsoft Encrypted File System enabled for all user accounts on the system. IT has assigned the recovery key to the administrator account on the network. Auditing is enabled on all objects that are accessed on this server and the logs are reviewed on a daily basis. All of the city's detectives, executive management, and the city manager maintain files on this server.

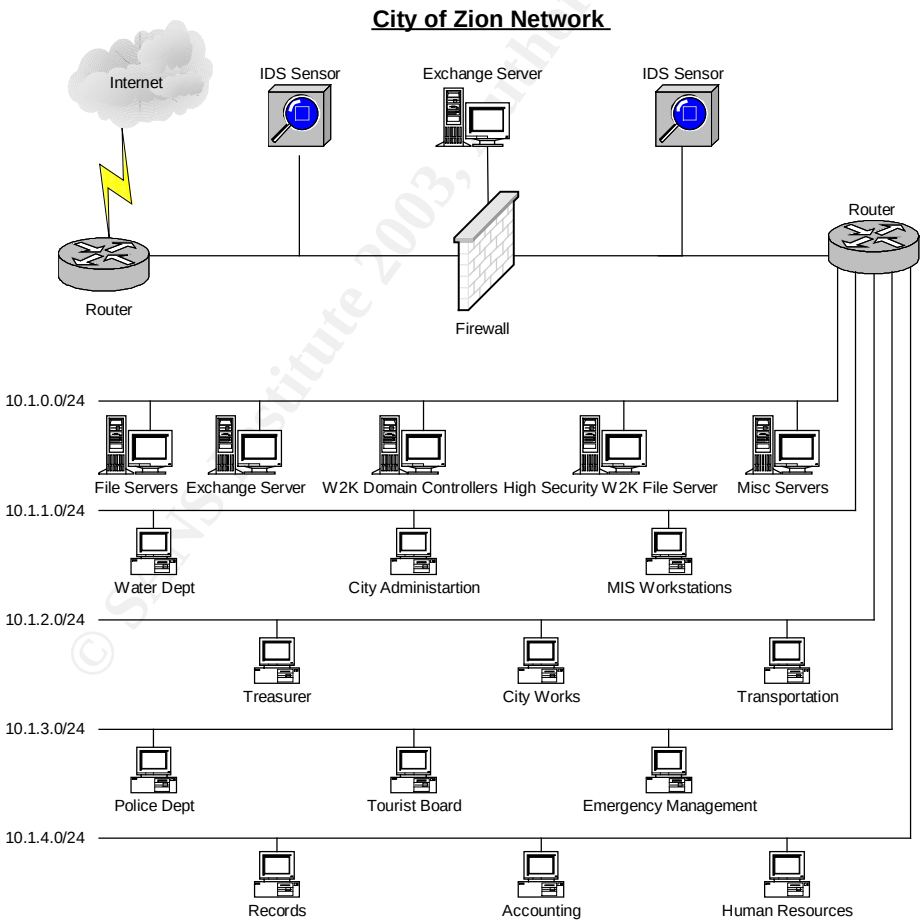


Figure 1

Clients on the network are a mixture of Windows 95/98/2000/XP of various makes and models. Only administrators can add clients to the domain and users do not have local administrator rights on their machines. All software has to be installed by IT after a supervisor has requested it. Users must contact the help desk to install software. All machines run an industry standard virus scanner that is updated from a central management server. There are no MAC filtering or switch port MAC assignments on the network switches.

The IT department for the city consists of three teams: development, networking, and helpdesk. Development consists of a DBA and 3 developers for in-house development of a proprietary Enterprise Resource Planning application. This application is used for city functions ranging from accounting to prisoner tracking. Networking consists of three technicians and a network manager; they are responsible for the network operating system, network infrastructure, and network administration. Network security is the responsibility of the network manager who is a technical manager. The final group is the help desk with five people: two first shift, two second shift, and one third shift. The help desk handles routine user issues over the phone and installs customized software that cannot be deployed by group policy or other deployment methods. Networking and helpdesk work closely with each other due to staff size limitations. The network manager also manages the helpdesk staff.

The Attack

Electronic Reconnaissance

John, the attacker, first browses the cities web site looking for any information that would assist him in determining what operating systems are in use and the general structure of the city organization. Using this resource he determines that most of the cities departments are based out of city hall, with some satellite offices holding auxiliary operating units. His main target, the investigative division of the police department, is housed in the city hall building. He also determines that the IT department for the city is based in the same location. After some searching he finds that the building is occupied 24 hours a day by various city departments, but the busiest time in the building is 8:00 AM until 5:00 PM Monday thru Friday when general public accessed is allowed.

The next phase John begins looking for areas that allow access 2nd shift or with irregular hours. John typically likes to access facilities in this time frame to avoid supervisors and there will be a smaller number of law enforcement personnel on the premises at these times. Looking at various job postings on the web site shows there are opening for 2nd shift clerks in the cities document processing department. After some searching, he finds that there is a reserve police unit of volunteer police officers that meet every Monday and Wednesday night in an

office that is shared with the police operations unit. From this John deduces there must be regular traffic in and out of the building throughout second shift.

While browsing through the web site, John finds an email address for tax payer's questions. John sends an innocuous email asking the address of the Tax department for the city. When he gets the email back he carefully analyses the headers of the message. The routing header indicates that the email was initiated from an Exchange 2000 server. After comparing the email address of the email from Taxes@zion.gov and noticing that all the email addresses listed in the employee directory are @zion.gov, John deducts that they are running in a single Windows domain, most likely a Windows 2000 domain. During his search of the city web site he locates an employee directory. He saves this information for later use.

John decides he will begin to look at the Internet facing systems of the city and see if there is an easy way to gain access to the network remotely. He begins by using nslookup to determine the public IP's that are being used for zion.gov. Figure 2 shows the output of this command. The result is a different network is being used for the web server then is pointed to by DNS. John then does an ARIN search on the two addresses. The result is that the web site seems to be hosted by a well known Internet Service Provider, and the MX record is pointing to an address space that is registered to the City of Zion. To make sure he has all the information available, he does a WHOIS and notes the administrative and technical contacts for the city's domain space. In the process, he notices the DNS hosting the zion.gov name space is a well known web hosting service.

```
zion.gov.                       SOA     ns1 bigisp corp. (6 900 600 86400 3600)
zion.gov.                       NS      ns1
zion.gov.                       MX      10   192.168.2.1
www                             A       192.168.3.1
zion.gov.                       SOA     ns1 bigisp corp. (6 900 600 86400 3600)
```

Figure 2

Using the employee directory he found earlier on the public web site, John begins doing a Google search on the names of the IT staff members. In his results he finds the resume for one of the network technicians posted on a web site. In the resume he lists working for the City of Zion. It further details he was responsible for administration of a Windows 2000 network, with Exchange 2000, and various other details about the network. Further search turns up another network technician offering advice on a USENET group about how to select an outsourced IDS vendor and indicates he has had good experience with outsourcing IDS. An article is found at a Microsoft Certification forum by one of the help desk technicians bragging about his company's firewall only allowing inbound email traffic.

