Incident Response For DMS

Barnes, Lawson, Michel

The incident response to computer crime for the Department of Math and Science is likely to be very similar to the methods used by any generic law enforcement. As the DMS is centralized in the Chapman Building, a relatively small, and more importantly public building, a fully equipped and authorized investigation team ready to go at the drop of a hat isn't very necessary, as criminals will likely carry out their schemes elsewhere. A minor offense can easily be dealt with by campus officials, but should a serious computer offense occur on campus, outside authorities are likely to be called in to assist the campus officials. The following are some basic procedures and criteria that officials would follow in the event of a serious computer crime here at the Department of Math and Science.

Law enforcement response to any instance of computer crime requires that all parties actively participate in the investigation. Each party involved must understand the delicate nature of electronic evidence and the principals and procedures of collecting and saving such data. As any investigator knows, altering, damaging, or even destroying evidence can make or break a case, and as such, all investigators involved need to take particular care to avoid doing so. Any kind of digital evidence is easily tampered with and can be done so completely accidentally by investigators unskilled or untrained well enough in computer forensics. The courts will heavily scrutinize any actions in the investigation that could possibly call into question the validity of the evidence collected.

To avoid this, the parties involved must have extensive knowledge in computers, and should have some high degree of technical training involved with collecting evidence off of a computer. Time is of the essence, and the investigation must be conducted quickly and thoroughly, emphasizing the importance of knowledgeable investigators. Also, cooperation between participants in the investigation is an obvious, yet necessary element of searching a crime scene for evidence, as the simplest misunderstanding or miscommunication can result in error.

Collecting data is the most important part of a forensic investigation, as it is here that the most mistakes can be made and the most damage caused by such mistakes. The crime scene must be secured and all people should be removed from the area in which the evidence is to be collected. Everything should be left the way it is found until thoroughly documented. The scene must be described in detail to such that the investigators can replicate the scene later. Photographs and detailed notes are essential.

Once the scene has been secured and the essential information documented, the actual collection of the evidence can be conducted. How the investigators go about collecting data may depend upon what kind of computer setup the investigation is being conducted on. If the computer is stand-alone personal computer that a student or faculty may have brought in, the steps to seizing it as evidence are rather simple. At a very basic level, there are three distinct steps to follow. The first step is to document the status of the computer, such as whether it is on or off or sleeping and what applications are running. The second step involves removing the power supply and any outside connections. The final step involves recording any distinguishing information about the setup, such as serial numbers, make and model descriptions and manufacturer and date of manufacture. Also, the connections of the computer must be assessed, including the outside connections as well as the internal ones, before the

computer setup is dismantled and packaged for further analysis of the evidence at the lab.

For a computer in a network, such as one of the many computers in the Chapman Building, the procedure is a bit more complicated since the computer is connected to so many others. The procedure is the same as for a stand-alone personal computer, but extensive knowledge of the network the computer is connected to is imperative. The network administrators and technicians would likely be called in for assistance, and a thorough investigation of the crime scene would be necessary to determine whether or not any of the other computers have been affected by or used in the crime. Depending on the complexity of the network (i.e. ranging from two or three computers to all the connected computers in Chapman) the investigation may be very complicated and time consuming.

Generally speaking, everything related to computing and communications upon campus is underneath the power and structure of DC&C. Therefore any subordinate plan must seek to facilitate that power and work within its structure. An incident response plan for the Department of Math and Science is thus dependent upon the structure DC&C imposes. A general method of communication between the two must also be present. In the event of an incident within DMS a written report detailing the damages, affected systems, the status of the network and any other relevant information should be copied and sent to DC&C for the purpose of documentation.

Currently, all that is considered DMS is within the building of Chapman. This includes a wireless network, two class C subnets and a plethora of faculty and student computers all with which are provided by DC&C. The two class C's house a faculty and wireless network, the .25 subnet, and a student lab network, the .27 subnet. These are composed of real IP space and static addressing. A router on top of the .25 subnet blocks any ICMP packets and prevents any faculty or wireless connections from being mapped. This router also acts as a firewall and filters access to ports on most .25 machines; the subnet is however shared with ASUAF machines which appear to be not behind a port filter. The .27 subnet is also not underneath a firewall and therefore has ports open according to the services offered on each computer. The laboratory is further protect from intrusion by not allowing users the ability to install programs that require system services. This concludes a general overview of the current state of affairs of these two subnets and the DMS network.