After putting all these details together, John summarizes his information:

- He is most likely looking at a Windows 2000 network.

- The DMZ is most likely secure and running an IDS by a 3rd party provider.
- Minimal services are contained on the DMZ.
- All of his targets are located in the same physical building.
- All email addresses seem to come from the same domain, so there is a good possibility there is one contiguous domain.
- The building is occupied 24 hours a day and public access to the building is 8:00 AM – 5:00 PM Monday thru Friday.
- Several offices are open on second shift.

From the provided information John assumes the organization is very paranoid about what happens at the perimeter of the network. Due to these factors he decides he will use the quietest methods possible to scan the network to determine what hosts and services are available on the DMZ.

Electronic Scanning

John decides to take the stealthiest way possible to scan the city's network from the Internet. He decides to do a SYN scan of the network to determine what hosts and what ports are open on those hosts. The SYN scan will be stealthier since it will not imitate a full 3 way handshake. He configures Nmap[12] to scan the network with SYN packets, at a paranoid rate, and send decoy packets that appear to have come from the host of the city's web site. By configuring the sneaky rate, Nmap will send a packet approximately every 15 seconds. This rate and the decoys should prevent the intrusion detection system from picking up the scan. The command he entered is detailed below:

```
C:\Program Files\NMapWin\bin>nmap -sS -O -D192.168.3.1 -T sneaky 192.168.2.1
```

The result of the Nmap scan (figure 3) shows that only one host is available on the network and that host is only accepting port 25 SMTP traffic. John notices this is the same IP address that the email from the city had came from.

```
Starting nmap V. 3.00 ( www.insecure.org/nmap )
Interesting ports on  (192.168.2.1):
(The 1600 ports scanned but not shown below are in state: closed)
Port       State       Service
25/tcp     open        smtp
Remote operating system guess: Windows Millennium Edition (Me), Win 2000, or Win
XP

Nmap run completed -- 1 IP address (1 host up) scanned in 5 seconds
```

Figure 3

After this scan has been completed, John decides to scan for open Modems using THC-Scan[13] war dialing utility. John sets the utility to scan the phone number blocks listed in the phone book for the city building. The only result John

[12] http://www.insecure.com/
[13] http://www.securityfocus.com/data/tools/auditing/pstn/thc-ts20.zip

gets from this is several fax machines. No modem lines are detected. In his next scanning he decides to war drive the city building using NetStumbler[14] to scan for potential wireless access to the City network. No wireless networks are detected from the wireless scan.

John assembles the information he has gathered from reconnaissance and scanning. Due to the restricted nature of the DMZ network the use of an attack on the DMZ has a low likelihood of success. There is a possibility of sending a user a Trojan or directing them to a site with cross-site scripting to get remote access. John decides against this approach because the general security stance indicates that the city takes perimeter network security seriously, there are probably port restrictions on the firewall for outbound traffic and there is most likely a proxy server of some sort in use. All of these factors would make a electronic attack from the Internet difficult at best. Lack of open modems makes using a dialup connection out of the question and the lack of wireless access points makes that entry impossible. John decides that the best way to get into the network will be to physically gain access to the network from an employee's desktop onsite.

Physical Evaluation

John decides to begin researching the general physical aspects of the city building from open sources such as the web site, city visitor's guide, and phone book maps. John notes in particular he wants to find the location of the police operations division/reserve police unit office that he found on his earlier web search, the clerk's office, the information technology department, and help desk locations when he is on site. He memorizes the names and departments of influential people in all of these departments; in the event he is stopped and questioned he will use this information to aid in social engineering. Several city courts hold sessions in the building, so John decides he will wear a suit and tie to blend in with the culture of the site. He also decides on wearing a suit to exploit the tendency of people to associate dress with authority.

John parks in a nearby parking garage and approaches the building; he notes two entrances, an employee entrance and a public entrance. He enters the public entrance. Guards use metal detectors to check for weapons as well as x-ray machines to evaluate bags and coats. No identification is required to enter the building and there are no sign in sheets. The first place he goes is the information desk where he asks the location of the city tax department. During the conversation, the attacker takes note of the employee's identification card and makes a mental note of what it looks like. After leaving the information desk, John looks at a posted directory and locates where the targeted offices are located. The first target he decides to visit is the IT department to verify the location of the help desk. When he arrives at the floor he takes mental note of the location of the help desk. During the process he realizes that the numbers of

[14] http://www.netstumbler.com/download.php?op=getit&lid=22

restricted areas are minimal, since he was never asked for identification from several employees he encountered.

The next place he visits is the tax clerks office, he notes that there is a public area separated by a glass window from the employee area. He realizes he would have to have a key to access the employee area. John saves the police operational/reserve office for the last place to visit due to the inquisitive nature of law enforcement. When he enters he notices a separate sub-office with a sign labeling it the Zion City Reserve Police office. The rest of the operational offices are a collection of cubes and offices. John approaches the receptionist and asks if it is the Sheriffs property department. The receptionist helpfully explains that is a separate department at the county building and gives its location. John thanks the receptionist and leaves the office.

On the way out of the building, John notices several items that will assist him with his attack. The first item he notices is that all floors have mail chutes that would be big enough to mail a thick envelope. This could be used to get the data out of the facility without detection. A second item he notices is a smoking area on the ground level within the security perimeter. He decides that he can use these areas to assist in coordinating the times of attack. He also notices every PC he has seen from visible screens appears to have the same desktop properties are running Microsoft Windows 2000 or XP. This adds more validity to his previous research in the organization running on a Microsoft Windows network. A final item he notes is the facility has heavy video surveillance on the ground level entry way and external cameras on the building perimeter.

With physical reconnaissance complete, John leaves the building. While returning to his car, he walks through the garage looking for identification cards that have been left in obvious places. He notices that one vehicle has an ID badge sitting in the seat and the doors on the car are unlocked. He quickly steals the identification and puts it in his pocket. John is pleased with his luck; he was planning on following an employee and stealing it from their car or residence. This saved him a tremendous amount of time and effort.

Physical Exploit

With his reconnaissance complete John prepares his strategy for getting Detective Mackey's files. He decides that the best approach would be to use Pwdump3 to get a copy of the SAM database and then use RainbowCrack to break the passwords quickly onsite. Then he will log on as the detective, which should map his user directory automatically. A laptop is configured with RainbowCrack and 5 Rainbow tables configured for alpha-numeric passwords. Several hacking tools are then installed on the laptop including: Pwdump3, PGP[15], Windows DCOM exploits[16], NMap, Nessus[17], NLTest[18] (determines Windows 2000 Domain Controllers), Enum[19], and several other tools.

[15] http://www.pgp.com

A statistics package is setup that runs pwdump3 during installation. This program has the pwdump3 executable renamed and the setup icon hidden. A batch file is labeled Install.bat that runs pwdump3 when executed; it then runs the setup for the statistics program. By using this simple method of creating a Trojan, he can have someone with administrative access run the install.bat file under the guise of installing the statistics program. He includes a configured wireless access point, two 1GB USB Pen Drives, and two envelopes with postage paid addressed to different PO Boxes under his control. John uses a laser printer, a color scanner, and some desktop publishing software to produce a city identification card with his picture on it and a bogus name.

On Monday at 4:30 PM John enters the city building through the primary entrance. His laptop is inspected by the guards, but they pay no attention to the wireless access point in the computer case. He proceeds to the restroom and puts on the fake identification card on. After a few minutes he exits the restroom and proceeds to the public smoking area. While sitting at the bench in the smoking are he eats a brown bagged lunch and smokes. He knows the Zion Police Reserve unit opens at 6:00 PM from information on the web site. At 6:05 PM he makes his way to the police reserve unit office.

When he reaches the office he walks into the Police Operations unit section of the office he begins looking through a few cubes. He is specifically looking for passwords that may have been written down on or near the workstations. If he can't locate a password, he plans on using the network connection to attempt an attack using some exploits he brought with him. After searching several cubes, he locates a non-descript cube. Under the keyboard he finds a password written on a yellow sticky note. He boots the PC at the desk, when the machine boots up into Windows 2000 the username that last logged in is displayed in the username box. John tries the password he found on the sticky note and the machine logs on. One of the Reserve unit officers walks past John and glances at him. John initiates some small talk with the officer and mentions he is working overtime on a statistical analysis for community policing. He uses the excuse he has to get back to work because he is on overtime to end the conversation. Satisfied the Reserve officer goes about his business.

John uses the Pen Drive to copy the NLtest command to the workstation and executes the program. The output is displayed in Figure 4. Ping is used to resolve the machine name ZIONDC1 to IP. The IP address of the domain controller is inserted in the trojaned statistics program so Pwdump3 will execute and pull the SAM database from the domain controller. It will then dump the

[16] http://www.packetstormsecurity.org
[17] http://www.nessus.org
[18] http://download.microsoft.com/download/winntsrv40/rktools/1.0/NT4/EN-US/sp4rk_i386.Exe
[19] http://razor.bindview.com/tools/files/enum.tar.gz

resulting text file onto the hard drive. To execute this program, the Pwdump3 utility will need to run under the context of a domain administrator.

```
E:\>nltest /dclist:zion
List of DCs in Domain zion
    \\ZIONDC1 (PDC)
The command completed successfully
```

Figure 4

Even though he has several exploits available that could get him Domain Administrator access, he decides to attempt social engineering. Using that method makes him more susceptible to detection, but he is confident his story will hold due to the lack of identification checks he has seen in both his reconnaissance and attack. John calls the help desk and tells the technician he needs a statistics program installed right away for a report due tomorrow. The technician indicates that first shift usually installs software, and John tells the help desk staff member its only one floor away from the help desk and the report he is working on is very important to the police chief. The technician concedes and comes downstairs and logs onto the machine. John makes small talk and praises the tech. The technician noticed the user had and employee ID and assumed he belonged. Once the installation has completed the tech logs off. John assures the technician he will tell the IT manager what a great technician he is.

When the tech leaves, John copies the pwdump3 file to a pen drive and then copies it to his laptop. Once on the laptop, he edits a copy of the text file for specific accounts he is looking for. He includes Vic Mackey, Administrator, and several IT staff members he found in the employee directory on the web site. By reducing the number of accounts, the time required to crack a useful account will be reduced. The ideal account to break would be the vmackey account. In the event he can't get the vmackey account password, he will get a domain administrator or an account operator password so he can change the vmackey accounts password.

In the days before the attack, John produced 5 Rainbow tables set for alphanumeric passwords. Each of the tables was generated using the recommended parameters for alphanumeric password. These settings are 5 tables with a chain length of 2,400 and a table size of 40,000,000 chains. Using 5 machines, John generates the tables in 40 hours and copies the tables to the laptop. The resulting 5 files are 640 MB in size each. The command used to begin this process is:

Rtgen <Character_Set> <Table_Number> <Chain_Length> <Table_Size> <comments>

Once this command is completed there is a large file with the extension .rt in the directory. This is the unsorted rainbow table and needs to be sorted to enhance

the efficiency of the cracking attempt. The rtsort command is executed against the unsorted rainbow table. To initiate this process the following command is entered:

Rtsort <RainbowTable_File_Name>

Once this command is complete, the Rainbow table can be backed up and stored for future use. John went through this process and copied the tables to the laptop.

The command used to initiate the cracking process is the following:

Rtcrack <Location_of_Tables>*.rt –f <Password_File> (-f indicates the text file is a pwdump file)

John uses the following command to initiate the password cracking process:

```
E:\rainbow\rainbowcrack-1.1-win>rcrack e:\tables\*.rt -f zionpass.txt
```

The results of the crack are displayed in figure 5. The crack for all the target passwords is found in 58.58 seconds with a 100% success rate. Now that he has the passwords he needs, John now begins the process of getting the information he needs.

```
statistics
---------------------------------------
plaintext found:          19 of 19 (100.00%)
total disk access time:   42.10 s
total cryptanalysis time: 58.58 s
total chain walk step:    40075601
total false alarm:        20131
total false alarm step:   20333130

username      password
---------------------------------------
Administrator Z10NL1V3S
AGriffin      MAYBERRY
HCallahan     44MAGPOWER
JSheridan     WHITESTAR
llacroix      NIGHTCRAWLER
llacroixadmin DIVIA23
MGarabaldi    L00NEYTOON
NKnight       4EVERKN1GHT
NKnightAdmin  4EVERKN1GHT
TWinters      PS1CORP
TWintersAdmin TH3CORP
VMackey       1SHIELD1
```

Figure 5

John logs onto the computer at the cube with the username vmackey and the password 1SHIELD1. This results in an incorrect password attempt access denied error message. Jon realizes LM stores the passwords in uppercase, but he is authenticating with Kerberos since he is on a Windows 2000 machine, so

the passwords can be upper or lowercase. The next password 1Shield1 allows him to logon. When the machine logs on, the detectives home drive is automatically mapped.