The current situation with the network instituted by DC&C leaves the Department of Math and Science with a couple problems. For starters, the most fundamental problem involves clarifying the responsibility of DMS in regards to the universities network of communication. As stated before there is a hierarchy: Statewide, DC&C, and then the subordinate departments of which DMS is a member. Because DMS is not responsible for its own communication privileges, it should not be responsible for responding to incidents belonging to it. This is to say that, any incident which is the result of actions by faculty members should not be handled by that same faculty. If this happens, it is the responsibility of DC&C to address and handle the incident. They, more than likely, will also be the only ones who can detect such an incident.

This, fortunately, does not eliminate all incident response from the department of Math and Science. This is a university and it is a place to learn and have academic freedom. The people who are most responsible for educating students are the individual departments. They do this by offering classless and providing services to

their attending majors and minors; and as a department they are responsible for any service it offers. Therefore, an incident response plan for DMS ought to pertain to the labs it offers to its students.

The current state of affairs suggest that the lab in room 103 is underneath the immediate authority of DC&C, rather than underneath the authority of DMS. This is because DC&C is in control of all real IP space upon campus. They are also the only ones in a position to use tools which monitor this space. Being in this position leaves DC&C as the one most capable of noticing any abuse of the DMS lab. Therefore incident response solely within their hands. Another problem with the current situation is that DC&C's system of checking and surveying is not suited for a computer science lab which is fundamentally different than a university's network. This may be contrary to the intentions DMS has for the lab. It is conceivable that some faculty members and students would like to have an environment without the limitations that DC&C imposes.

At this point there are two solutions, each of which have different incident prevention plans. The first solution is to maintain the laboratories in their current state, institute a centralized logging server which also automatically port-scans all DMS laboratory machines for erroneous open ports and further more, institute packet shaping to limit the bandwidth each machine has to the outside network. This way if any machine were to run a service not allowed by DC&C, the detection of that service could be done by DMS. The response to that incident will involve bringing the network back to its pre-incident state, warning or punishing the perpetrator, and informing DC&C of the infringement.

The second solution is to create a private network for academic exploration and another network with real IP space for student services. This separation and structure is preferable because it sections off security holes while maintaining student services. This means that a lab must be administrated separately from the immediate authority embodied in DC&C. It also means that any incident within the private network can be handled solely by DMS per its own policy. The privately addressed lab should have a central logging system and should be composed of static IP's in order to make the logs easier to read. The other network with real IP space is acceptably underneath the authority of DC&C and should also embody the preventative maintenance of solution number one.

No matter what solution the becomes, there are basic services of the network that will not change between the solutions. A user-based network will have shared hard disk space and private folders. It is therefore important to back up the data of both the file server and independent machines periodically. A laboratory which does not have physical access to the machines is infeasible and therefore the machines should be protected against arbitrary operating systems; this is to prevent users from having write access to devices they should not have complete access to.

The current state of affairs is somewhat questionable. The general census of DMS network users is one of act first and ask questions latter; it has the opinion of "we generally do whatever we want and if DC&C has a problem with it they let us know." Which is also coupled with an opinion of "damn that firewall is suxxor." In the face of security DC&C is the man in charge; yet when services are in question it is up to DMS. Having real IP space is either a security risk or a hamper on the ability for students to explore.

The first step of an incident response should happen before any incidents occur. Be prepared, know what equipment you have installed, and what security measures are in

place. Understand your vulnerabilities and how to minimize them. Know who is responsible for responding to computer compromises.

How do you find out what computing and networking equipment is installed in the Department of Math and Science? With whom do you do you talk, to find out? On campus, the Division of Computing & Communications "is responsible for campus-wide computing which includes maintaining network and technical support, training in information technology, web support and maintenance, and facilitating administrative computing at the University of Alaska Fairbanks." DC&C is the computing authority on campus.