John looks through the files and notices several folders relating to the case against Bob Soprano. To be safe, he checks the size of all the files in vmackey's folder and found it to be only 200 MB. John copies all the detectives' files on the shared drive to the local machine. Once these are copied, he compresses all the files, including the pwdump file, using WinZip to a single file. John then copies the file to his thumb drive and to his laptop. He then uses PGP and his public key to encrypt the file using his public key. Once this is complete he copies the encrypted files to each of the Pen Drives. The secret key is at an offsite location in the event the files are seized or discovered.

Keeping Access

Now that he has gathered the information he needs, John wants to make sure he has a way back into the system. To accomplish this, John decides he will install the wireless access point he brought with him. He finds a space between the cubical and the wall where he can plug the wireless access point in to split the connection to the desktop. John carefully hides the access point between the wall and the cubical wall where it is not visible to the casual observer. The access point has been configured with a WEP key to password protect the access point and the SSID has been configured to AP1234 to look innocuous to someone who may be scanning for open access points. He knows WEP can be easily cracked with enough traffic, but this isn't an issue since he plans to use the access point for 48 hours at the most.

He also decides to crack all the user accounts in the pwdump3 file once he leaves the facility. He thinks about creating a user account with access to the system, but since he had all the network passwords for all the accounts pending cracking, he decides it may draw too much attention. The password file contains 1500 user accounts and lab experience has shown that RainbowCrack can crack 1500 passwords with in 1 hour 45 minutes with a 93% success rate independent of the machines processor speed.

Since he has gained the password for the Administrator account and several accounts with Domain Administrator privileges, he decides against installing any backdoor software. He wants to get out of the facility as soon as possible and analyze the data he has already gotten. At this point he could do anything to the network he wished, but time is his primary concern. He is only interested in the data he can sell.

Covering Tracks

Since he has administrative access to the network he knows he can erase any event logs that may have been generated from his one failed logon attempt, successful logon, and access of the files objects in the home directory. He decides it would be too obvious to clear the event logs. There is an option of using Winzapper[20] to remove the entries in the event log, but that would require a reboot of the server and would be too big of a signature.

John installs Access Data SecureClean[21] utility using the RunAs utility to run the installation program as the administrator. This utility securely deletes files by over-writing them 7 times. Files that have been erased using this method meet Department of Defense standards for destruction of classified information. John uses this utility to delete the detective's files from the workstation, the compressed file, and the password dump file that was left on the hard drive. After these files are deleted, John removes the SecureClean program.

The Pen drives are placed in addressed envelopes that are addressed to different PO Boxes under John's control. On his way out John plans to drop the envelopes in the public mail chutes. In the event he is caught on-site he can have a confederate get the data. He hides the compressed data file on his laptop in an alternate data stream in the windows directory on the local hard drive. In the worst case if he is caught and the file found in the alternate data stream, the file will be impossible to decrypt without the secret key.

Now that he has acquired the data he has came for, John logs on and off the local workstation using the username and password of the stations owner. This is to not raise any suspicions with the owner seeing a different username in the username sign in box. The desk is rearranged and he wipes any area he touched with a rag to disrupt any finger prints. Once completed, he leaves the facility, carefully dropping the envelopes in the mail chute.

Incident Response

Preparation

The city has not developed a formal incident handling policy, but has implemented some informal policies and procedures for handling incidents. Nick Knight, the network manager has been designated the organizations incident handler as part off his job. Nick has worked with the organization to develop some incident preparation prior to adopting a formal incident handling policy. Due to a lack of budget, Nick is the sole member of the security team, supervises the network team, and help desk team. This has led to a situation where duties have to be juggled and the development of a full incident handling policy has been impossible.

[20] http://www.ntsecurity.nu/toolbox/winzapper/
[21] http://www.accessdata.com/Product05_Overview.htm?ProductNum=05

Due to the organization being a city government, it has been clearly established that any investigation into criminal activity that occurs on the network will be reported to law enforcement. The city has a forensic computer crime unit and a internet crime task force unit in the police department. These resources are available to the IT department whenever they are needed. This unit consists of 5 law enforcement personnel with 3 of those forensic investigators and the other 2 are veteran detectives with training in electronic crime issues.

Nick has worked with Lucian Lacroix, the cities CIO, to develop a communications plan in the event of an incident. All technical co-ordination will be done by Nick and all departmental communication will be done by Lucian. They devised this division to keep the work at a manageable level. Lucian has worked extensively with senior management and the other department heads to open clear channels of communication. The city manager has mandated that any media comments concerning an incident will be devised with Lucian's involvement and released with his approval. City management has provided pre-authorization for the IT department to use whatever overtime and other resources that are needed to restore normal operations.

Nick has developed an initial response team for major incidents that includes the network team, physical security, law enforcement, legal council, public relations, and human resources. They have had several scenarios that have involved employees misusing the organizations information systems that prompted this team to be assembled. Nick maintains a list of all the contact information for everyone on this team and everyone in the IT department. Each member of the networking team is issued a city cell phone to assist in communications.

Due to the sensitivity of some of the information different department's store, a file server has been designated as a high security server. This server is a Windows 2000 server that has been configured with Microsoft's Encrypted File System (EFS) to encrypt all user files on the file server. EFS encrypts the users files without user intervention, the key is associated with the user account, so the files decrypt as the user access them without any user intervention. This server has also been configured to audit all access to the user files on the system. These logs are reviewed for anomalies every 24 hrs. Any abnormal activity is immediately investigated.

Wireless networking is not installed or permitted in the city building due to the associated security issues. Occasional scans are performed using NetStumbler to determine if there any rouge access points. Modems are only allowed via an outbound modem pool attached to the network. Users are prohibited from installing modems on their workstations and there are routine inspections for modems every 6 months. Any user that is found with a modem on their machine or installing a wireless access point faces disciplinary action.

Identification

At 9:00 AM on Wednesday, Talya Winters one of the network technicians, brings Nick a copy of the logs an excerpt of these is in appendix A. It appears the vmackey account logged in at 7:00 PM Tuesday night from a machine named PD-OPT-25, a PC in the operations area. The audit log shows that all the files in his user directory were copied. Logs show that the files were copied from a machine in the police operations division area and not the investigation area. Nick calls Vic at his desk and finds out that Vic was on vacation yesterday; there was no way he accessed his files. Nick notifies Vic that his files may have been compromised. Due to the sensitivity of the files, law enforcement begins the process of determining what the impact of the lost information is and how they will react to it. Nick phones Lucian telling him about the event and that he is in the process of investigating the event.

Nick tells Talya to begin pulling event logs from the domain controllers, secure server, and other file servers. She is instructed to export the event logs to a file and copy them to CDR media. Then she will generate MD5 checksums on the file for evidence and chain of custody purposes. By having the logs on write once media, they will not have to worry about tampering. Nick instructs the network team to begin analyzing the logs further to determine if there are any other anomalous events recorded within a 3 hour time period of when the vmackey account was accessed.

The city network uses a naming convention that includes the department and port switch that the computer is connected to for identification. Nick locates the computer that was used to access the detectives account. He calls the owner of the machine and tells him not to work any further on the machine until he gets there. Due to the sensitive nature of the files that were compromised, Nick decides they need to treat the evidence and investigation as if it were a crime scene. It is better to have a stricter evidence acquisition from the beginning in case it does have to go to court. At 10:00 AM, Nick calls Detective Jennings from the Forensic Computer Crime Unit (FCCU) to do the forensic acquisition of the workstation. They have much more experience in forensics then his staff and will perform a more detailed analysis.

Nick arrives at the suspect machine and begins interviewing the user to determine if anything strange had occurred. The user, Larry Cairns, didn't know anything and didn't notice anything out of the ordinary. Jennings arrives several minutes later with his forensic acquisition kit. The scene is photographed and a general description of the environment is noted. He then unplugs the computer to power it down; this is the standard procedure for the FCCU. Once the machine is powered down, the wiring and peripherals are photographed and documented. Serial numbers are taken for the CPU and they are photographed. Evidence tape is put across the floppy and CD-ROM drives of the machine. During this processes, Nick notices a sticky note with a password on it. Nick questions Larry about the password and he confirms it's his password. Nick scolds him and

lectures about password security. While removing the cables and preparing the CPU for movement, Nick notices the cable is going to an access point. Nick knows this access point does not belong on the network and it was hidden. Larry is clueless about the access point and it's purposed. At this point, Larry is not considered a suspect. Jennings & Nick finish inventorying the seized equipment, noting details, and noting serial numbers of seized peripherals. Once everything is collected, Jennings takes the equipment back for forensic analysis. He is given a list of the files the logs indicated were moved, and the time frame when the attacked happened.

At 12:00 PM, Talya calls Nick and tells him she has found a disturbing series of events in the event logs. First, at 6:30 PM LCairn had a successful logon attempt from machine PD-OPT-25. After that event, at 6:45 PM, Richard Doyles administrative account (RDoyleAdmin), a 2nd shift help desk staff member, logged in. Then there was an unsuccessful logon by vmackey with an incorrect password. Then there is a successful logon by vmackey. After that, all the files in vmackeys folder were accessed. Finally and most importantly, the Administrator account had a successful logon. All the other entries in the event logs have shown normal activity. Nick instructed Talya to document her findings and continue looking for any other discrepancy. Nick contacts Lucian at 12:15 PM and notifies him of what the event logs have shown. He then calls Richard at home and his cell phone, but has to leave a message.

Detective Jennings calls Nick at 12:30 PM and tells him they have completed the initial analysis of the machine. The machine had a secure deletion program installed on the hard drive. The slack space on the hard disk showed that a directory had been overwritten at 7:15 PM the night before. The Documents and Settings directory has folders for LCairn that were created several months earlier, a folder named RDoyalAdmin created yesterday, and a folder called vmackey created yesterday. The last two folders were created the day before right after each other. Jennings notes that if a secure deletion program was used, recovery would be impossible. This is due to most over writing programs overwriting the data 7 times, this would make recovery impossible.

At 12:45 PM Richard returned Nicks call, he explains that he was called around 6:30 PM the night before by an employee named Leonard Lawrence in the police operations section that was working late. He then detailed how he logged on the machine with his admin account and installed the program. When asked what the account the individual was logged in as Richard didn't know and admitted he didn't look who was logged in. Richard described the employee and indicated he had an employee ID. Nick told him he needed to come into the office as soon as possible; they needed to go over more details of what happened. He assured Richard he wasn't in trouble. Nick quickly called human resources and inquired if they had an employee by the name Leonard Lawrence. HR responded that no such employee was ever employed with the city.

Nick calls a meeting with Lucian and the network team at 1:15 PM to develop a situational analysis. They have had sensitive information stolen from a sensitive server, they conclude from the available evidence that it could not have been accidental. They note that the attacker accessed 3 different accounts: LCairns, Vmackey, and Administrator. Only one failed logon attempt was detected from these attempts and the last two account logons were after Richard had logged in. Once the attacker logged on as Vmackey, they accessed his files. A secure deletion program was installed using the Administrator account for the domain. That password is only known by the network team. The attacker also installed a wireless access point, which they assume is for remote access. From this information they deduce the password database was compromised. This includes the Administrator account, which has super user privileges to all network resources.

During the course of the meeting they develop a plan of action to handle the incident. The plan is to reset all administrative passwords, infrastructure passwords, and stand alone equipment passwords. After this is complete, they will need to reset the user's passwords and force them to change passwords. They also decide to do a physical sweep of the building to search for modems and wireless access points. To help with finding access points, they decide they will have a team go through the building and use NetStumbler to search for any potential rouge access points. After these steps have been taken to contain the problem, they will start checking the integrity of servers. They decide Lucian will handle the political side to give Nick more time to focus on the technical recovery. Nick will report the team's process to Lucian every hour. The meeting adjourns at 2:15 PM and the team begins the containment phase.

Containment

Nick realizes that he the will need to have as many IT staff as possible to assist in the recovery process. He briefs the IT staff that they have an incident and the nature of the incident. First shift is told they will need to stay 3 hours after shift and report 1 hour early the next day. Second shift is told they will need to stay 3 hours late and third shift is told the will need to come in 3 hours early. One of the secretaries is tasked with contacting the off duty IT staff.

Physical security and law enforcement are notified of the incident, the times, and that Richard saw the suspect. The video from the surveillance camera is pulled and physical security begins analyzing the tape. At this point, the criminal investigation is being turned over to law enforcement for follow up. Physical security is also notified that IT will require two security officers to escort two different teams to search for wireless access points.