There are common misconceptions regarding networking here in Chapman. Many people assume there is a router in the building; while this may have been true in the past, it is not correct now. Chapman is connected through two Cisco Catalyst 3548XL switches and one Cisco Catalyst WS1924R switch. These provide a total of 120 ports, about 100 of which are in use. The switches run through a fiber Gb Ethernet and this, in turn, is connected to a Cisco 6509 switch, then to the routers and from the routers to the internet. Another misconception is that University computers are behind a firewall. Again, this may have been true in the past, but is not correct at the present time. While student ports and student lab ports are fire walled, faculty computers, currently, are not behind a network firewall. This includes the computers in subnet 25 (137.229.**25**.x.)

What should now be clear to network users is, do not assume you know how the network system works. Ensure that you are up to date on how the network currently functions. Systems change over time, and what was true in the past may not be so now. Regardless of which department has responsibility for campus computing, DMS should ensure that its computers do not run unnecessary services and are secure. Programmers should use the correct tool for each programming job, frequently, C or C++ would be an inappropriate choice and can introduce vulnerabilities.

Any incident response plan should be coordinated with DC&C. If a computer is compromised, DC&C should be informed and they will probably perform the initial response. If it is a serious breach, evidence will not be contaminated and, if warranted, any investigation should be able to be successfully conducted. Also, by informing DC&C, they will be able to stay current on system compromises. This helps DC&C in the prevention of future incidents.

The mildly notorious Kevin Mitnick used 'social engineering' in his illegal hacking pursuits. "You try to make an emotional connection with the person on the other side to create a sense of trust," he said. "That is the whole idea: to create a sense of trust and then exploiting it." This deceitful approach worked for gaining information from some people. What Mitnick did was pervert sound principles of computer security. Trust, cooperation and a cross flow of information between The Department of Math and Science and DC&C, is probably the best incident response plan possible.

A University is not built on a strong central authority, it is rather like a union of semi-independent states. Enforcing rules on unwilling students is difficult, enforcing rules on unwilling faculty is harder. While DC&C has ultimate responsibility for campus-wide computing, an atmosphere of trust, respect, and cooperation is more conducive

to maintaining network security than distrust and derision. From what I have observed, a healthy relationship seems to exist between DMS and DC&C, but there is room to improve in the cross flow of information. DMS can be a valuable resource for DC&C, and in fact probably already is. The inverse also holds true, DC&C has much to offer DMS.

Partial topology of Chapman

dec1.cs.uaf.edu 137.229.25.16
ibm1.cs.uaf.edu 137.229.25.17
sun1.cs.uaf.edu 137.229.25.18
ibm4.cs.uaf.edu 137.229.25.23
ncd1.cs.uaf.edu 137.229.25.31
ncd2.cs.uaf.edu 137.229.25.32
ncd3.cs.uaf.edu 137.229.25.33
ncd5.cs.uaf.edu 137.229.25.35
ncd7.cs.uaf.edu 137.229.25.37
ncd8.cs.uaf.edu 137.229.25.38
ncd9.cs.uaf.edu 137.229.25.39
sgi3.cs.uaf.edu 137.229.25.104
linux0.cs.uaf.edu 137.229.25.160
linux1.cs.uaf.edu 137.229.25.161
linux2.cs.uaf.edu 137.229.25.162
linux3.cs.uaf.edu 137.229.25.163
linux4.cs.uaf.edu 137.229.25.164
linux5.cs.uaf.edu 137.229.25.165
deuel.as.uaf.edu 137.229.25.166
linux7.cs.uaf.edu 137.229.25.167
linux8.cs.uaf.edu 137.229.25.168
nt01.chapman-lab.uaf.edu 137.229.27.195
nt02.chapman-lab.uaf.edu 137.229.27.196
nt03.chapman-lab.uaf.edu 137.229.27.197
nt04.chapman-lab.uaf.edu 137.229.27.198
nt05.chapman-lab.uaf.edu 137.229.27.199
nt06.chapman-lab.uaf.edu 137.229.27.200
nt07.chapman-lab.uaf.edu 137.229.27.201
nt08.chapman-lab.uaf.edu 137.229.27.202
nt09.chapman-lab.uaf.edu 137.229.27.203
nt10.chapman-lab.uaf.edu 137.229.27.204
nt11.chapman-lab.uaf.edu 137.229.27.205
nt12.chapman-lab.uaf.edu 137.229.27.206
nt13.chapman-lab.uaf.edu 137.229.27.207
nt14.chapman-lab.uaf.edu 137.229.27.208
nt15.chapman-lab.uaf.edu 137.229.27.209
nt16.chapman-lab.uaf.edu 137.229.27.210
nt17.chapman-lab.uaf.edu 137.229.27.211
nt18.chapman-lab.uaf.edu 137.229.27.212
nt19.chapman-lab.uaf.edu 137.229.27.213
nt20.chapman-lab.uaf.edu 137.229.27.214
nt21.chapman-lab.uaf.edu 137.229.27.215

These scans were done using nmap from my home

dec1.cs.uaf.edu (137.229.25.16):
Port State Service
21/tcp open ftp
25/tcp open smtp

ibm1.cs.uaf.edu (137.229.25.17):
Port State Service
21/tcp open ftp
25/tcp open smtp

Interesting ports on ibm4.cs.uaf.edu (137.229.25.23): (IBM HTTP SERVER)
Port State Service
21/tcp open ftp
80/tcp open http

ncd1.cs.uaf.edu (137.229.25.31):
Port State Service
21/tcp open ftp

Interesting ports on ncd2.cs.uaf.edu (137.229.25.32): (IBM HTTP SERVER)
Port State Service
21/tcp open ftp
80/tcp open http

Interesting ports on ncd3.cs.uaf.edu (137.229.25.33): (IBM HTTP SERVER)
Port State Service
21/tcp open ftp
80/tcp open http

Interesting ports on ncd5.cs.uaf.edu (137.229.25.35): (IBM HTTP SERVER)
Port State Service
21/tcp open ftp
80/tcp open http

ncd7.cs.uaf.edu (137.229.25.37): (IBM HTTP SERVER)
Port State Service
21/tcp open ftp
80/tcp open http

ncd8.cs.uaf.edu (137.229.25.38):
Port State Service
21/tcp open ftp

ncd9.cs.uaf.edu (137.229.25.39):
Port State Service
21/tcp open ftp

sgi3.cs.uaf.edu (137.229.25.104):

Port State Service
21/tcp open ftp
25/tcp open smtp

linux7.cs.uaf.edu (137.229.25.167):
Port State Service
21/tcp open ftp
25/tcp open smtp

linux8.cs.uaf.edu (137.229.25.168):
Port State Service
21/tcp open ftp
25/tcp open smtp

These scans were done using nmap from linux2.cs.uaf.edu (137.229.25.162.)

dec1.cs.uaf.edu 137.229.25.16
Port State Service
11/tcp open systat
13/tcp open daytime
17/tcp open qotd
21/tcp open ftp
23/tcp open telnet
25/tcp open smtp
79/tcp open finger
111/tcp open sunrpc
512/tcp open exec
513/tcp open login
514/tcp open shell
515/tcp open printer
704/tcp open elcsd
1024/tcp open kdm
1025/tcp open listen
1030/tcp open iad1
1031/tcp open iad2
1032/tcp open iad3
6000/tcp open X11

ibm1.cs.uaf.edu 137.229.25.17
Port State Service
21/tcp open ftp
23/tcp open telnet
25/tcp open smtp
37/tcp open time
79/tcp open finger
111/tcp open sunrpc
199/tcp open smux
512/tcp open exec
513/tcp open login
514/tcp open shell
624/tcp open unknown
629/tcp open unknown
636/tcp open ldapssl
639/tcp open unknown
650/tcp open unknown
745/tcp open unknown
790/tcp open unknown
848/tcp open unknown
853/tcp open unknown
1024/tcp open kdm
2401/tcp open cvspserver

sun1.cs.uaf.edu 137.229.25.18
Port State Service
111/tcp open sunrpc
4045/tcp open lockd
32771/tcp open sometimes-rpc5
32774/tcp open sometimes-rpc11