The investigation division contacts the FBI Computer Crime Unit about the incident. Their suggestion is to secure all available evidence and they will send special agents to assist in an investigation. Agents will not be on scene for at

least 24 hours. They suggest that the IT department secure the network to prevent further intrusion and information loss. Since the primary piece of evidence is the workstation used in the attack and the event logs. All of this data has been acquired using standard forensic techniques and evidence handling methods.

Tools that be used for this incident includes Pwdump3 a password dump utility that will be used to extract hashed to audit the password database. LC4 from @Stake will be used for actual password cracking and auditing of the password database. NetStumbler will be used to search for rogue wireless access points in the building. Microsoft Visual Basic will be used to develop the script that will reset the passwords for the accounts. Other tools that are in the incident jump kit that could be used during this incident are Knoppix Linux to boot an NTFS partition for analysis, Encase by Guidance Software for forensic analysis, a portable disk duplicator with MD5 generator, and other management utilities.

Using the Pwdump3 utility, the network team makes a copy of the current SAM to use for comparison to make sure that the passwords have been changed. The copy is burned to CD-R and an MD5 checksum is ran against the file to verify the file integrity. The Active Directory information is then backed up to a portable tape drive using Microsoft Backup. The system state item is selected in the Microsoft backup and the system partition is backed up. The tape is then pulled from the tape backup, labeled for the incident, and put in the data safe. After these have been completed, the team begins the process of resetting the passwords.

Nick instructs the networking team to begin resetting all administrative passwords on the network. The Administrator password is the first account that is reset and that account is used to disable and reset the passwords for all IT staff and IT administrative accounts. The team was also told to look through all the administrative groups (Domain Admin, Schema Admin, Enterprise Admin, etc.) to make sure all the accounts in those groups get disabled. After all the accounts are disabled, the staff is to change their passwords in person. After the administrative and IT staff member accounts have been reset, they are to reset the passwords on all server local administrator accounts and all application service accounts. Once these passwords have been changed, the infrastructure equipment including all routers, switches, firewalls, and other stand alone equipment is to be changed.

One member of the development team is instructed to work with the network team to develop a script that will reset all the user account passwords. It will then pull the employee name and employee ID number which is also the users social security number from the employee database. Once this has executed, the script will reset the user's password to their employee number and mark the account for a password reset. Visual Basic is the primary development environment for the development team and they have developed administrative scripts in the past

using the Microsoft Active Directory Service Interface (ADSI) components to manipulate the Active Directory database. Nick instructs them to develop the script and test in the lab environment. Once it is completed they are to notify Nick and they can plan to implement the script in production. The rest of the development team is instructed to change the administrative passwords for the database and review the database logs to look for abnormal activity.

The help desk staff is divided into two teams of two people, one second shift and one first shift employee. At 8:00 PM the first shift employees will be sent home and the 3rd shift employees will assume their roles. Each of these teams will be assigned a security officer with keys to all areas. The will search every computer and Ethernet jack for wireless network access points and modems. Security will also act as witnesses of the IT employees actions in sensitive areas to prevent controversies. After the search is complete, the help desk team will assist 2nd shift employees with password changes. Voicemail will be configured on the helpdesk phone indicating users should leave a message if they have an emergency. Networking will take any emergency calls that come in; normal problems will be queued and addressed at a later time. Both teams will report their progress on an hourly basis to Nick.

Lucian calls an emergency meeting with the city manager and the executive city staff. He briefs them about the situation, how they believe it occurred, and what the plan is to solve the problem. The handling plan is communicated and any questions are answered. After this meeting is complete, a meeting is called with the department heads of all the city departments. All of the managers are briefed on the situation and given an outline of what is being done to resolve the problem. They are also informed the help desk is only accepting emergency calls and they should not expect the usual levels of service for the next 24-48 hours. Finally, all managers are reminded that only the PR department is allowed to communicate with the news media regarding the issue. During this meeting the executives and department heads passwords are reset to their employee ID number and they are instructed to reset their passwords. This is to prevent false information from being disseminated by an attacker.

At 8:00 PM Nick calls a meeting of the MIS staff to determine the status of the incident handling. Pizza and drinks are furnished for the staff at the meeting. At this point all administrative, service, and infrastructure accounts have been changed. No evidence of further hacker activity has been found and all systems appear to be operating normally. The development team has determined there have been no obvious attacks to the database servers and no strange activity on those systems. They have also completed the script and tested it in a lab environment. It works as planned and can be configured to only affect designated organizational units in Active Directory. This allows the program to be limited to accounts that have not been reset. Lucian is in the meeting and gives approval for proceeding with the en masse password reset. He notes they will leave a voicemail on everyone's phone indicating the password change, signs placed in

department non-public areas, and he will call each department head to tell them the password procedure.

At the end of the meeting, all first shift help desk staff are sent home and told to arrive an hour early. They will be sent home the next day an hour early. All members of the development team are sent home except for the developer who wrote the script. They will be allowed to take comp time for the extra time over their normal hours. The script developer will be given the following day off due to the amount of time to deploy the script. Networking will develop the signage of the password change, photocopy, and assist the help desk team in deploying them. Once that is complete, one of the networking team members will remain to supervise the script deployment. The rest will leave, but will report for work one hour early the next day. Each team member will be given a day of comp time to take the next week.

The script is executed in production at 9:00 PM and runs without any errors. To prevent the users from using the same password they had before the password change, the domain password policy is set to disallow the previous two passwords. Help desk teams are sent the second shift departments to assist users in changing their passwords. Both help desk teams call indicating users are changing there passwords and there seem to be no problems.

Thursday morning, the network team splits up and visits each of the departments to assist where necessary. Shortly after 9:00 AM help desk calls taper off and become more normalized. With the volume down, the networking team begins evaluating servers for abnormal activity and potential signs of intrusion. Continued wireless sweeps are made of the building to look for potential rouge access points. No other access points are found and no other covert devices are located. Nick briefs Lucian about the status of the incident and that they have the situation contained. Lucian meets with the city manager and briefs them of the situation.

Eradication

Insuring all passwords have been changed is the first step to ensuring any of the passwords acquired by the attacker are useless. A copy is made of the current SAM database and LC4 is used to inventory passwords. The passwords are compared to the SAM file that was dumped prior to the password change script. All passwords have been changed to a new password which is ether the users choice or reset to the users employee ID.