ibm4.cs.uaf.edu 137.229.25.23
Port State Service
7/tcp open echo
9/tcp open discard
13/tcp open daytime
19/tcp open chargen
21/tcp open ftp
23/tcp open telnet
37/tcp open time
80/tcp open http
111/tcp open sunrpc
199/tcp open smux
512/tcp open exec
513/tcp open login
514/tcp open shell
543/tcp open klogin
544/tcp open kshell
818/tcp open unknown
920/tcp open unknown
921/tcp open unknown
2401/tcp open cvspserver
6000/tcp open X11
6112/tcp open dtspc
9090/tcp open zeus-admin
32771/tcp open sometimes-rpc5
32786/tcp open sometimes-rpc25

ncd1.cs.uaf.edu 137.229.25.31
Port State Service
7/tcp open echo

9/tcp open discard
13/tcp open daytime
19/tcp open chargen
21/tcp open ftp
23/tcp open telnet
37/tcp open time
111/tcp open sunrpc
199/tcp open smux
512/tcp open exec
513/tcp open login
514/tcp open shell
543/tcp open klogin
544/tcp open kshell
806/tcp open unknown
807/tcp open unknown
880/tcp open unknown
2401/tcp open cvspserver
6000/tcp open X11
6112/tcp open dtspc
9090/tcp open zeus-admin
32771/tcp open sometimes-rpc5
32772/tcp open sometimes-rpc7

ncd2.cs.uaf.edu 137.229.25.32
Port State Service
7/tcp open echo
9/tcp open discard
13/tcp open daytime
19/tcp open chargen
21/tcp open ftp
23/tcp open telnet
37/tcp open time
80/tcp open http
111/tcp open sunrpc
199/tcp open smux
512/tcp open exec
513/tcp open login
514/tcp open shell
543/tcp open klogin
544/tcp open kshell
726/tcp open unknown
916/tcp open unknown
917/tcp open unknown
2401/tcp open cvspserver
6000/tcp open X11
6112/tcp open dtspc
9090/tcp open zeus-admin
32771/tcp open sometimes-rpc5
32772/tcp open sometimes-rpc7

ncd3.cs.uaf.edu 137.229.25.33
Port State Service
7/tcp open echo
9/tcp open discard
13/tcp open daytime
19/tcp open chargen
21/tcp open ftp
23/tcp open telnet
37/tcp open time
80/tcp open http
111/tcp open sunrpc
199/tcp open smux
512/tcp open exec
513/tcp open login
514/tcp open shell
543/tcp open klogin
544/tcp open kshell
901/tcp open samba-swat
902/tcp open unknown
970/tcp open unknown
2401/tcp open cvspserver
6000/tcp open X11
6112/tcp open dtspc
9090/tcp open zeus-admin
32772/tcp open sometimes-rpc7
32775/tcp open sometimes-rpc13

ncd5.cs.uaf.edu 137.229.25.35
Port State Service
7/tcp open echo
9/tcp open discard
13/tcp open daytime
19/tcp open chargen
21/tcp open ftp
23/tcp open telnet
37/tcp open time
80/tcp open http
111/tcp open sunrpc
512/tcp open exec
513/tcp open login
514/tcp open shell
543/tcp open klogin
544/tcp open kshell
714/tcp open unknown
902/tcp open unknown
903/tcp open unknown
2401/tcp open cvspserver
6000/tcp open X11
6112/tcp open dtspc
32775/tcp open sometimes-rpc13

ncd7.cs.uaf.edu 137.229.25.37

Port	State	Service
7/tcp	open	echo
9/tcp	open	discard
13/tcp	open	daytime
19/tcp	open	chargen
21/tcp	open	ftp
23/tcp	open	telnet
37/tcp	open	time
80/tcp	open	http
111/tcp	open	sunrpc
199/tcp	open	smux
512/tcp	open	exec
513/tcp	open	login
514/tcp	open	shell
543/tcp	open	klogin
544/tcp	open	kshell
651/tcp	open	unknown
901/tcp	open	samba-swat
902/tcp	open	unknown
2401/tcp	open	cvspserver
6000/tcp	open	X11
6112/tcp	open	dtspc
9090/tcp	open	zeus-admin
32778/tcp	open	sometimes-rpc19

ncd8.cs.uaf.edu 137.229.25.38

Port	State	Service
21/tcp	open	ftp
23/tcp	open	telnet
111/tcp	open	sunrpc
512/tcp	open	exec
513/tcp	open	login
514/tcp	open	shell
543/tcp	open	klogin
544/tcp	open	kshell
6000/tcp	open	X11

ncd9.cs.uaf.edu 137.229.25.39

Port	State	Service
7/tcp	open	echo
9/tcp	open	discard
13/tcp	open	daytime
19/tcp	open	chargen
21/tcp	open	ftp
23/tcp	open	telnet
37/tcp	open	time
111/tcp	open	sunrpc
199/tcp	open	smux
512/tcp	open	exec
513/tcp	open	login
514/tcp	open	shell
543/tcp	open	klogin
544/tcp	open	kshell
880/tcp	open	unknown
974/tcp	open	unknown
975/tcp	open	unknown
2401/tcp	open	cvspserver
6000/tcp	open	X11
6112/tcp	open	dtspc
9090/tcp	open	zeus-admin
32771/tcp	open	sometimes-rpc5
32772/tcp	open	sometimes-rpc7

sgi3.cs.uaf.edu 137.229.25.104

Port	State	Service
1/tcp	open	tcpmux
7/tcp	open	echo
9/tcp	open	discard
13/tcp	open	daytime
19/tcp	open	chargen
21/tcp	open	ftp
23/tcp	open	telnet
25/tcp	open	smtp
37/tcp	open	time
79/tcp	open	finger
111/tcp	open	sunrpc
512/tcp	open	exec
513/tcp	open	login
514/tcp	open	shell
515/tcp	open	printer
638/tcp	open	unknown
795/tcp	open	unknown
1024/tcp	open	kdm
1031/tcp	open	iad2
5232/tcp	open	sgi-dgl
6000/tcp	open	X11

linux1.cs.uaf.edu 137.229.25.161

Port	State	Service
22/tcp	open	ssh
111/tcp	open	sunrpc
631/tcp	open	cups
707/tcp	open	unknown
6000/tcp	open	X11

linux2.cs.uaf.edu 137.229.25.162

Port	State	Service
22/tcp	open	ssh

111/tcp open sunrpc
981/tcp open unknown
5680/tcp open canna
6000/tcp open X11
22273/tcp open wnn6
22289/tcp open wnn6_Cn
22305/tcp open wnn6_Kr
22321/tcp open wnn6_Tw

linux3.cs.uaf.edu 137.229.25.163
Port State Service
111/tcp open sunrpc
672/tcp open unknown
6000/tcp open X11

linux4.cs.uaf.edu 137.229.25.164
22/tcp open ssh
111/tcp open sunrpc
667/tcp open unknown
6000/tcp open X11

linux5.cs.uaf.edu 137.229.25.165
Port State Service
22/tcp open ssh
6000/tcp open X11

linux7.cs.uaf.edu 137.229.25.167
Port State Service
7/tcp open echo
9/tcp open discard
13/tcp open daytime
19/tcp open chargen
21/tcp open ftp
23/tcp open telnet
25/tcp open smtp
37/tcp open time
111/tcp open sunrpc
113/tcp open auth
135/tcp open loc-srv
512/tcp open exec
513/tcp open login
514/tcp open shell
515/tcp open printer
4045/tcp open lockd

linux8.cs.uaf.edu 137.229.25.168
Port State Service
7/tcp open echo
9/tcp open discard
13/tcp open daytime
19/tcp open chargen
21/tcp open ftp
23/tcp open telnet
25/tcp open smtp
37/tcp open time
111/tcp open sunrpc
113/tcp open auth
135/tcp open loc-srv
512/tcp open exec
513/tcp open login
514/tcp open shell
515/tcp open printer
1508/tcp open diagmond
4045/tcp open lockd

nt01.chapman-lab.uaf.edu 137.229.27.195
Port State Service
42/tcp open nameserver
80/tcp open http (chapman nt lab)
135/tcp open loc-srv
139/tcp open netbios-ssn
443/tcp open https