A weekly schedule for the next 3 weeks is developed for a detailed search for access points and modems. The network team will search using NetStumbler to determine if any access points are broadcasting. Second and Third shift will be accompanied by physical security to do a desk to desk search for access points. In the future, monthly access point searches are scheduled. Due to the incident,

physical security is instructed by their management to aggressively check identification of persons entering the building and questioning anyone they haven't seen in the facility before. Random floor patrols are scheduled after standard operating hours to increase the chance of detecting an intruder.

Implementing a security awareness program for users is the next element of the eradication process. A consultant is hired to develop a basic user security awareness program to focus on password security and physical security. This will have a component indicating the importance of contacting security when someone is out of place, and not giving people access without proper identification. The program should consist of printed materials and a short seminar that will be mandatory in-service training for staff members. As part of security awareness, all IT staff is instructed that software can only be installed with the user's supervisor's approval and must be performed by the first shift helpdesk or networking staff. Any employee that doesn't follow that procedure will face disciplinary action.

Securing sensitive files on the high security server is the next area the network team addresses. A third party cryptography solution will be used to secure the files on the high security server. The system will use an authentication system other then the Windows username and password. This system will also have an escrow key system to provide the IT department the ability to recover files in the event an employee leaves the organization. These escrow keys will be stored on CDR and secured in the IT data safe. A project plan to research and develop this technology is developed for future implantation. PGP Corporate Edition is implemented for users who store files on the secure server as a temporary solution. Users are trained on how to use the product and key handling procedure. This is temporary until a solution that meets all the organizations needs can be located.

To increase the difficulty of cracking passwords in the future, IT decides to phase out the storage of LM hashes on the network to make cracking passwords more difficult. Microsoft article Q299656 describes the registry changes that the IT staff will make to the domain controllers to prevent LM hashes from being stored on the network[22]. These changes will be performed on all domain controllers to make compromising the password database more difficult. This will disable the ability to authenticate with the domain for Windows 98 and earlier machines. Due to the few numbers of Windows 98 and earlier clients, IT decides they will upgrade these clients to a new version of Windows. A project plan will be designed to upgrade all machines to at least Windows 2000 for all clients and an eventual move to full Kerberos authentication with no legacy support.

Network redesign is another element that needs to be done in order to properly secure the network. The secure server will be moved to a separate subnet that is protected by a firewall. All clients that will need access to the subnet will use a

[22] http://support.microsoft.com/default.aspx?scid=kb;en-us;299656

VPN implementation with workstation and user certificates to terminate the VPN connection. This will allow only authorized machines to access the subnet and mitigates the risk of an attacker using IP spoofing or a man in the middle attack to bypass a standard packet filtering firewall. Another network design element that will be implement is port security on all the switches will be implemented. All ports will be configured to accept only one MAC address on a given port. This will deter access points from being installed on the network. While possible, the chance of detection would be greatly increased. The high security server will be placed in its own separate domain from the rest of the network to further isolate it. This will prevent a compromised administrative password on the main city network from gaining administrative privileges on the secure network. While the management burden is increases, the limited number of users that use the secure network makes it feasible.

Recovery

Due to the nature of the attack, there is a possibility of rootkits being installed on the server. Evidence of this has shown that the attacker seems to have been interested in acquiring a very limited amount of data. The IT department decides they will increase their monitoring efforts to look for suspicious activity. It has been decided the cost of rebuilding all the servers is greater then the risk of a root kit being installed. Event logs on the domain controllers and file servers are reviewed for suspicious activity several times a day. The team is looking for multiple failed logon attempts, access attempts to sensitive files, and configuration changes to the servers.

The tape backups the night before the incident are compared to the backups the night of the backup. No major differences are found between system files or stored user data. This gives further support to indicate the attacker was interested in stealing specific data and not to gaining control of the network or planting data. Frequent access point checks have not turned up additional access points or modems that have been installed. When compared with the video surveillance time stamps of the intruder entering and exiting, it appears he didn't have time to plant additional access points. The continued scans and searches for wireless access points will be a permanent procedure.

To assist in detecting further hack activity, the IT department develops a plan to distribute several Snort[23] sensors on ingress points to the server subnet. Snort is used as the intrusion detection system with an ACID[24] console to provide a log of alerts. Standard alerts are set on the sensor; alerts are reviewed throughout the day. A long term plan of a managed solution for intrusion detection is established to allow greater monitoring. Monitoring this system is time consuming, but it provides the network team a greater view of what activity is present on the network.

[23] http://www.snort.org
[24] http://www.andrew.cmu.edu/~rdanyliw/snort/snortacid.html

After a week of continued monitoring no malicious activity is located and all access seems to be normal. The law enforcement investigation was unable to locate the individual responsible for the attack. Due to the rapid detection of the compromised files, the police department was able to secure witnesses of several cases that were being handled by Detective Mackey. All notes and evidence from the case that were acquired or generated by the IT department were turned over to law enforcement in the event a suspect was located.

Lessons Learned

One week after the incident, Nick has determined that no further attacks or breaches have been attempted. The directed nature of the attack and the specific attack of one particular user has made this the most likely scenario. Nick compiles his notes from the case and prepares an incident report, timeline, and suggestions for improvement. Physical security is cited as the primary cause of the incident and the primary weakness of the system. This report is submitted to Lucian, who submits to the city manager. Due to this incident, Lucian recommends establishing a security awareness program and request a cross departmental team to enhance physical access to sensitive areas of the facilities.

The IT team is brought together to review the incident and go over the technical details that would increase their efficiency in the future. Items that are raised during the meeting are better communication between team members, pre-generated scripts, and greater intrusion detection systems. One of the points in the meeting that came up was how working with physical security assisted in the incident. In the future they realize they need to perform some security awareness with the physical security to help them identify physical attacks on information systems. All notes and summaries of the incident are archived in a folder and stored with the network documentation in the event a similar event happens in the future.

Summary

We have shown that an attacker can use the RainbowCrack program to rapidly attack the LM hashes that store password information in a Microsoft networked environment. Rapid decryption of passwords gives the user a rapid way of compromising a network and locating specific information on that network. The speed increase provided by this program makes it a practical tool for an attacker that can gain physical access to the network. With a physical attack, the attacker wants to gain access to their target information and leave the scene as fast as they possibly can. Attackers can gain physical access to the facility in this case by social engineering. Other methods could be used in different scenarios to gain physical access such as breaking and entering or by bribing an internal employee. Regardless of what method is used to gain physical access, the tools

that provide a means to gain faster access to information systems show the importance of maintaining physical security.