nt02.chapman-lab.uaf.edu 137.229.27.196
Port State Service
21/tcp open ftp
25/tcp open smtp
80/tcp open http
135/tcp open loc-srv
139/tcp open netbios-ssn
443/tcp open https
445/tcp open microsoft-ds
1031/tcp open iad2

nt03.chapman-lab.uaf.edu 137.229.27.197
Port State Service
135/tcp open loc-srv
139/tcp open netbios-ssn
445/tcp open microsoft-ds
1026/tcp open nterm

nt04.chapman-lab.uaf.edu 137.229.27.198
Port State Service
135/tcp open loc-srv
139/tcp open netbios-ssn
445/tcp open microsoft-ds
1025/tcp open listen

nt05.chapman-lab.uaf.edu 137.229.27.199
Port State Service

135/tcp open loc-srv
139/tcp open netbios-ssn
445/tcp open microsoft-ds
1026/tcp open nterm

nt06.chapman-lab.uaf.edu 137.229.27.200
Port State Service
135/tcp open loc-srv
139/tcp open netbios-ssn
445/tcp open microsoft-ds
1032/tcp open iad3
1521/tcp open ncube-lm
2030/tcp open device2
8080/tcp open http-proxy

nt07.chapman-lab.uaf.edu 137.229.27.201
Port State Service
135/tcp open loc-srv
139/tcp open netbios-ssn
445/tcp open microsoft-ds
1026/tcp open nterm

nt08.chapman-lab.uaf.edu 137.229.27.202
Port State Service
135/tcp open loc-srv
139/tcp open netbios-ssn
445/tcp open microsoft-ds
1026/tcp open nterm

nt09.chapman-lab.uaf.edu 137.229.27.203
Port State Service
135/tcp open loc-srv
139/tcp open netbios-ssn
445/tcp open microsoft-ds
1026/tcp open nterm

nt10.chapman-lab.uaf.edu 137.229.27.204
Port State Service
135/tcp open loc-srv
139/tcp open netbios-ssn
445/tcp open microsoft-ds
1026/tcp open nterm

nt11.chapman-lab.uaf.edu 137.229.27.205
Port State Service
135/tcp open loc-srv
139/tcp open netbios-ssn
445/tcp open microsoft-ds
4144/tcp open wincim

nt12.chapman-lab.uaf.edu 137.229.27.206
Port State Service
135/tcp open loc-srv
139/tcp open netbios-ssn
445/tcp open microsoft-ds

nt13.chapman-lab.uaf.edu 137.229.27.207
Port State Service
135/tcp open loc-srv
139/tcp open netbios-ssn
445/tcp open microsoft-ds

nt14.chapman-lab.uaf.edu 137.229.27.208
Port State Service
135/tcp open loc-srv
139/tcp open netbios-ssn
445/tcp open microsoft-ds
1026/tcp open nterm

nt15.chapman-lab.uaf.edu 137.229.27.209
Port State Service
135/tcp open loc-srv
139/tcp open netbios-ssn
445/tcp open microsoft-ds
1025/tcp open listen

nt16.chapman-lab.uaf.edu 137.229.27.210
Port State Service
135/tcp open loc-srv
139/tcp open netbios-ssn
445/tcp open microsoft-ds
1025/tcp open listen

nt17.chapman-lab.uaf.edu 137.229.27.211
Port State Service
135/tcp open loc-srv
139/tcp open netbios-ssn
445/tcp open microsoft-ds
1026/tcp open nterm

nt18.chapman-lab.uaf.edu 137.229.27.212
Port State Service
135/tcp open loc-srv
139/tcp open netbios-ssn
445/tcp open microsoft-ds
1026/tcp open nterm

nt19.chapman-lab.uaf.edu 137.229.27.213
Port State Service
135/tcp open loc-srv

139/tcp open netbios-ssn
445/tcp open microsoft-ds

nt20.chapman-lab.uaf.edu 137.229.27.214
Port State Service
135/tcp open loc-srv
139/tcp open netbios-ssn
445/tcp open microsoft-ds
1026/tcp open nterm

nt21.chapman-lab.uaf.edu 137.229.27.215
Port State Service
135/tcp open loc-srv
139/tcp open netbios-ssn