Physical security is the basis for all other layers of electronic security, but is often the most neglected area. To compound this, most organizations do not have a good integration between their IT security and their physical security staff. Quality of physical security staff becomes another area of concern for organizations. On average, physical security guards are poorly paid, but have universal access to all the organization's facilities. This should be a concern for any organization, as a bribed or extorted security officer could compromise all of an organizations network infrastructure.

Other areas of concern are security awareness training for end users to reinforce the importance of physical and electronic security. Users should be encouraged to question people they don't feel belong in an area, and report those people to physical security. Individuals without employee identification should be questioned and prevented from entering sensitive areas. Many organizations develop complex network security measures, but ignore the physical security and human factor element.

Security professionals should develop physical security skills that are often ignored or overshadowed by electronic security skills. Even the best firewall and electronic security policies will not stop an attacker that can physically gain access to network infrastructure. Network design should include provisions to isolate critical infrastructure in secure area that limit physical access to the bests means possible, that fits the organizations need. Overall, security professionals should realize that for a price or cause, someone will attempt to gain physical access to steal information and the contingency should be planned for that some will attempt a physical intrusion.

References

[1] Project RainbowCrack – Zhu Shuanglei – Kingnet Security Inc. – October 12, 2003 – http://www.antsight.com/zsl/rainbowcrack/

[2] Advanced Instant NT Password Cracker – Luca Wullschleger and Cluade Hochreutiner – Swiss Institute of Technology – August 2003 - http://lasecpc13.epfl.ch/ntcrack/

[3] Making A Faster Cryptanalytic Time-Memory Trade-Off – Philippe Oechslin - Laboratoire de Cryptographie, EPFL - http://lasecwww.epfl.ch/pub/lasec/doc/Oech03.pdf

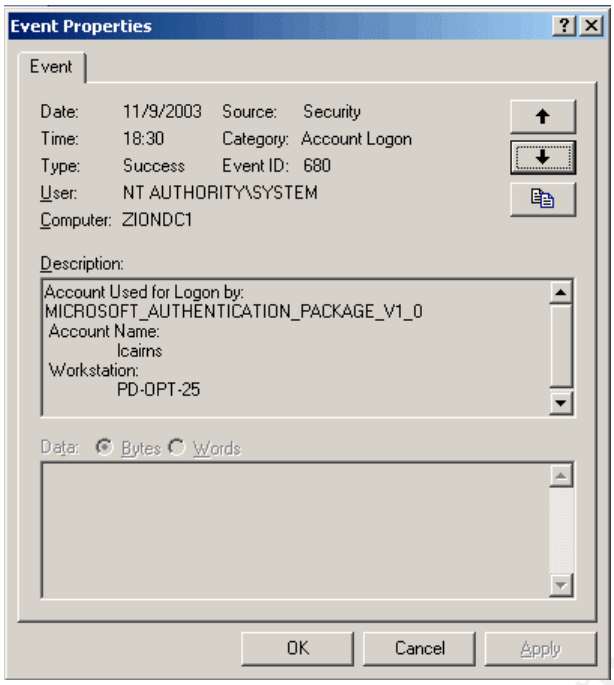
[4] NT Cryptography – Alan Ramsbottem – NTBugtraq – July 17, 1997 - http://www.ntbugtraq.com/default.asp?sid=1&pid=47&aid=17

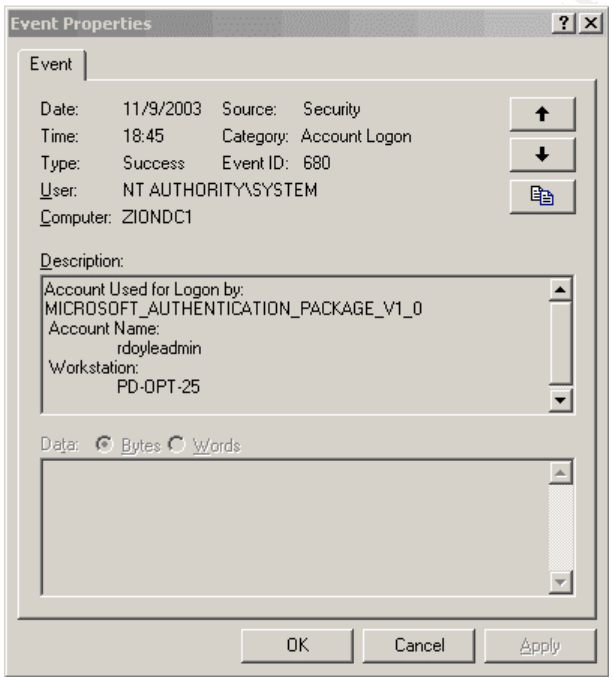
[5] Skoudis, Ed. Counter Hack: A Step-by-Step Guide to Computer Attacks and Effective Defenses. Prentice Hall 2002. 289.

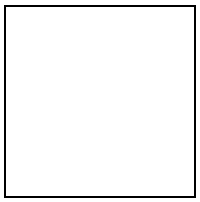
[6] A Cryptanalytic time-memory trade off – IEEE Transactions on Information Theory, IT-26:401-406, 1980.

[7] Cryptography and Data Security, Page 100. Addison-Wesley, 1982.

Appendix A







Last Updated: May 23rd, 2017

Upcoming Training

SANS Madrid 2017	Madrid, Spain	May 29, 2017 - Jun 03, 2017	Live Event
SANS Atlanta 2017	Atlanta, GA	May 30, 2017 - Jun 04, 2017	Live Event
Community SANS Virginia Beach SEC504*	Virginia Beach, VA	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Thailand 2017	Bangkok, Thailand	Jun 12, 2017 - Jun 30, 2017	Live Event
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC504: Hacker Tools, Techniques, Exploits and Incident Handling	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Mentor Session - SEC504	Reston, VA	Jun 13, 2017 - Aug 01, 2017	Mentor
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
Community SANS Seattle SEC504	Seattle, WA	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS ICS & Energy-Houston 2017	Houston, TX	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Sacramento SEC504	Sacramento, CA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Ottawa SEC504	Ottawa, ON	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
Community SANS Des Moines SEC504	Des Moines, IA	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Annapolis SEC504	Annapolis, MD	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Phoenix SEC504	Phoenix, AZ	Jul 24, 2017 - Jul 29, 2017	Community SANS
Security Awareness Summit & Training 2017	Nashville, TN	Jul 31, 2017 - Aug 09, 2017	Live Event
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
Community SANS Raleigh SEC504	Raleigh, NC	Aug 07, 2017 - Aug 12, 2017	Community SANS
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event